



Podręcznik użytkownika

T2500G-10TS (TL-SG3210)

1910012485 REV2.0.0

Listopad 2018

SPIS TREŚCI

Informacje wstępne

Do kogo skierowany jest przewodnik	1
Założenia przewodnika	1
Dodatkowe informacje.....	2

Jak zacząć

Informacje ogólne.....	4
Dostęp do interfejsu webowego (GUI)	5
Logowanie	5
Zapisywanie konfiguracji	6
Wyłączanie serwera	7
Zmiana adresu IP i bramy domyślnej przełącznika	7
Dostęp do interfejsu linii poleceń (CLI).....	9
Logowanie przez konsolę (przełączniki z portem konsoli).....	9
Logowanie przez Telnet.....	11
Logowanie przez SSH.....	12
Wyłączanie logowania przez Telnet	16
Wyłączanie logowania przez SSH.....	17
Polecenie copy running-config startup-config	17
Zmiana adresu IP i bramy domyślnej przełącznika	17

Zarządzanie systemem

System.....	20
Informacje ogólne	20
Obsługiwane funkcje	20
Konfiguracja informacji systemowych	21
Przez GUI	21
Podgląd najważniejszych ustawień systemowych.....	21
Zmiana opisu urządzenia	25
Konfiguracja czasu systemowego	26
Konfiguracja czasu letniego.....	27
Konfiguracja systemowych parametrów adresu IP	28
Konfiguracja systemowych parametrów adresu IPv6.....	29
Przez CLI.....	32

Podgląd najważniejszych informacji systemowych.....	32
Zmiana opisu urządzenia	33
Konfiguracja czasu systemowego	34
Konfiguracja czasu letniego.....	37
Konfiguracja systemowych parametrów adresu IP	39
Konfiguracja systemowych parametrów adresu IPv6.....	40
Zarządzanie kontami użytkowników	43
Przez GUI	43
Tworzenie kont	43
Konfiguracja hasła dostępu	44
Przez CLI.....	45
Tworzenie kont	45
Konfiguracja hasła dostępu	47
Konfiguracja narzędzi systemowych.....	49
Przez GUI	49
Konfiguracja pliku rozruchowego	49
Przywracanie ustawień przełącznika	51
Tworzenie kopii zapasowej pliku konfiguracyjnego	51
Aktualizacja firmware'u.....	52
Konfiguracja automatycznej instalacji DHCP	52
Restartowanie przełącznika	54
Resetowanie przełącznika.....	55
Przez CLI.....	55
Konfiguracja pliku rozruchowego	55
Przywracanie konfiguracji przełącznika	57
Tworzenie kopii zapasowej pliku konfiguracyjnego	57
Aktualizacja firmware'u.....	58
Konfiguracja automatycznej instalacji DHCP	58
Restartowanie przełącznika	60
Resetowanie przełącznika.....	61
Konfiguracja EEE.....	62
Przez CLI.....	62
Konfiguracja szablonów SDM	64
Przez GUI	64
Przez CLI.....	65
Konfiguracja przedziałów czasowych.....	67
Przez GUI	67
Dodawanie pozycji z przedziałami czasowymi.....	67

Konfiguracja okresu wakacyjnego	69
Przez CLI.....	70
Dodawanie pozycji z przedziałami czasowymi.....	70
Konfiguracja okresu wakacyjnego	71

Zarządzanie interfejsami

Interfejs fizyczny	74
Informacje ogólne	74
Obsługiwane funkcje	74
Konfiguracja podstawowych parametrów	75
Przez GUI	75
Przez CLI.....	76
Konfiguracja funkcji izolacji portów	79
Przez GUI	79
Przez CLI.....	80
Konfiguracja funkcji Loopback Detection.....	82
Przez GUI	82
Przez CLI.....	84
Przykłady konfiguracji.....	86
Przykładowa konfiguracja izolacji portu	86
Wymagania sieciowe	86
Schemat konfiguracji	86
Przez GUI.....	86
Przez CLI	88
Przykładowa konfiguracja funkcji Loopback Detection.....	89
Wymagania sieciowe	89
Schemat konfiguracji	90
Przez GUI.....	90
Przez CLI	91

Konfiguracja LAG

Grupy agregacji łączy (LAG).....	94
Informacje ogólne	94
Obsługiwane funkcje	94
Konfiguracja LAG	95
Przez GUI	96
Konfiguracja algorytmu równoważenia obciążenia pasma	96

Konfiguracja trybu statycznego LAG lub LACP	97
Przez CLI.....	99
Konfiguracja algorytmu równoważenia obciążenia pasma	99
Konfiguracja trybu statycznego LAG lub LACP	100
Przykład konfiguracji	10
Wymagania sieciowe.....	104
Schemat konfiguracji.....	104
Przez GUI	105
Przez CLI.....	106

Konfiguracja DDM

Informacje ogólne.....	109
Konfiguracja DDM.....	110
Przez GUI	110
Konfiguracja globalna DDM.....	110
Konfiguracja wartości progowych.....	111
Sprawdzanie stanu DDM.....	115
Przez CLI.....	115
Konfiguracja globalna DDM.....	115
Konfiguracja wyłączenia portów dla DDM.....	116
Konfiguracja wartości progowych.....	117
Przeglądanie konfiguracji DDM	123
Sprawdzanie stanu DDM.....	124

Zarządzanie tablicą adresów MAC

Tablica adresów MAC	126
Informacje ogólne	126
Obsługiwane funkcje	126
Konfiguracja adresów MAC	128
Przez GUI	128
Dodawanie wpisów statycznych adresów MAC.....	128
Zmiana czasu utraty ważności wpisów adresów dynamicznych.....	130
Dodawanie wpisów filtrowania adresów MAC	131
Wyświetlanie wpisów tablicy adresów	131
Przez CLI.....	132
Dodawanie wpisów statycznych adresów MAC	132
Zmiana czasu utraty ważności wpisów adresów dynamicznych.....	133

Dodawanie wpisów filtrowania adresów MAC	134
Konfiguracja zabezpieczeń	136
Przez GUI	136
Konfiguracja komunikatów trap	136
Ograniczanie liczby adresów MAC zapamiętywanych w sieciach VLAN.....	137
Przez CLI.....	138
Konfiguracja komunikatów trap	138
Ograniczanie liczby adresów MAC w sieciach VLAN.....	140
Przykład konfiguracji zabezpieczeń.....	142
Wymagania sieciowe	142
Schemat konfiguracji.....	142
Przez GUI	143
Przez CLI.....	144

Konfiguracja 802.1Q VLAN

Informacje ogólne.....	146
Konfiguracja 802.1Q VLAN	147
Przez GUI	147
Konfiguracja PVID portów	147
Konfiguracja VLAN	149
Przez CLI.....	150
Tworzenie sieci VLAN.....	150
Konfiguracja portu.....	151
Dodawanie portu do określonej sieci VLAN	152
Przykład konfiguracji	154
Wymagania sieciowe	154
Schemat konfiguracji.....	154
Topologia sieci.....	155
Przez GUI	155
Przez CLI.....	158

Konfiguracja MAC VLAN

Informacje ogólne.....	162
Konfiguracja MAC VLAN	164
Przez GUI	164
Konfiguracja 802.1Q VLAN	164
Wiązanie adresu MAC z VLAN	164

Włączanie MAC VLAN dla portu	165
Przez CLI	166
Konfiguracja 802.1Q VLAN	166
Wiązanie adresu MAC z VLAN	166
Włączanie MAC VLAN dla portu	167
Przykład konfiguracji	168
Wymagania sieciowe	168
Schemat konfiguracji	168
Przez GUI	169
Przez CLI	174

Konfiguracja protokołu VLAN

Informacje ogólne	179
Konfiguracja protokołu VLAN	180
Przez GUI	180
Konfiguracja 802.1Q VLAN	180
Tworzenie szablonów protokołu	181
Konfiguracja protokołu VLAN	182
Przez CLI	183
Konfiguracja 802.1Q VLAN	183
Tworzenie szablonu protokołu	183
Konfiguracja protokołu VLAN	184
Przykład konfiguracji	187
Wymagania sieciowe	187
Schemat konfiguracji	187
Przez GUI	189
Przez CLI	195

Konfiguracja VLAN-VPN

VLAN-VPN	200
Informacje ogólne	200
Obsługiwane funkcje	201
Podstawowa konfiguracja VLAN-VPN	202
Przez GUI	202
Konfiguracja 802.1Q VLAN	202
Podstawowa konfiguracja VLAN-VPN	203
Przez CLI	204

Konfiguracja 802.1Q VLAN	204
Podstawowa konfiguracja VLAN-VPN	204
Elastyczna konfiguracja VLAN-VPN	207
Przez GUI	207
Przez CLI	208
Przykłady konfiguracji	210
Przykład podstawowego VLAN VPN	210
Wymagania sieciowe	210
Schemat konfiguracji	210
Przez GUI	211
Przez CLI	218
Przykład elastycznego VLAN VPN	221
Wymagania sieciowe	221
Schemat konfiguracji	222
Przez GUI	222
Przez CLI	231

Konfiguracja GVRP

Informacje ogólne	235
Konfiguracja GVRP	236
Przez GUI	237
Przez CLI	239
Przykład konfiguracji	242
Wymagania sieciowe	242
Schemat konfiguracji	242
Przez GUI	243
Przez CLI	247

Konfiguracja multicastu L2

Multicast warstwy 2	252
Informacje ogólne	252
Obsługiwane funkcje	254
Konfiguracja IGMP Snooping	255
Przez GUI	255
Konfiguracja globalna IGMP Snooping	255
Konfiguracja IGMP Snooping dla VLAN-ów	256
Konfiguracja IGMP Snooping dla portów	260

Konfiguracja statycznego dołączania hostów do grup	260
Konfiguracja funkcji IGMP Accounting i IGMP Authentication	261
Przez CLI	263
Globalna konfiguracja IGMP Snooping	263
Konfiguracja IGMP Snooping dla VLAN-ów	264
Konfiguracja IGMP Snooping dla portów	269
Konfiguracja statycznego dołączania hostów do grup	270
Konfiguracja funkcji IGMP Accounting i IGMP Authentication	271
Konfiguracja MLD Snooping	275
Przez GUI	275
Konfiguracja globalna MLD Snooping	275
Konfiguracja MLD Snooping dla VLAN-ów	276
Konfiguracja MLD Snooping dla portów	279
Konfiguracja statycznego dołączania hostów do grup	280
Przez CLI	280
Konfiguracja globalna MLD Snooping	280
Konfiguracja MLD Snooping dla VLAN-ów	281
Konfiguracja MLD Snooping dla portów	286
Konfiguracja statycznego dołączania hostów do grup	287
Konfiguracja MVR	289
Przez GUI	289
Konfiguracja VLAN-ów standardu 802.1Q	289
Globalna konfiguracja MVR	290
Dodawanie grup multicastowych do MVR	291
Konfiguracja MVR dla portów	292
(Opcjonalnie) Statyczne dodawanie portów do grup MVR	293
Przez CLI	294
Konfiguracja VLAN-ów standardu 802.1Q	294
Globalna konfiguracja MVR	294
Konfiguracja MVR dla portów	296
Konfiguracja filtrowania pakietów multicastu	299
Przez GUI	299
Tworzenie profili multicast	299
Konfiguracja filtrowania pakietów multicastu dla portów	301
Przez CLI	302
Tworzenie profili multicast	302
Tworzenie powiązań portów z profilami	305
Przeglądanie informacji Multicast Snooping	309

Przez GUI	309
Przeglądanie tablicy adresów IPv4 multicast	309
Przeglądanie statystyk pakietów IPv4 na poszczególnych portach	310
Przeglądanie tablicy adresów IPv6 multicast	311
Przeglądanie statystyk pakietów IPv6 na poszczególnych portach	312
Przez CLI	313
Przeglądanie informacji o Multicast Snooping IPv4	313
Przeglądanie informacji o Multicast Snooping IPv6	313
Przykłady konfiguracji	314
Przykład podstawowej konfiguracji IGMP Snooping	314
Wymagania sieciowe	314
Schemat konfiguracji	314
Przez GUI	315
Przez CLI	317
Przykład konfiguracji MVR	319
Wymagania sieciowe	319
Topologia sieci	319
Schemat konfiguracji	320
Przez GUI	320
Przez CLI	323
Przykład konfiguracji Unknown Multicast i Fast Leave	326
Wymagania sieciowe	326
Schemat konfiguracji	327
Przez GUI	327
Przez CLI	329
Przykład konfiguracji filtrowania pakietów multicastu	330
Wymagania sieciowe	330
Schemat konfiguracji	330
Topologia sieci	331
Przez GUI	331
Przez CLI	335

Konfiguracja Spanning Tree

Spanning Tree	339
Informacje ogólne	339
Podstawowe pojęcia	340
Podstawowe pojęcia STP/RSTP	340

Podstawowe pojęcia MSTP	343
STP Security.....	345
Konfiguracja STP/RSTP	347
Przez GUI	347
Konfiguracja parametrów STP/RSTP na portach.....	347
Konfiguracja globalna STP/RSTP.....	349
Sprawdzanie konfiguracji STP/RSTP	351
Przez CLI.....	353
Konfiguracja parametrów STP/RSTP na portach.....	353
Konfiguracja parametrów globalnych STP/RSTP	355
Włączanie STP/RSTP globalnie.....	357
Konfiguracja MSTP.....	359
Przez GUI	359
Konfiguracja parametrów na portach w CIST	359
Konfiguracja regionu MSTP	362
Konfiguracja globalna MSTP	366
Sprawdzanie konfiguracji MSTP	368
Przez CLI.....	369
Konfiguracja parametrów na portach w CIST	369
Konfiguracja regionu MSTP	372
Konfiguracja globalnych parametrów MSTP.....	375
Włączanie globalnie funkcji Spanning Tree.....	377
Konfiguracja zabezpieczeń STP	379
Przez GUI	379
Przez CLI.....	380
Konfiguracja zabezpieczeń STP	380
Przykład konfiguracji MSTP	383
Wymagania sieciowe.....	383
Schemat konfiguracji.....	383
Przez GUI	384
Przez CLI.....	390
Konfiguracja LLDP	
LLDP.....	398
Informacje ogólne	398
Obsługiwane funkcje	398
Konfiguracja LLDP	399

Przez GUI	399
Globalna konfiguracja LLDP	399
Konfiguracja LLDP dla portów	401
Przez CLI	402
Konfiguracja globalna	402
Konfiguracja portów	404
Konfiguracja LLDP-MED	407
Przez GUI	407
Globalna konfiguracja LLDP	407
Globalna konfiguracja LLDP-MED	407
Konfiguracja LLDP-MED dla portów.....	408
Przez CLI	410
Konfiguracja globalna	410
Konfiguracja portów	411
Przeglądanie ustawień LLDP	414
Przez GUI	414
Przeglądanie informacji urządzenia o LLDP	414
Przeglądanie statystyk LLDP	418
Przez CLI	419
Przeglądanie ustawień LLDP-MED.....	420
Przez GUI	420
Przez CLI	423
Przykład konfiguracji	424
Wymagania sieciowe	424
Topologia sieci.....	424
Schemat konfiguracji.....	424
Przez GUI	424
Przez CLI.....	425
Konfiguracja L2PT	
Informacje ogólne.....	433
Konfiguracja L2PT	435
Przez GUI	435
Przez CLI.....	436
Przykład konfiguracji	440
Wymagania sieciowe	440
Schemat konfiguracji.....	440

Przez GUI	441
Przez CLI.....	441

Konfiguracja PPPoE ID Insertion

Informacje ogólne.....	444
Konfiguracja PPPoE ID Insertion.....	445
Przez GUI	445
Przez CLI.....	446

Konfiguracja usługi DHCP

DHCP	450
Informacje ogólne	450
Obsługiwane funkcje	450
Konfiguracja DHCP Relay	452
Przez GUI	452
Włączanie DHCP Relay i konfiguracja Opcji 82.....	452
Konfiguracja DHCP VLAN Relay	454
Przez CLI.....	455
Włączanie DHCP Relay	455
(Opcjonalnie) Konfiguracja opcji 82	456
Konfiguracja DHCP VLAN Relay	457
Konfiguracja DHCP L2 Relay	459
Przez GUI	459
Włączanie DHCP L2 Relay	459
Konfiguracja opcji 82 dla portów.....	460
Przez CLI.....	461
Włączanie DHCP L2 Relay	461
Konfiguracja opcji 82 dla portów.....	462
Przykład wdrożenia DHCP VLAN Relay	464
Wymagania sieciowe	464
Schemat konfiguracji.....	464
Przez GUI	465
Przez CLI.....	465

Konfiguracja QoS

QoS.....	472
Informacje ogólne	472

Obsługiwane funkcje	472
Konfiguracja usług Class of Service	474
Przez GUI	475
Konfiguracja priorytetyzacji portów	475
Konfiguracja priorytetyzacji 802.1p	477
Konfiguracja priorytetyzacji DSCP	479
Konfiguracja ustawień harmonogramu	481
Przez CLI	483
Konfiguracja priorytetyzacji portów	483
Konfiguracja priorytetyzacji 802.1p	485
Konfiguracja priorytetyzacji DSCP	488
Konfiguracja ustawień harmonogramu	492
Konfiguracja kontroli przepustowości	495
Przez GUI	495
Konfiguracja limitu prędkości	495
Konfiguracja Storm Control	496
Przez CLI	497
Konfiguracja limitu prędkości	497
Konfiguracja Storm Control	498
Konfiguracja Voice VLAN	501
Przez GUI	501
Konfiguracja adresów OUI	501
Konfiguracja globalna Voice VLAN	502
Dodawanie portów do Voice VLAN	503
Przez CLI	504
Konfiguracja Auto VoIP	507
Przez GUI	507
Przez CLI	508
Przykłady konfiguracji	512
Przykład dla usług Class of Service	512
Wymagania sieciowe	512
Schemat konfiguracji	512
Przez GUI	513
Przez CLI	515
Przykład dla usługi Voice VLAN	517
Wymagania sieciowe	517
Schemat konfiguracji	518
Przez GUI	518

Przez CLI	522
Przykład dla usługi Auto VoIP	525
Wymagania sieciowe	525
Schemat konfiguracji	526
Przez GUI.....	526
Przez CLI	531

Konfiguracja Access Security

Access Security	537
Informacje ogólne	537
Obsługiwane funkcje	537
Konfiguracja Access Security.....	538
Przez GUI	538
Konfiguracja funkcji Access Control.....	538
Konfiguracja funkcji HTTP	541
Konfiguracja funkcji HTTPS.....	543
Konfiguracja funkcji SSH.....	546
Konfiguracja funkcji Telnet	547
Konfiguracja parametrów portu szeregowego.....	548
Przez CLI.....	548
Konfiguracja funkcji Access Control.....	548
Konfiguracja funkcji HTTP	550
Konfiguracja funkcji HTTPS.....	552
Konfiguracja funkcji SSH.....	554
Konfiguracja funkcji Telnet	557
Konfiguracja parametrów portu szeregowego.....	557

Konfiguracja AAA

Informacje ogólne.....	560
Konfiguracja AAA.....	561
Przez GUI	562
Dodawanie serwerów	562
Konfiguracja grup serwerów.....	564
Konfiguracja listy metod	565
Konfiguracja listy aplikacji AAA	566
Konfiguracja konta logowania i hasła dostępu.....	567
Przez CLI.....	568

Dodawanie serwerów	568
Konfiguracja grup serwerów	570
Konfiguracja listy metod	571
Konfiguracja listy aplikacji AAA	573
Konfiguracja konta logowania i hasła dostępu.....	576
Przykład konfiguracji	578
Wymagania sieciowe	578
Schemat konfiguracji.....	578
Przez GUI	579
Przez CLI.....	581

Konfiguracja 802.1x

Informacje ogólne.....	585
Konfiguracja 802.1x	587
Przez GUI	587
Konfiguracja serwera RADIUS	587
Konfiguracja globalna 802.1x.....	590
Konfiguracja 802.1x na portach.....	591
Sprawdzanie stanu wystawcy uwierzytelnienia.....	593
Przez CLI.....	594
Konfiguracja serwera RADIUS	594
Konfiguracja globalna 802.1x.....	596
Konfiguracja 802.1x na portach.....	598
Sprawdzanie stanu wystawcy uwierzytelnienia.....	600
Przykład konfiguracji	602
Wymagania sieciowe	602
Schemat konfiguracji.....	602
Topologia sieci.....	602
Przez GUI	603
Przez CLI.....	605

Konfiguracja Port Security

Informacje ogólne.....	609
Konfiguracja Port Security	610
Przez GUI	610
Przez CLI.....	611

Konfiguracja ACL

Informacje ogólne.....	615
Konfiguracja ACL	616
Przez GUI	616
Konfiguracja zakresu czasu	616
Tworzenie ACL	616
Konfiguracja reguł ACL.....	617
Konfiguracja reguły MAC ACL.....	617
Konfiguracja reguły IP ACL.....	621
Konfiguracja łączonej reguły ACL	624
Konfiguracja reguły IPv6 ACL	630
Konfiguracja wiązania ACL.....	634
Przez CLI.....	635
Konfiguracja zakresu czasu	635
Configuring ACL	635
Configuring Policy.....	644
Configuring ACL Binding.....	646
Viewing ACL Counting	647
Przykład konfiguracji ACL.....	648
Przykład konfiguracji MAC ACL	648
Wymagania sieciowe	648
Schemat konfiguracji	648
Przez GUI.....	649
Przez CLI	655
Przykład konfiguracji IP ACL.....	656
Wymagania sieciowe	656
Schemat konfiguracji	657
Przez GUI.....	657
Przez CLI	664
Przykład konfiguracji dla łączonej listy ACL.....	666
Wymagania sieciowe	666
Schemat konfiguracji	666
Przez GUI.....	667
Przez CLI	672

Konfiguracja IMPB IPv4

IMPB IPv4	675
-----------------	-----

Informacje ogólne	675
Obsługiwane funkcje	675
Konfiguracja wiązania IP-MAC	676
Przez GUI	676
Ręczne wiązanie wpisów	676
Wiązanie wpisów poprzez ARP Scanning	678
Wiązanie wpisów poprzez DHCP Snooping	680
Wyświetlanie wpisów wiązania	681
Przez CLI	682
Ręczne wiązanie wpisów	682
Wiązanie wpisów poprzez DHCP Snooping	684
Wyświetlanie wpisów wiązania	685
Konfiguracja funkcji ARP Detection	686
Przez GUI	686
Dodawanie wpisów wiązania IP-MAC	686
Włączanie funkcji ARP Detection	686
Konfiguracja funkcji ARP Detection na portach	687
Wyświetlanie statystyk ARP	688
Przez CLI	689
Dodawanie wpisów wiązania IP-MAC	689
Włączanie funkcji ARP Detection	689
Konfiguracja funkcji ARP Detection na portach	691
Wyświetlanie statystyk ARP	692
Konfiguracja funkcji IPv4 Source Guard	693
Przez GUI	693
Dodawanie wpisów wiązania IP-MAC	693
Konfiguracja funkcji IPv4 Source Guard	693
Przez CLI	694
Dodawanie wpisów wiązania IP-MAC	694
Konfiguracja funkcji IPv4 Source Guard	694
Przykłady konfiguracji	696
Przykład dla ARP Detection	696
Wymagania sieciowe	696
Schemat konfiguracji	696
Przez GUI	697
Przez CLI	699
Przykład dla IP Source Guard	701
Wymagania sieciowe	701

Schemat konfiguracji	701
Przez GUI	701
Przez CLI	703

Konfiguracja IMPB IPv6

IMPB IPv6	706
Informacje ogólne	706
Obsługiwane funkcje	706
Konfiguracja wiązania IPv6-MAC	708
Przez GUI	708
Ręczne wiązanie wpisów	708
Wiązanie wpisów poprzez ND Snooping	709
Wiązanie wpisów przez DHCPv6 Snooping	711
Wyświetlanie wpisów wiązania	712
Przez CLI	713
Ręczne wiązanie wpisów	713
Wiązanie wpisów poprzez ND Snooping	715
Wiązanie wpisów przez DHCPv6 Snooping	716
Wyświetlanie wpisów wiązania	717
Konfiguracja funkcji ND Detection	718
Przez GUI	718
Dodawanie wpisów wiązania IPv6-MAC	718
Włączanie funkcji ND Detection	718
Konfiguracja funkcji ND Detection na portach	719
Wyświetlanie statystyk ND	720
Przez CLI	720
Dodawanie wpisów wiązania IPv6-MAC	720
Włączanie funkcji ND Detection	722
Konfiguracja funkcji ND Detection na portach	722
Wyświetlanie statystyk ND	722
Konfiguracja funkcji IPv6 Source Guard	724
Przez GUI	724
Dodawanie wpisów wiązania IPv6-MAC	724
Konfiguracja funkcji IPv6 Source Guard	724
Przez CLI	725
Dodawanie wpisów wiązania IPv6-MAC	725
Konfiguracja funkcji IPv6 Source Guard	725

Przykłady konfiguracji	727
Przykład dla ND Detection.....	727
Wymagania sieciowe	727
Schemat konfiguracji.....	727
Przez GUI.....	728
Przez CLI	730
Przykład dla IPv6 Source Guard	731
Wymagania sieciowe	731
Schemat konfiguracji.....	732
Przez GUI.....	732
Przez CLI	734

Konfiguracja filtrowania DHCP

Filtrowanie DHCP	736
Informacje ogólne	736
Obsługiwane funkcje	736
Konfiguracja filtrowania DHCPv4	738
Przez GUI	738
Konfiguracja podstawowych parametrów filtrowania DHCPv4.....	738
Konfiguracja legalnych serwerów DHCPv4.....	740
Przez CLI.....	740
Konfiguracja podstawowych parametrów filtrowania DHCPv4.....	740
Konfiguracja legalnych serwerów DHCPv4.....	742
Konfiguracja filtrowania DHCPv6	744
Przez GUI	744
Konfiguracja podstawowych parametrów filtrowania DHCPv6.....	744
Konfiguracja legalnych serwerów DHCPv6.....	745
Przez CLI.....	746
Konfiguracja podstawowych parametrów filtrowania DHCPv6.....	746
Konfiguracja legalnych serwerów DHCPv6.....	747
Przykłady konfiguracji	749
Przykład dla filtrowania DHCPv4	749
Wymagania sieciowe	749
Schemat konfiguracji.....	749
Przez GUI.....	750
Przez CLI	751
Przykład dla filtrowania DHCPv6	752

Wymagania sieciowe	752
Schemat konfiguracji	753
Przez GUI	753
Przez CLI	755

Konfiguracja DoS Defend

Informacje ogólne.....	758
Konfiguracja DoS Defend	759
Przez GUI	759
Przez CLI	760

Monitorowanie systemu

Informacje ogólne.....	764
Monitorowanie procesora	765
Przez GUI	765
Przez CLI	765
Monitorowanie pamięci	767
Przez GUI	767
Przez CLI	767

Monitorowanie ruchu

Monitorowanie ruchu.....	770
Przez GUI	770
Przez CLI	773

Port Mirroring

Mirroring	775
Przez GUI	775
Przez CLI	777
Przykłady konfiguracji	779
Wymagania sieciowe	779
Schemat konfiguracji	779
Przez GUI	779
Przez CLI	781

Konfiguracja DLDAP

Informacje ogólne.....	783
------------------------	-----

Konfiguracja DLDP	784
Przez GUI	784
Przez CLI	786

Konfiguracja SNMP i RMON

SNMP	789
Informacje ogólne	789
Podstawowe pojęcia	789
Konfiguracja SNMP	793
Przez GUI	793
Włączanie SNMP	793
Tworzenie widoku SNMP	794
Tworzenie społeczności SNMP (SNMP v1/v2c)	795
Tworzenie grupy SNMP (SNMP v3)	796
Tworzenie użytkowników SNMP (SNMP v3)	797
Przez CLI	799
Włączanie SNMP	799
Tworzenie widoku SNMP	800
Tworzenie społeczności SNMP (SNMP v1/v2c)	801
Tworzenie grupy SNMP (SNMP v3)	802
Tworzenie użytkowników SNMP (SNMP v3)	804
Konfiguracja powiadomień	806
Przez GUI	806
Konfiguracja informacji o hostach NMS	806
Włączanie SNMP Traps	808
Przez CLI	810
Konfiguracja hostów NMS	810
Włączanie SNMP Traps	811
RMON	817
Konfiguracja RMON	818
Przez GUI	818
Konfiguracja Statystyk	818
Konfiguracja Historii	819
Konfiguracja Zdarzeń	820
Konfiguracja Alarmu	821
Przez CLI	824
Konfiguracja Statystyk	824

Konfiguracja Historii.....	825
Konfiguracja Zdarzeń.....	826
Konfiguracja Alarmu	827
Przykład konfiguracji	830
Wymagania sieciowe.....	830
Schemat konfiguracji.....	831
Przez GUI	831
Przez CLI.....	836

Konfiguracja dzienników systemowych

Informacje ogólne.....	843
Konfiguracja dzienników systemowych.....	844
Przez GUI	845
Konfiguracja dzienników lokalnych.....	845
Konfiguracja dzienników zdalnych	845
Tworzenie kopii zapasowych dzienników.....	846
Wyświetlanie tablicy dzienników.....	847
Przez CLI.....	847
Konfiguracja dzienników lokalnych.....	847
Konfiguracja dzienników zdalnych	849
Przykład konfiguracji	851
Wymagania sieciowe.....	851
Schemat konfiguracji.....	851
Przez GUI	851
Przez CLI.....	852

Diagnostyka urządzenia i sieci

Diagnostyka urządzenia	854
Przez GUI	854
Przez CLI.....	855
Diagnostyka sieci.....	856
Przez GUI	856
Rozwiązywanie problemów poprzez testy Ping	856
Rozwiązywanie problemów poprzez testy Tracert.....	857
Przez CLI.....	858
Konfiguracja testu Ping.....	858
Konfiguracja testu Tracert.....	859

Informacje wstępne

Niniejszy podręcznik konfiguracji zawiera informacje dotyczące zarządzania przełącznikiem T2500G-10TS(TL-SG3210). Zapoznaj się uważnie z podręcznikiem przed rozpoczęciem pracy.

Do kogo skierowany jest przewodnik

Niniejszy przewodnik przeznaczony jest dla administratorów sieci zaznajomionych z pojęciami z dziedziny IT i terminologią sieciową.


Założenia przewodnika

Niektóre urządzenia opisane w tym przewodniku mogą nie być dostępne w twoim kraju lub regionie. Informacje o dostępnych modelach znajdują się na stronie <https://www.tp-link.com/pl/>.

Korzystając z tego przewodnika pamiętaj, że funkcje przełącznika mogą się nieznacznie różnić w zależności od posiadanego modelu i wersji oprogramowania. Wszystkie zrzuty ekranu, rysunki, parametry i opisy znajdujące się w tym przewodniku mają charakter poglądowy.

Informacje zawarte w tym dokumencie mogą ulegać zmianom bez uprzedniego powiadomienia. W procesie przygotowywania niniejszego dokumentu dołożono wszelkich starań, aby zapewnić dokładność i rzetelność treści, ale wszelkie oświadczenia, informacje i zalecenia zawarte w tym dokumencie nie stanowią gwarancji ani pośredniej, ani wyrażonej wprost. Użytkownicy ponoszą pełną odpowiedzialność za użytkowanie zakupionych produktów.

W niniejszym przewodniku występują następujące oznaczenia:

Symbol  odnosi się do hasła *Uwaga*. Uwagi zawierają sugestie lub odniesienia, które są pomocne przy użytkowaniu urządzenia.

- Przez GUI:

Menu Name > Submenu Name > Tab page odnosi się do struktury menu. **SYSTEM > System Info > System Summary** oznacza, że strona System Summary wyświetli się po naciśnięciu opcji System Info, która z kolei znajduje się w sekcji System.

Pogrubiona czcionka oznacza przycisk, ikonę paska narzędzi, menu lub element menu.

- Przez CLI:

Pogrubiona czcionka	Niepodlegające zmianom słowo kluczowe. Przykład: show logging
----------------------------	---

Zwykła czcionka	Stała (jedna opcja do wyboru spośród kilku dostępnych). Przykład: no bandwidth {all ingress egress}
{ }	Elementy w nawiasach klamrowych { } są wymagane.
[]	Elementy w nawiasach kwadratowych [] są opcjonalne,
	Alternatywne elementy są pogrupowane w nawiasach i oddzielone pionowymi kreskami . Przykład: speed {10 100 1000}
<i>Kursywa czcionki</i>	Zmienna (należy podać rzeczywistą wartość). Przykład: bridge aging-time <i>aging-time</i>

Często występujące połączenie:

{ [] [] }	Należy wybrać co najmniej jeden element z nawiasu kwadratowego. Przykład: bandwidth {[ingress <i>ingress-rate</i>] [egress <i>egress-rate</i>]}
-------------	---

To polecenie można zastosować w trzech przypadkach:

- bandwidth ingress** *ingress-rate* służy do ograniczania przepustowości na wejściu.
- bandwidth egress** *egress-rate* służy do ograniczania przepustowości na wyjściu.
- bandwidth ingress** *ingress-rate* **egress** *egress-rate* służy do ograniczania przepustowości na wejściu i wyjściu.

Dodatkowe informacje

- Najnowsze wersje oprogramowania i dokumenty znajdują się w na stronie Do pobrania pod adresem <https://www.tp-link.com/pl/support>.
- Instrukcja instalacji (IG) znajduje się na tej samej stronie, co ten przewodnik, a także w opakowaniu produktu.
- Szczegółowe specyfikacje urządzeń znajdują się na stronach produktowych pod adresem <https://www.tp-link.com/pl/>.
- Forum wsparcia technicznego TP-Link znajduje się pod adresem <https://community.tp-link.com/en/business/>.
- Kontakt do wsparcia technicznego znajduje się na stronie Wsparcie pod adresem <https://www.tp-link.com/pl/support>.

Część 1

Jak zacząć

ROZDZIAŁY

1. Informacje ogólne
2. Dostęp do interfejsu webowego (GUI)
3. Dostęp do interfejsu linii poleceń (CLI)

1 Informacje ogólne

Dostęp do przełącznika można uzyskać poprzez GUI (graficzny interfejs użytkownika, określany w tej instrukcji także jako interfejs webowy) lub poprzez CLI (interfejs linii poleceń). Zarówno GUI, jak i CLI obsługują te same funkcje przełącznika, jednak konfiguracja poprzez interfejs webowy jest bardziej intuicyjna niż konfiguracja poprzez interfejs linii poleceń. Wybór metody zależy od określonych zastosowań oraz od osobistych preferencji użytkownika.

2 Dostęp do interfejsu webowego (GUI)

Dostęp do interfejsu webowego przełącznika uzyskać można przez uwierzytelnianie przez stronę internetową. Do uwierzytelniania użytkowników przełącznik wykorzystuje dwa wbudowane serwery sieciowe, serwer HTTP i HTTPS.

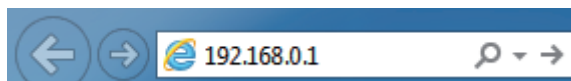
Poniższy przykład prezentuje, jak zalogować się przez serwer HTTP.

2.1 Logowanie

Aby zarządzać przełącznikiem przez przeglądarkę hosta::

- 1) Upewnij się, że ścieżka pomiędzy hostem a przełącznikiem jest dostępna.
- 2) Uruchom przeglądarkę. Przykładowe obsługiwane przeglądarki:
 - IE 8.0, 9.0, 10.0, 11.0
 - Firefox 26.0, 27.0
 - Chrome 32.0, 33.0
- 3) W pasku adresu przeglądarki wpisz adres IP przełącznika. Domyślny adres to 192.168.0.1.

Rys. 2-1 Wpisywanie adresu IP przełącznika w przeglądarce



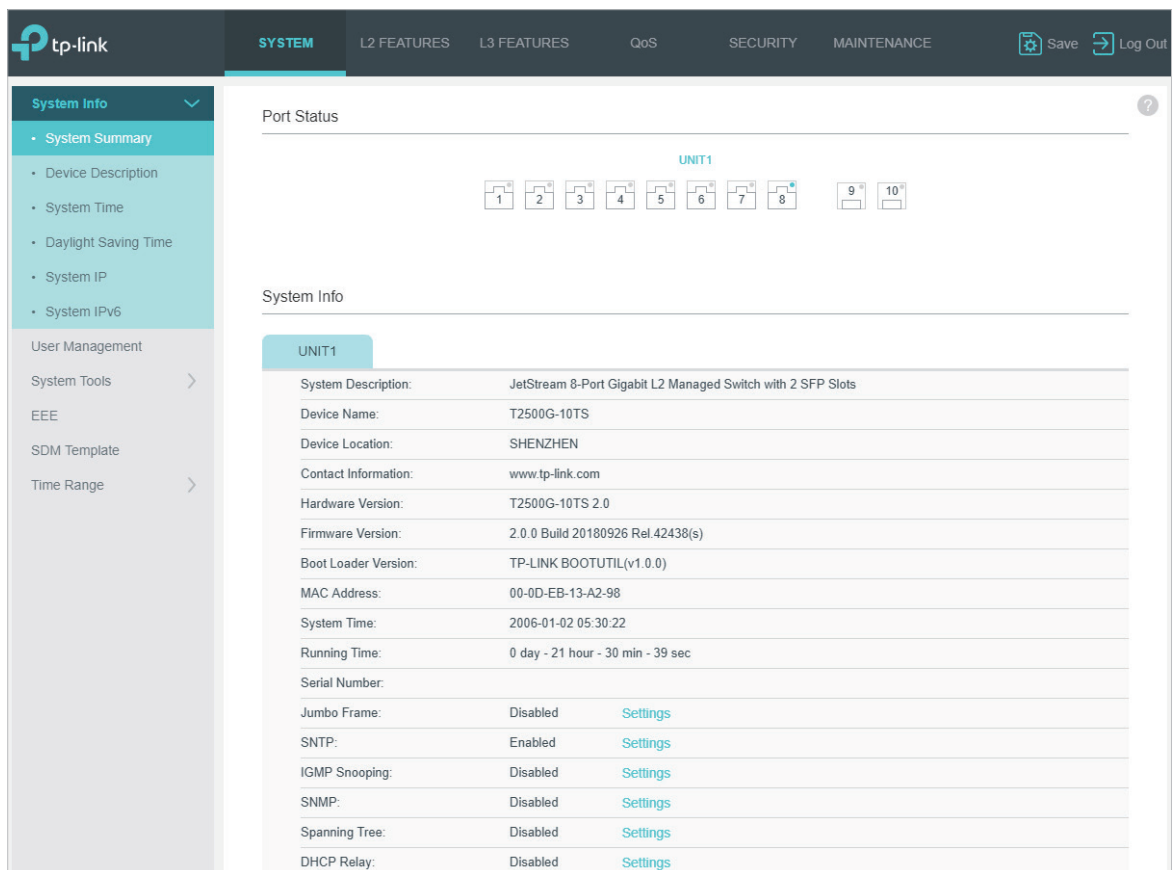
- 4) W wyskakującym oknie logowania wpisz nazwę użytkownika i hasło (domyślna wartość obu pól to: **admin**).

Rys. 2-1 Uwierzytelnianie logowania

A screenshot of a login form. It has two input fields: 'Username' with the text 'admin' and a user icon, and 'Password' with masked characters '.....' and a lock icon. Below the password field is a checkbox labeled 'Remember Me'. At the bottom is a large teal button labeled 'Log In'.

- 5) Poniżej zamieszczono zdjęcie typowego interfejsu webowego. W interfejsie możesz sprawdzić aktualny status przełącznika oraz skonfigurować przełącznik.

Rys. 2-2 Interfejs webowy



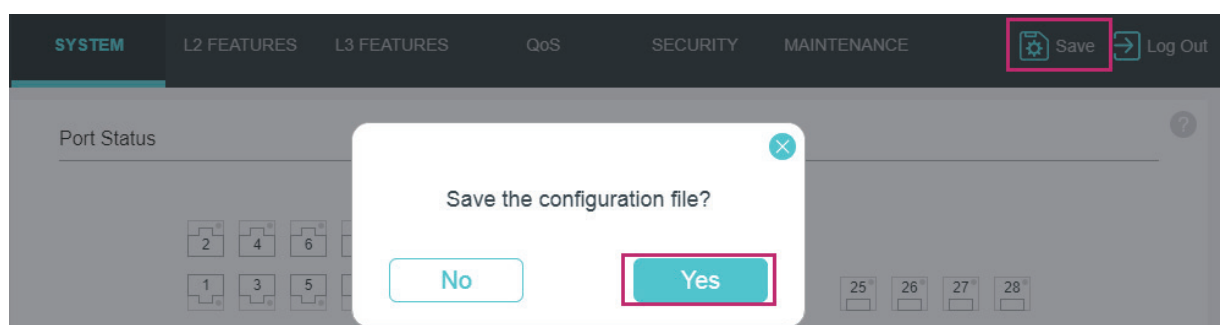
2.2 Zapisywanie konfiguracji

Pliki konfiguracyjne przełącznika dzielą się na dwa typy - plik bieżącej konfiguracji i plik konfiguracji startowej.

Po przeprowadzeniu konfiguracji na subinterfejsach i kliknięciu **Apply** zmiany zostaną zapisane w pliku bieżącej konfiguracji. Po restarcie przełącznika ustawienia zostaną utracone.

Chcąc zachować konfigurację po restarcie przełącznika należy użyć funkcji **Save** w interfejsie głównym - konfiguracja zostanie zapisana w pliku konfiguracji startowej.

Rys. 2-3 Zapisywanie konfiguracji



2.3 Wyłączanie serwera

Aby zablokować dostęp do interfejsu webowego, możesz wyłączyć serwer HTTP lub HTTPS.

Przejdź do **SECURITY > Access Security > HTTP Config**, wyłącz serwer HTTP i kliknij **Apply**.

Rys. 2-4 Wyłączanie serwera HTTP

Global Config

HTTP: Enable

Port: (1-65535)

Apply

Przejdź do **SECURITY > Access Security > HTTPS Config**, wyłącz serwer HTTPS i kliknij **Apply**.

Rys. 2-5 Wyłączanie serwera HTTPS

Global Config

HTTPS: Enable

SSL Version 3: Enable

TLS Version 1: Enable

Port: (1-65535)

Apply

2.4 Zmiana adresu IP i bramy domyślnej przełącznika

W celu uzyskania dostępu do przełącznika, ustaw adres IP przełącznika. Jeżeli chcesz, żeby przełącznik miał dostęp do sieci, skonfiguruj bramę domyślną urządzenia. Tylko komputery w zarządzającej sieci VLAN mają dostęp do interfejsu zarządzania przełącznikiem. Domyślnie wszystkie porty w sieci zarządzającej VLAN należą do VLAN 1, możesz więc połączyć się z przełącznikiem poprzez każdy port. Domyślny adres IP to **192.168.0.1**. Przełącznik nie ma bramy domyślnej. Poniższy przykład prezentuje zmianę adresu IP i bramy domyślnej przełącznika,

- 1) Przejdź do **SYSTEM > System Info > System IP**. Podaj ID sieci zarządzającej VLAN. Ustaw tryb adresu IP jako **Static**. Wpisz nowy adres IP, maskę podsieci i bramę domyślną. Upewnij się, że ścieżka między hostem a nowym adresem IP przełącznika jest dostępna. Kliknij **Apply**.

Rys. 2-6 Zmiana IP przełącznika i bramy domyślnej

System IP Config

MAC Address: 00-0A-EB-13-A2-11


Management VLAN ID: (1-4094)

IP Address Mode: Static DHCP BOOTP

IP Address: (Format: 192.168.0.1)

Subnet Mask: (Format: 255.255.255.0)

Default Gateway: (Format: 192.168.0.1)

- 2) Aby uzyskać dostęp do przełącznika, w polu adresowym przeglądarki wpisz nowy adres IP.
- 3) Kliknij  Save, aby zapisać ustawienia.

3 Dostęp do interfejsu linii poleceń (CLI)

Użytkownicy mogą przez konsolę (tylko w przypadku przełączników z portem konsoli), połączenie Telnet lub SSH uzyskać dostęp do CLI przełącznika i zarządzać urządzeniem przez linie poleceń.

Połączenie przez konsolę wymaga bezpośredniego podłączenia hosta do portu konsoli przełącznika. Połączenie przez Telnet i SSH umożliwia zarówno dostęp lokalny, jak i dostęp zdalny.

Poniższa tabela prezentuje typowe wykorzystanie dostępu do interfejsu linii poleceń.

Tabela 3-1 Lista metod

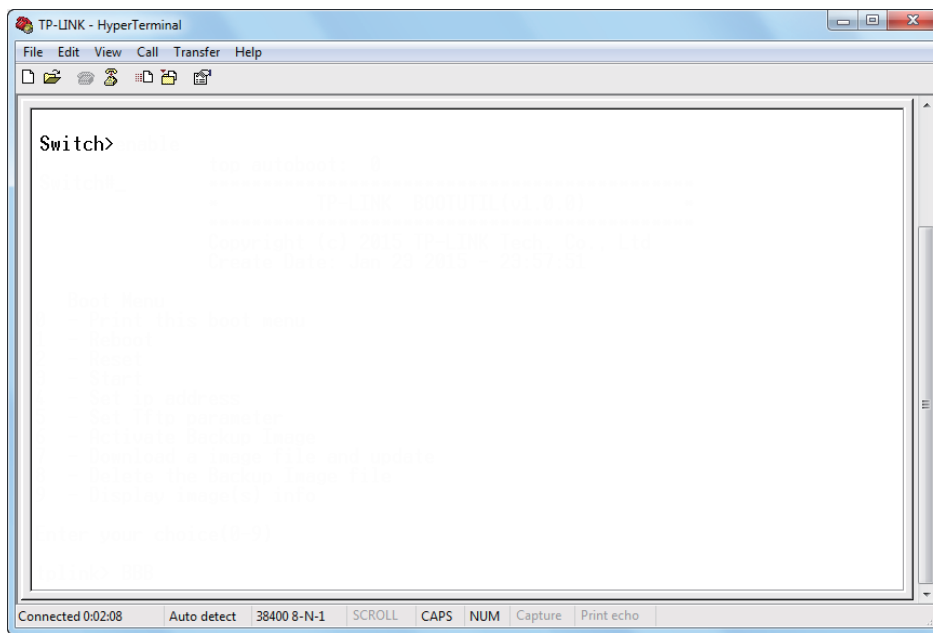
Metoda	Wykorzystywany port	Typowe zastosowanie
Konsola	Port konsoli (bezpośrednio połączony)	HyperTerminal
Telnet	Port RJ-45	CMD
SSH	Port RJ-45	Putty

3.1 Logowanie przez konsolę (przełączniki z portem konsoli)

Wykonaj poniższe kroki, aby zalogować się do przełącznika za pomocą portu konsoli:

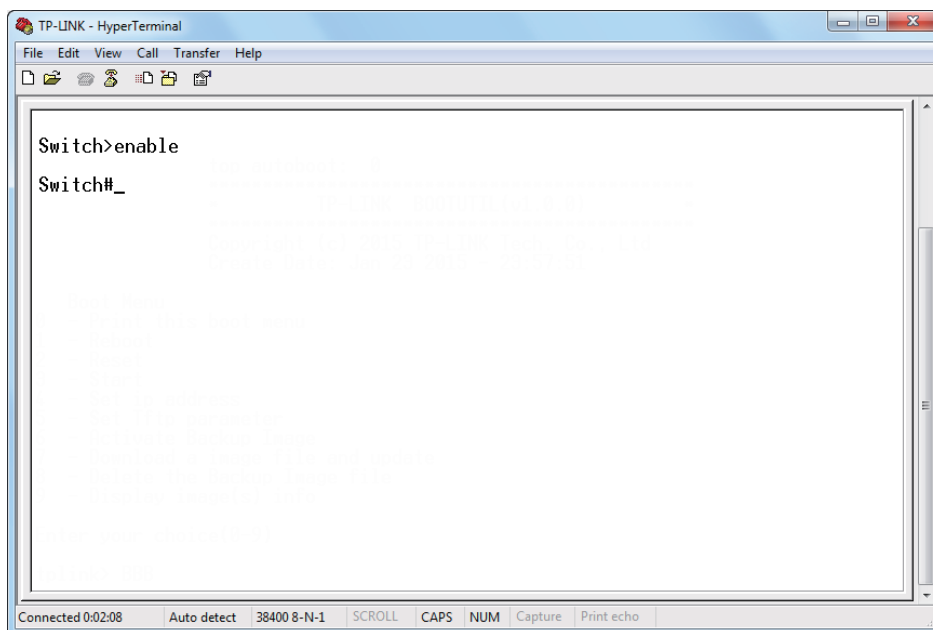
- 1) Podłącz komputer lub terminal do portu konsoli przełącznika za pomocą kabla szeregowego.
- 2) Uruchom emulator terminala (np. HyperTerminal) na komputerze i skonfiguruj go w następujący sposób:
 - Baud Rate: 38400bps
 - Data Bits: 8
 - Parity: None
 - Stop Bits: 1
 - Flow Control: None
- 3) Naciśnij **Enter** w oknie głównym. Wyświetli się **Switch>**, co oznacza, że logowanie do przełącznika powiodło się i można już korzystać z CLI.

Rys. 3-1 Okno główne CLI



- 4) Wpisz **enable**, aby uruchomić tryb User EXEC i przejść do dalszej konfiguracji przełącznika.

Rys. 3-2 Tryb User EXEC



 **Uwaga:**

Jeśli korzystasz z Windows XP, przejdź do **Start > Wszystkie programy > Akcesoria > Komunikacja > HyperTerminal**, aby otworzyć HyperTerminal i skonfigurować powyższe ustawienia w celu zalogowania się do przełącznika.

3.2 Logowanie przez Telnet

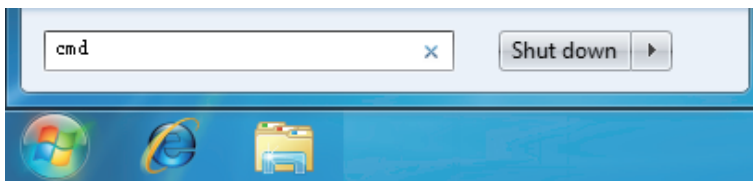
Domyślnie przełącznik wykorzystuje do uwierzytelniania tryb logowania lokalnego (Login Local Mode).

Tryb logowania lokalnego: wymagane jest podanie nazwy użytkownika i hasła (domyślna wartość obu pól to: admin).

Poniższe kroki prezentują, jak zarządzać przełącznikiem poprzez tryb logowania lokalnego:

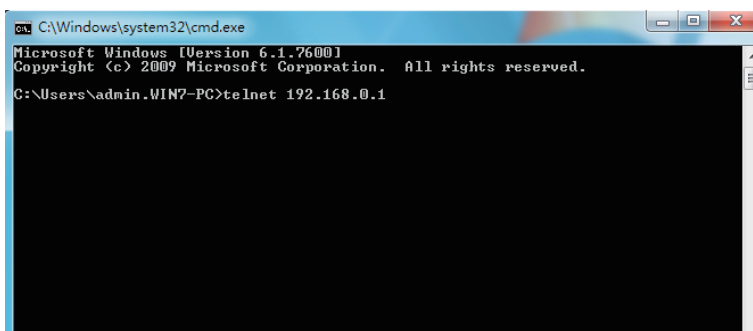
- 1) Upewnij się, że przełącznik i komputer należą do tej samej sieci LAN (Local Area Network). Kliknij **Start**, wpisz **cmd** w pasku wyszukiwania i kliknij **Enter**.

Rys. 3-3 Otwieranie okna cmd



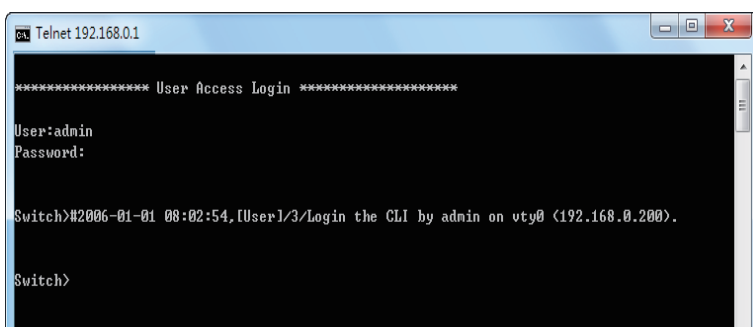
- 2) W oknie cmd wpisz **telnet 192.168.0.1** i kliknij **Enter**.

Rys. 3-4 Logowanie do przełącznika



- 2) Wpisz nazwę użytkownika i hasło logowania (domyślnie **admin**). Kliknij **Enter**, aby włączyć tryb User EXEC.

Rys. 3-5 Włączanie trybu User EXEC



- 3) Po wpisaniu polecenia **enable** wejdiesz w tryb Privileged EXEC. Domyślnie hasło nie jest wymagane. Możesz później ustawić hasło dla użytkowników, którzy chcą mieć dostęp do tego trybu.

Rys. 3-6 Włączanie trybu Privileged EXEC

```

Telnet 192.168.0.1
***** User Access Login *****
User:admin
Password:

Switch#2006-01-01 08:21:11,[User]/3/Login the CLI by admin on vty0 (192.168.0.200).

Switch>enable
Switch#_

```

Możesz teraz zarządzać przełącznikiem za pomocą poleceń CLI poprzez połączenie Telnet.

3.3 Logowanie przez SSH

Logowanie przez SSH obsługuje dwa tryby: Password Authentication Mode (uwierzytelnianie hasła) i Key Authentication Mode (uwierzytelnianie klucza). Wybór trybu zależy od określonych potrzeb i zastosowania:

- Password Authentication Mode: wymagane jest podanie nazwy użytkownika i hasła (domyślna wartość obu pól to: admin).
- Key Authentication Mode (zalecany): wymagane jest podanie klucza publicznego do przełącznika i klucza prywatnego do oprogramowania klienta (PuTTY). Klucz publiczny i klucz prywatny możesz wygenerować przez narzędzie PuTTY Key Generator.

Przed zalogowaniem się przez SSH postępuj zgodnie z krokami przedstawionymi poniżej w celu włączenia SSH w emulatorze terminala:

Rys. 3-7 Włączanie SSH

```

Telnet 192.168.0.1
***** User Access Login *****
User:admin
Password:

Switch#2006-01-01 08:10:29,[User]/3/Login the CLI by admin on vty0 (192.168.0.200).

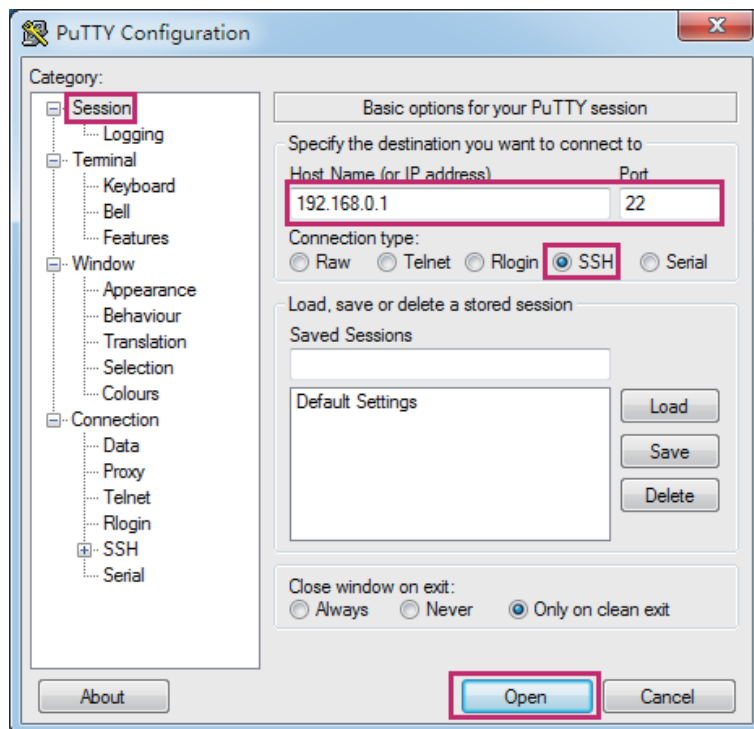
Switch>enable
Switch#config
Switch(config)#ip ssh server ← Enable SSH Function
Switch(config)#_

```

Password Authentication Mode

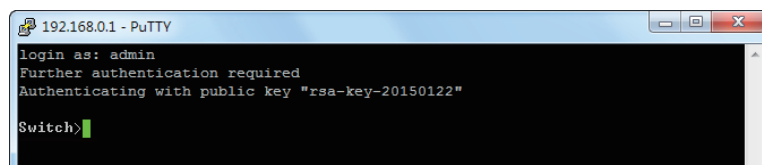
- 1) Uruchom PuTTY i przejdź do strony Session. Wpisz adres IP przełącznika w polu **Host Name** i pozostaw domyślną wartość 22 w polu **Port**; w rubryce Connection type wybierz **SSH**. Kliknij **Open**.

Rys. 3-8 Konfiguracja w PuTTY



- 2) Wpisz nazwę użytkownika i hasło, aby zalogować się do przełącznika, a następnie kontynuuj konfigurację przełącznika.

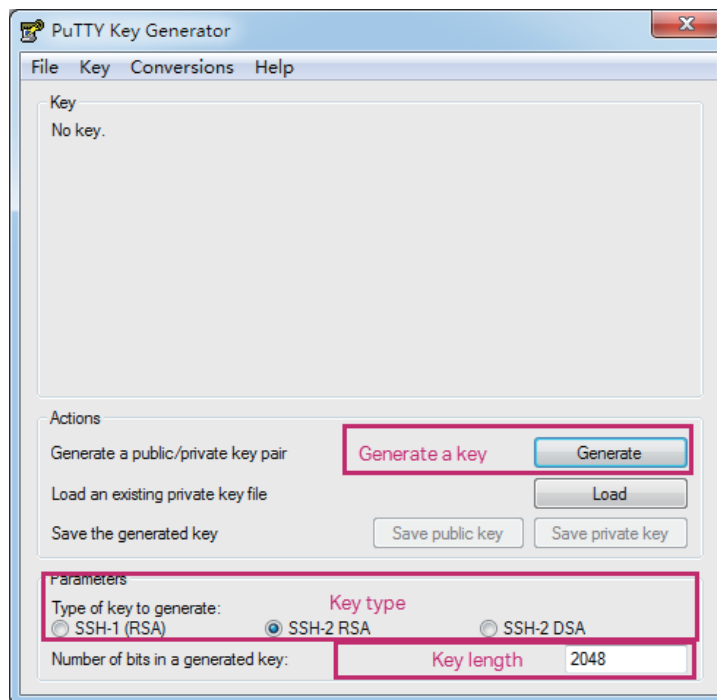
Rys. 3-9 Logowanie do przełącznika



Key Authentication Mode

- 1) Uruchom narzędzie PuTTY Key Generator. W sekcji **Parameters** wybierz typ klucza i wpisz długość klucza. W sekcji **Actions** kliknij **Generate**, aby wygenerować publiczny/prywatny zestaw dwóch kluczy. Na poniższym rysunku wygenerowano zestaw kluczy SSH-2 RSA, a każdy z kluczy ma długość 1024 bitów.

Rys. 3-10 Generowanie publicznego/prywatnego zestawu dwóch kluczy



Uwaga:

- Długość klucza powinna wynosić od 512 do 3072 bitów.
- Możesz przyspieszyć proces generowania klucza poprzez szybkie i przypadkowe ruchy myszką w sekcji Key.

- 2) Po wygenerowaniu kluczy kliknij **Save public key**, aby zapisać klucz publiczny na serwerze TFTP; kliknij **Save private key**, aby zapisać klucz prywatny na hoście.

Rys. 3-11 Zapisywanie wygenerowanych kluczy



- 3) W narzędziu HyperTerminal pobierz z serwera TFTP na przełącznik plik z kluczem publicznym, jak pokazano poniżej:

Rys. 3-12 Pobieranie klucza publicznego na przełącznik

```

Telnet 192.168.0.1
***** User Access Login *****
User:admin
Password:
#2006-01-27 08:06:01, [User1/5/Login the CLI by admin on vty0 (192.168.0.200)].

Switch>enable
Switch#configure
Switch(config)#ip ssh download v2 public ip-address 192.168.0.100
Start to download SSH key file.....
Download SSH key file OK.
Switch(config)

```

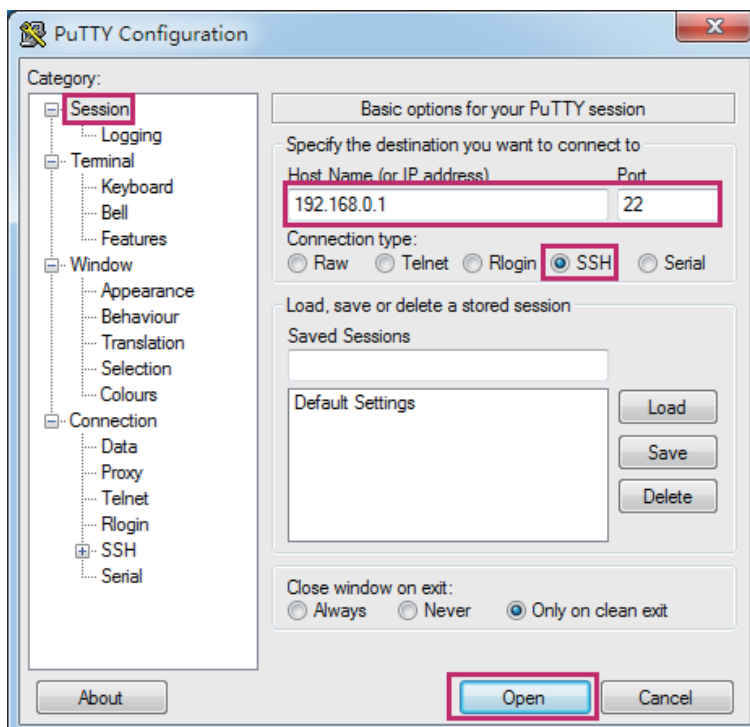
The filename of the public key The IP address of the TFTP server

Uwaga:

- Typ klucza powinien być zgodny z typem pliku klucza. W powyższym CLI v1 odpowiada SSH-1 (RSA), a v2 odpowiada SSH-2 RSA oraz SSH-2 DSA.
- Nie można przerywać procesu pobierania klucza.

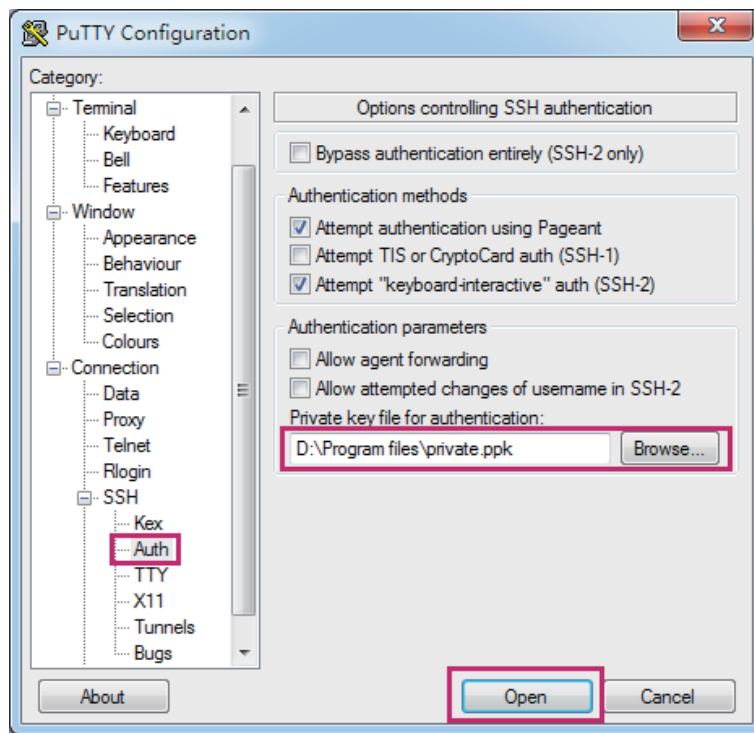
- 4) Po pobraniu klucza publicznego uruchom PuTTY i przejdź do strony **Session**. Wpisz adres IP przełącznika i w rubryce Connection type wybierz **SSH** (w polu Port pozostaw wartość domyślną).

Rys. 3-13 Konfiguracja nazwy hosta i typu połączenia



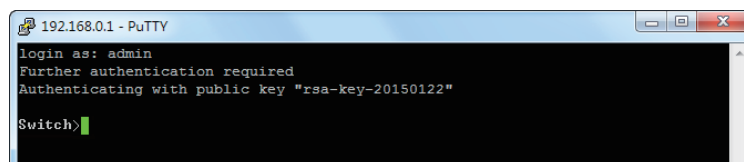
- 5) Przejdź do **Connection > SSH > Auth**. Kliknij **Browse**, aby pobrać plik z kluczem prywatnym do PuTTY. Kliknij **Open**, aby rozpocząć połączenie i negocjację.

Rys, 3-14 Pobieranie klucza prywatnego do PuTTY



- 6) Po zakończeniu negocjacji wpisz nazwę użytkownika, aby się zalogować. Jeśli możliwe jest zalogowanie się bez wpisywania hasła, oznacza to, że uwierzytelnianie klucza powiodło się.

Rys. 3-15 Logowanie do przełącznika



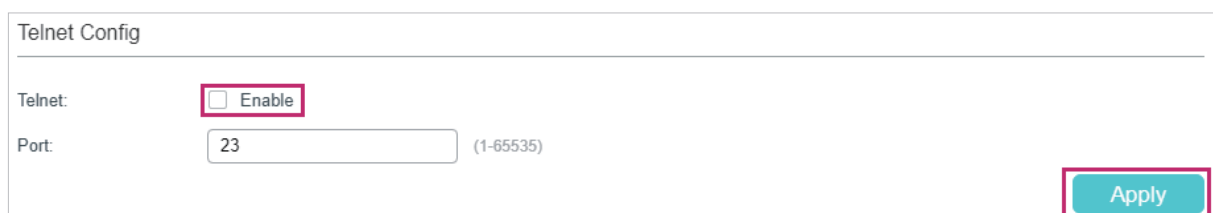
3.4 Wyłączenie logowania przez Telnet

Aby zablokować dostęp przez Telnet do interfejsu CLI, możesz wyłączyć funkcję Telnet.

- Przez GUI:

Wybierz **SECURITY > Access Security > Telnet Config**, wyłącz funkcję Telnet i kliknij **Apply**.

Rys, 3-16 Wyłączenie logowania przez Telnet



- Przez CLI:

Switch#configure

Switch(config)#telnet disable

3.5 Wyłączanie logowania przez SSH

Aby zablokować dostęp przez SSH do interfejsu CLI, możesz wyłączyć serwer SSH.

- Przez GUI:

Wybierz **SECURITY > Access Security > SSH Config**, wyłącz serwer SSH i kliknij **Apply**.

Rys. 3-1 Wyłączanie serwera SSH

Global Config

SSH:	<input type="checkbox"/> Enable	
Protocol V1:	<input checked="" type="checkbox"/> Enable	
Protocol V2:	<input checked="" type="checkbox"/> Enable	
Idle Timeout:	<input type="text" value="120"/>	seconds (1-120)
Maximum Connections:	<input type="text" value="5"/>	(1-5)
Port:	<input type="text" value="22"/>	(1-65535)

Apply

- Przez CLI:

Switch#configure

Switch(config)#no ip ssh server

3.6 Polecenie copy running-config startup-config

Pliki konfiguracyjne przełącznika dzielą się na dwa typy - plik bieżącej konfiguracji i plik konfiguracji startowej.

Po wpisaniu każdej linii poleceń zmiany zostaną zapisane w pliku bieżącej konfiguracji. Po restarcie przełącznika konfiguracje zostaną utracone.

Chcąc zachować konfigurację po restarcie przełącznika należy użyć polecenia **copy running-config startup-config**, a konfiguracja zostanie zapisana w pliku konfiguracji startowej.

Switch(config)#end

Switch#copy running-config startup-config

3.7 Zmiana adresu IP i bramy domyślnej przełącznika

Jeżeli chcesz uzyskać dostęp do przełącznika, możesz ustawić adres IP przełącznika. Jeżeli chcesz, żeby przełącznik miał dostęp do sieci, możesz skonfigurować bramę domyślną

urządzenia. Tylko komputery w sieci zarządzającej VLAN mają dostęp do interfejsu zarządzania przełącznikiem. Domyślnie wszystkie porty w sieci zarządzającej VLAN należą do VLAN 1, możesz więc połączyć się z przełącznikiem przez każdy port. Domyślny adres IP to **192.168.0.1**. Przełącznik nie ma bramy domyślnej. Poniższy przykład prezentuje ustawianie adresu IP przełącznika jako **192.168.0.10/24** i konfigurację bramy domyślnej jako **192.168.0.100**.

```
Switch#configure
```

```
Switch(config)#interface vlan 1
```

```
Switch(config-if)#ip address 192.168.0.10 255.255.255.0 gateway 192.168.0.100
```

Połączenie zostanie zerwane. Należy wtedy połączyć się przez Telnet z nowym adresem IP przełącznika: **192.168.0.10**.

```
C:\Users\Administrator>telnet 192.168.0.10
```

```
User: admin
```

```
Password: admin
```

```
Switch>enable
```

```
Switch#copy running-config startup-config
```

Część 2

Zarządzanie systemem

ROZDZIAŁY

1. System
2. Konfiguracja informacji systemowych
3. Zarządzanie kontami użytkowników
4. Konfiguracja narzędzi systemowych
5. Konfiguracja EEE
6. Konfiguracja szablonów SDM
7. Konfiguracja przedziałów czasowych

1 System

1.1 Informacje ogólne

W sekcji System można przeglądać informacje systemowe, a także konfigurować parametry i funkcje systemowe przełącznika.

1.2 Obsługiwane funkcje

Informacje systemowe

Na bieżąco sprawdzaj stan portów przełącznika, przeglądaj informacje systemowe, konfiguruj opisy urządzeń, czas systemowy, czas letni oraz systemowy adres IP/IPv6.

Zarządzanie kontami użytkowników

Zarządzaj kontami użytkowników logujących się do przełącznika. Do wyboru są różne typy użytkowników oraz różne poziomy dostępu dla kont. Dostosuj te ustawienia do swoich potrzeb.

Narzędzia systemowe

Skorzystaj z możliwości konfiguracji pliku startowego przełącznika, tworzenia kopii zapasowej ustawień i przywracania ich z pliku, aktualizacji firmware'u urządzenia, a także resetu lub restartu przełącznika.

EEE

EEE (Energy Efficient Ethernet) to technologia ograniczania zużycia energii przez przełączniki w okresach niskiego przepływu danych. Aby uruchomić oszczędzanie energii, włącz tę funkcję dla wybranych portów.

Szablon SDM

Szablon SDM (Switch Database Management) służy priorytetyzacji zasobów sprzętowych dla określonych funkcji. Przełącznik zapewnia trzy szablony, które przydzielają różnym zastosowaniom określone zasoby sprzętowe.

Przedział czasowy

Funkcja umożliwia konfigurację przedziałów czasowych oraz powiązanie ich z regułami ACL.

2 Konfiguracja informacji systemowych

Dostęp do ustawień systemowych umożliwia:

- podgląd najważniejszych ustawień systemowych;
- zmianę opisu urządzenia;
- zmianę czasu systemowego;
- konfigurację czasu letniego;
- konfigurację systemowych parametrów adresu IP;
- konfigurację systemowych parametrów adresu IPv6.

2.1 Przez GUI

2.1.1 Podgląd najważniejszych ustawień systemowych

Aby uzyskać podgląd informacji systemowych, wybierz **SYSTEM > System Info > System Summary**. Tutaj znajdziesz informacje o stanie portów oraz ustawieniach systemowych przełącznika.

Podgląd stanu portów

W sekcji **Port Status** możesz śledzić stan oraz poziom wykorzystania przepustowości łącza dla każdego portu przełącznika.

Rys. 2-1 Podgląd informacji systemowych



Poniższa tabela wyjaśnia znaczenie możliwych stanów portów

Stan portu	Wyjaśnienie
	Dany port 1000 Mb/s nie jest połączony z urządzeniem.
	Dany port 1000 Mb/s działa z prędkością 1000 Mb/s..
	Dany port 1000Mb/s działa z prędkością 10 Mb/s lub 100Mb/s.
	Dany port SFP nie jest połączony z urządzeniem.



Dany port SFP działa z prędkością 1000 Mb/s.



Dany port SFP działa z prędkością 100 Mb/s.

Aby uzyskać szczegółowe informacje o danym porcie, najedź na niego kursorem.

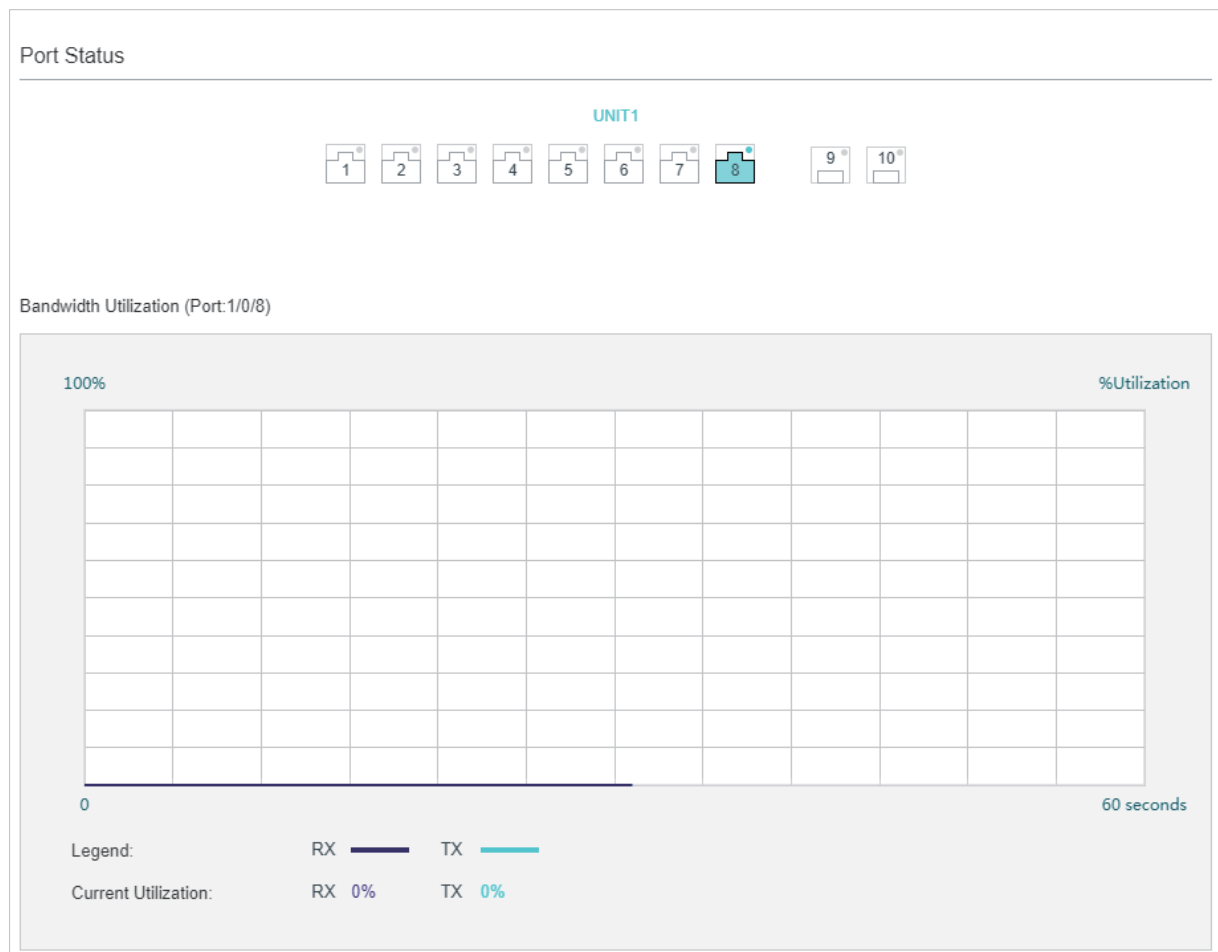
Rys. 2-2 Informacje o porcie

Port: 1/0/4	
Type:	Auto RJ45
Speed:	1000M, Full Duplex
Status:	Link Up

Informacje o porcie	Wyjaśnienie
Port	Numer portu.
Type	Typ portu
Speed	Maksymalna prędkość transmisji i tryb duplexu portu
Status	Stan połączenia portu

Gdy klikniesz określony port, pojawi się informacja o wykorzystywanej przepustowości łącza.

Rys. 2-3 Wykorzystywana przepustowość łącza



RX Wykorzystywana przepustowość łącza przez pakiety odbierane na danym porcie.

TX Wykorzystywana przepustowość łącza przez pakiety wysyłane na danym porcie.

Podgląd informacji systemowych

W sekcji **System Info** możesz uzyskać informacje systemowe przełącznika.

Rys. 2-4 Informacje systemowe

System Info	
UNIT1	
System Description:	JetStream 8-Port Gigabit L2 Managed Switch with 2 SFP Slots
Device Name:	T2500G-10TS
Device Location:	SHENZHEN
Contact Information:	www.tp-link.com
Hardware Version:	T2500G-10TS 2.0
Firmware Version:	2.0.0 Build 20181022 Rel.38882(s)
Boot Loader Version:	TP-LINK BOOTUTIL(v1.0.0)
MAC Address:	00-0D-EB-13-A2-98
System Time:	2006-01-01 08:16:37
Running Time:	0 day - 0 hour - 16 min - 56 sec
Serial Number:	
Jumbo Frame:	Disabled Settings
SNTP:	Disabled Settings
IGMP Snooping:	Disabled Settings
SNMP:	Disabled Settings
Spanning Tree:	Disabled Settings
DHCP Relay:	Disabled Settings
802.1X:	Disabled Settings
HTTP Server:	Enabled Settings
Telnet:	Enabled Settings
SSH:	Disabled Settings

System Description	Opis systemowy przełącznika.
Device Name	Nazwa przełącznika. Możesz ją edytować na stronie Device Description.
Device Location	Lokalizacja przełącznika. Możesz ją edytować na stronie Device Description.
Contact Information	Informacje kontaktowe dla przełącznika. Możesz je edytować na stronie Device Description.
Hardware Version	Wersja sprzętowa przełącznika.
Firmware Version	Wersja firmware'u przełącznika.
Boot Loader Version	Wersja programu rozruchowego przełącznika.
MAC Address	Adres MAC przełącznika.
System Time	Czas systemowy przełącznika.

Running Time	Czas pracy przełącznika.
Serial Number	Numer seryjny przełącznika.
Jumbo Frame	Informacja o stanie ramki Jumbo (włączona/wyłączona). Po kliknięciu Settings przejdziesz do strony konfiguracyjnej ramki Jumbo.
SNTP	Informacja o miejscu pobierania czasu systemowego (Serwer NTP). Po kliknięciu Settings przejdziesz do strony konfiguracyjnej czasu systemowego.
IGMP Snooping	Informacje o stanie usługi IGMP Snooping (włączona/wyłączona). Po kliknięciu Settings przejdziesz do strony konfiguracyjnej IGMP Snooping.
SNMP	Informacja o stanie usługi SNMP (włączona/wyłączona). Po kliknięciu Settings przejdziesz do strony konfiguracyjnej SNMP.
Spanning Tree	Informacja o stanie usługi Spanning Tree (włączona/wyłączona). Po kliknięciu Settings przejdziesz do strony konfiguracyjnej Spanning Tree.
DHCP Relay	Informacja o stanie usługi DHCP Relay (włączona/wyłączona). Po kliknięciu Settings przejdziesz do strony konfiguracyjnej DHCP Relay.
802.1x	Informacja o dostępności standardu 802.1x. Po kliknięciu Settings przejdziesz do strony konfiguracyjnej standardu..
HTTP Server	Informacja o stanie serwera HTTP (włączony/wyłączony). Po kliknięciu Settings przejdziesz do strony konfiguracyjnej serwera HTTP.
Telnet	Informacja o stanie usługi Telnet (włączona/wyłączona). Po kliknięciu Settings przejdziesz do strony konfiguracyjnej Telnet.
SSH	Informacja o stanie szyfrowania SSH (włączone/wyłączone). Po kliknięciu Settings przejdziesz do strony konfiguracyjnej SSH.

2.1.2 Zmiana opisu urządzenia

Wybierz z menu **SYSTEM > System Info > Device Description**, aby otworzyć poniższą stronę.

Rys. 2-5 Zmiana opisu urządzenia

Device Description

Device Name: (1-32 characters)

Device Location: (1-32 characters)

System Contact: (1-32 characters)

[Apply](#)

1) W sekcji **Device Description** skonfiguruj poniższe parametry.

Device Name	Wpisz nazwę przełącznika.
-------------	---------------------------

Device Location Określ lokalizację przełącznika.

System Contact Wprowadź informacje kontaktowe.

2) Kliknij **Apply**.

2.1.3 Konfiguracja czasu systemowego

Wybierz z menu **SYSTEM > System Info > System Time**, aby otworzyć poniższą stronę.

Rys. 2-6 Zmiana czasu systemowego

Time Info

Current System Time: Sunday, January 1, 2006 11:06:23
 Current Time Source: NTP Server

Time Config

Configure Manually Get Time from NTP Server Synchronize with PC's Clock

Time Zone: (GMT+08:00) Beijing, Urumqi, Hong Kong, Taipei ▼

Primary NTP Server: (Format: 192.168.0.1 or 2001::1)

Secondary NTP Server: (Format: 192.168.0.1 or 2001::1)

Update Rate: hours (1-24)

Apply

W sekcji **Time Info** uzyskasz informacje o aktualnym czasie przełącznika.

Current System Time Aktualna data i czas przełącznika.

Current Time Source Informacja o sposobie pobierania czasu przez przełącznik.

Aby skonfigurować czas systemowy, wykonaj poniższe kroki w sekcji **Time Config**:

1) Wybierz jedną metodę pobierania czasu systemowego i uzupełnij odpowiednie parametry.

Manual Ustaw czas systemowy ręcznie.

Date: Wprowadź datę systemową.

Time: Wprowadź czas systemowy.

Get Time from NTP Server

Pobierz czas systemowy z serwera czasu. Upewnij się, że serwer NTP jest dostępny w twojej sieci. Jeżeli chcesz skorzystać z serwera NTP poprzez łącze internetowe, upewnij się najpierw, że przełącznik jest połączony z Internetem.

Time Zone: Wybierz swoją strefę czasową.

Primary Server: Wprowadź adres IP preferowanego serwera czasu.

Secondary Server: Wprowadź adres IP alternatywnego serwera czasu. Gdy preferowany serwer czasu nie będzie dostępny, urządzenie może pobrać czas z alternatywnego serwera.

Update Rate: Określ częstotliwość pobierania czasu z serwera NTP (od 1 do 24 godzin).

Synchronize with PC's Clock

Zsynchronizuj czas systemowy z zegarem aktualnie zalogowanego hosta..

2) Kliknij **Apply**.

2.1.4 Konfiguracja czasu letniego

Wybierz z menu **SYSTEM > System Info > Daylight Saving Time**, aby otworzyć poniższą stronę.

Rys. 2-7 Konfiguracja czasu letniego

Aby skonfigurować czas letni, wykonaj poniższe kroki:

- 1) W sekcji **DST Config** włącz funkcję czasu letniego.
- 2) Wybierz metodę ustawiania czasu letniego i uzupełnij odpowiednie parametry.

Predefined Mode

Jeżeli wybierzesz **Predefined Mode**, wybierz skonfigurowany wcześniej harmonogram czasu letniego dla przełącznika.

USA: Czas letni w USA. Trwa od godziny 2:00 drugiej niedzieli marca do godziny 2:00 pierwszej niedzieli listopada.

Australia: Czas letni w Australii. Trwa od godziny 2:00 pierwszej niedzieli października do 3:00 pierwszej niedzieli kwietnia.

Europe: Czas letni w Europie. Trwa od godziny 1:00 ostatniej niedzieli marca do godziny 1:00 ostatniej niedzieli października.

New Zealand: Czas letni w Nowej Zelandii. Trwa od godziny 2:00 ostatniej niedzieli września do godziny 3:00 pierwszej niedzieli kwietnia.

Recurring Mode Jeżeli wybierzesz **Recurring Mode**, określ cykl czasu letniego dla przełącznika. Te ustawienia będą obowiązywać także w kolejnych latach.

Offset: Określ wartość przesunięcia zegara do przodu.

Start Time: Określ termin początkowy dla czasu letniego. Odstęp pomiędzy terminem początkowym a końcowym powinien być dłuży niż 1 dzień, ale krótszy niż 1 rok (365 dni).

End Time: Określ termin końcowy czasu letniego. Odstęp pomiędzy terminem początkowym a końcowym powinien być dłuży niż 1 dzień, ale krótszy niż 1 rok (365 dni).

Date Mode Jeżeli wybierzesz **Date Mode**, określ całkowity okres czasu letniego dla przełącznika. Te ustawienia będą obowiązywać tylko jednorazowo.

Offset: Określ wartość przesunięcia zegara do przodu.

Start Time: Określ termin początkowy dla czasu letniego. Odstęp pomiędzy terminem początkowym a końcowym powinien być dłuży niż 1 dzień, ale krótszy niż 1 rok (365 dni).

End Time: Określ termin końcowy czasu letniego. Odstęp pomiędzy terminem początkowym a końcowym powinien być dłuży niż 1 dzień, ale krótszy niż 1 rok (365 dni).

3) Kliknij **Apply**.

2.1.5 Konfiguracja systemowych parametrów adresu IP

Wybierz z menu **SYSTEM > System Info > System IP**, aby wyświetlić poniższą stronę.

Rys. 2-8 Konfiguracja parametrów systemowych adresu IP

System IP Config

MAC Address: 00-0A-EB-13-A2-11

Management VLAN ID: (1-4094)

IP Address Mode: Static DHCP BOOTP

IP Address: (Format: 192.168.0.1)

Subnet Mask: (Format: 255.255.255.0)

Default Gateway: (Format: 192.168.0.1)

[Apply](#)

Aby skonfigurować parametry systemowe adresu IP, wykonaj poniższe kroki:

1) Skonfiguruj odpowiednie parametry systemowe adresu IP

Management VLAN ID Określ sieć VLAN dla swojego przełącznika. Do interfejsu zarządzania przełącznikiem dostęp będą mogły uzyskać jedynie komputery korzystające z tej sieci VLAN. Domyślnie wybraną siecią jest VLAN 1, która obejmuje wszystkie porty, dlatego dostęp do przełącznika można uzyskać korzystając z dowolnego portu.

IP Address Mode	Wybierz tryb przydzielania adresów IP dla interfejsu. Static: Przydzielanie statycznego adresu IP dla interfejsu zarządzania. DHCP: Przydzielanie adresu IP dla interfejsu zarządzania poprzez serwer DHCP. BOOTP: Przydzielanie adresu IP dla interfejsu zarządzania poprzez serwer BOOTP.
DHCP Option 12	Jeżeli wybrałeś przydzielanie adresu IP w trybie DHCP, skonfiguruj tę opcję. DHCP Option 12 służy do określania nazwy klienta.
IP Address	Wprowadź adres IP interfejsu zarządzania, jeżeli wybrałeś przydzielanie adresu IP w trybie Static.
Subnet Mask	Wprowadź maskę podsieci interfejsu zarządzania, jeżeli wybrałeś przydzielanie adresu IP w trybie Static.
Default Gateway	Wprowadź bramę domyślną interfejsu zarządzania, jeżeli wybrałeś przydzielanie adresu IP w trybie Static. Brama domyślna to adres IP, na który pakiet zostanie następnie przesłany.

2) Kliknij **Apply**.

2.1.6 Konfiguracja systemowych parametrów adresu IPv6

Wybierz z menu **SYSTEM > System Info > System IPv6**, aby wyświetlić poniższą stronę.

Rys. 2-9 Konfiguracja systemowych parametrów adresu IPv6

System IPv6 Config

Management VLAN ID: VLAN1

IPv6 Enable: Enable

Link-local Address Mode: Manual Auto

Link-local Address: (Format: fe80::1)

Status: Normal

Enable global address auto configuration via RA message

Enable global address auto configuration via DHCPv6 Server

Apply

Global Address Config

+ Add - Delete

	Index	Global Address	Prefix Length	Type	Preferred Lifetime	Valid Lifetime	Status
No entries in this table.							
Total: 0							

1) W sekcji **System IPv6 Config** włącz funkcję IPv6 dla interfejsu i skonfiguruj odpowiednie parametry. Następnie kliknij **Apply**.

Management VLAN ID	Sieć VLAN przełącznika. Do interfejsu zarządzania przełącznikiem dostęp będą mogły uzyskać jedynie komputery korzystające z tej sieci VLAN. Domyślnie wybraną siecią jest VLAN 1, która obejmuje wszystkie porty, dlatego dostęp do przełącznika można uzyskać korzystając z dowolnego portu.
IPv6 Enable	Włącz funkcję IPv6 w interfejsie zarządzania.
Link-local Address Mode	Wybierz tryb konfiguracji adresu lokalnego dla łącza. Manual: Ten tryb umożliwia ręczny przydział adresu lokalnego dla łącza. Auto: W tym trybie przełącznik automatycznie generuje adres lokalny dla łącza.
Link-local Address	Jeżeli wybierzesz tryb "Manual", wprowadź adres lokalny dla łącza.
Status	Stan adresu lokalnego dla łącza. Nie można korzystać z adresu IPv6, który nie przeszedł kontroli DAD. Duplicate Address Detection służy wykrywaniu konfliktów adresów. Podczas kontroli DAD adres IPv6 może otrzymać trzy różne statusy: Normal: Adres lokalny dla łącza przeszedł kontrolę DAD i można z niego korzystać. Try: Adres lokalny dla łącza jest w trakcie kontroli DAD i nie można z niego aktualnie korzystać. Repeat: Adres lokalny dla łącza został uznany za duplikat, co oznacza, że jest już używany przez inny węzeł i nie można z niego korzystać.

- 2) Skonfiguruj globalny adres IPv6 interfejsu, wybierając jeden z poniższych sposobów:


Poprzez komunikat RA:

Enable global address auto configuration via RA message	Wybranie tej opcji umożliwi automatyczne wygenerowanie adresu globalnego i innych informacji przez interfejs, zgodnie z prefiksem adresu i innymi parametrami konfiguracji otrzymanymi w komunikacie RA (Router Advertisement).
---	---

Poprzez serwer DHCPv6:

Enable global address auto configuration via DHCPv6 Server	Wybranie tej opcji umożliwi przełącznikowi pobranie adresu globalnego z serwera DHCPv6.
--	---

Ręcznie:

W sekcji **Global Address Config** kliknij  **Add**, aby ręcznie przydzielić globalny adres IPv6 do interfejsu.

Global Address

Address Format: EUI-64 Not EUI-64

Global Address: (Format:3001::1)

Prefix Length: (1-64)

Address Format	Wybierz format adresu globalnego zgodnie ze swoimi potrzebami. EUI-64: Oznacza, że musisz podać tylko prefiks adresu, a system automatycznie utworzy adres globalny. Not EUI-64: Oznacza, że musisz podać stały adres globalny.
Global Address	Jeżeli wybierzesz format EUI-64, wprowadź tutaj prefiks adresu. W innym wypadku wprowadź tutaj stały adres IPv6.
Prefix Length	Skonfiguruj długość prefiksu adresu globalnego.

3) Przeglądaj parametry globalnego adresu w sekcji **Global Address Config**.

Global Address	Sprawdź lub edytuj adres globalny.
Prefix Length	Sprawdź lub edytuj długość prefiksu adresu globalnego.
Type	Tryb konfiguracji adresu globalnego. Manual: Oznacza, że dany adres został skonfigurowany ręcznie. Auto: Oznacza, że dany adres został utworzony automatycznie, na podstawie wiadomości RA, lub został pobrany z serwera DHCPv6.
Preferred Lifetime	Okres ważności preferowania adresu globalnego. Preferred lifetime to okres preferowania ważnego adresu IPv6. Po upłygnięciu tego okresu adres staje się przestarzały, ale nadal można z niego korzystać. Aby jednak urządzenie mogło nawiązać nowe połączenie, konieczna jest zmiana adresu.
Valid Lifetime	Okres ważność adresu globalnego. Valid lifetime to okres ważności adresu IPv6. Po upłygnięciu tego okresu adres wygasa i nie można już z niego korzystać.

Status	<p>Stan adresu lokalnego dla łącza. Nie można korzystać z adresu IPv6, który nie przeszedł kontroli DAD. Duplicate Address Detection służy wykrywaniu konfliktów adresów. Podczas kontroli DAD adres IPv6 może otrzymać trzy różne statusy:</p> <p>Normal: Adres lokalny dla łącza przeszedł kontrolę DAD i można z niego korzystać.</p> <p>Try: Adres lokalny dla łącza jest w trakcie kontroli DAD i nie można z niego aktualnie korzystać.</p> <p>Repeat: Adres lokalny dla łącza został uznany za duplikat, co oznacza, że jest już używany przez inny węzeł i nie można z niego korzystać.</p>
--------	--

2.2 Przez CLI

2.2.1 Podgląd najważniejszych informacji systemowych

Aby uzyskać podgląd informacji systemowych przełącznika w trybie privileged EXEC lub w innym trybie konfiguracji, można skorzystać z poniższych poleceń:

```
show interface status [ fastEthernet port | gigabitEthernet port | ten-gigabitEthernet port ]
```

Wyświetla stan interfejsu.

port: Wprowadź numer portu Ethernet.

```
show system-info
```

Wyświetla informacje systemowe, w tym opis systemowy, nazwę urządzenia, lokalizację urządzenia, informacje kontaktowe, wersję sprzętową, wersję firmware'u, czas systemowy, czas działania itd..

Poniższy przykład przedstawia sposób, w jaki można sprawdzić stan interfejsu i uzyskać dostęp do informacji systemowych przełącznika.

```
Switch#show interface status
```

Port	Status	Speed	Duplex	FlowCtrl	Jumbo	Active-Medium
-----	-----	----	-----	-----	-----	-----
Gi1/0/1	LinkDown	N/A	N/A	N/A	Disable	Copper
Gi1/0/2	LinkDown	N/A	N/A	N/A	Disable	Copper
Gi1/0/3	LinkUp	1000M	Full	Disable	Disable	Copper
...						

```
Switch#show system-info
```

System Description - JetStream 8-Port Gigabit L2 Managed Switch with 2 SFP Slots

System Name - T2500G-10TS

System Location - SHENZHEN
Contact Information - www.tp-link.com
Hardware Version - T2500G-10TS 2.0
Software Version - 2.0.0 Build 20180926 Rel.42438(s)
Bootloader Version - TP-LINK BOOTUTIL(v1.0.0)
Mac Address - 00-0A-EB-13-23-A0
Serial Number -
System Time - 2017-12-12 11:23:32
Running Time - 1 day - 2 hour - 33 min - 42 sec

2.2.2 Zmiana opisu urządzenia

Wykonaj poniższe kroki, aby skonfigurować opis urządzenia.

Krok 1	configure Uruchom tryb konfiguracji globalnej.
Krok 2	hostname [<i>hostname</i>] Określ nazwę systemową przełącznika. <i>hostname</i> : Podaj nazwę urządzenia, wprowadzając od 1 do 32 znaków. Domyślną nazwą jest model przełącznika.
Krok 3	location [<i>location</i>] Określ lokalizację systemową przełącznika. <i>location</i> : Wprowadź lokalizację urządzenia. Pole może zawierać maksymalnie 32 znaki. Domyślną lokalizacją jest "SHENZHEN".
Krok 4	contact-info [<i>contact-info</i>] Podaj systemowe informacje kontaktowe. <i>contact-info</i> : Wprowadź informacje kontaktowe. Pole może zawierać maksymalnie 32 znaki. Domyślnie podany jest adres "www.tp-link.com".
Krok 5	show system-info Sprawdź informacje systemowe, w tym opis systemowy, nazwę urządzenia, lokalizację urządzenia, informacje kontaktowe, wersję sprzętową, wersję firmware'u, czas systemowy, czas działania itd.
Krok 6	end Powróć do trybu privileged EXEC.
Krok 7	copy running-config startup-config Zapisz ustawienia w pliku konfiguracyjnym.

Poniższy schemat przedstawia przykładową konfigurację parametrów, w tym ustawianie Switch_A jako nazwy urządzenia, BEIJING jako lokalizacji oraz http://www.tp-link.com jako informacji kontaktowej.

Switch#configure**Switch(config)#hostname** Switch_A**Switch(config)#location** BEIJING**Switch(config)#contact-info** http://www.tp-link.com**Switch(config)#show system-info**

System Description - JetStream 8-Port Gigabit L2 Managed Switch with 2 SFP Slots

System Name - Switch_A

System Location - BEIJING

Contact Information - http://www.tp-link.com

...

Switch(config)#end**Switch#copy running-config startup-config**

2.2.3 Konfiguracja czasu systemowego

Wykonaj poniższe kroki, aby skonfigurować czas systemowy:

 **Uwaga:**

Tryb Synchronize with PC's Clock nie może być obsługiwany za pomocą poleceń CLI.

Krok 1 configure

Uruchom tryb konfiguracji globalnej.

Krok 2 Skorzystaj z poniższego polecenia, aby ustawić czas systemowy ręcznie:

system-time manual time

Skonfiguruj czas systemowy ręcznie.

time: Ręcznie wprowadź datę i czas w formacie MM/DD/RRRR-GG:MM:SS. Poprawna wartość roku mieści się w przedziale 2000 - 2037.

Skorzystaj z poniższej komendy, aby ustawić czas systemowy poprzez pobranie go z serwera NTP. Upewnij się, że serwer NTP jest dostępny. Jeżeli serwer NTP wymaga połączenia internetowego, połącz najpierw przełącznik z Internetem.

system-time ntp { *timezone* } { *ntp-server* } { *backup-ntp-server* } { *fetching-rate* }

timezone: Określ swoją lokalną strefę czasową, wybierając z przedziału UTC-12:00 - UTC+13:00.

Poniższej znajdziesz informacje o poszczególnych strefach czasowych:

UTC-12:00 — Strefa czasowa zachodniej strony linii zmiany daty.

UTC-11:00 — Uniwersalny czas koordynowany-11.

UTC-10:00 — Strefa czasowa Hawajów.

UTC-09:00 — Strefa czasowa Alaski.

UTC-08:00 — Czas pacyficzny (US, Kanada).

UTC-07:00 — Czas górski (US, Kanada).

UTC-06:00 — Czas centralny (US, Kanada).

UTC-05:00 — Czas wschodni (US, Kanada).

UTC-04:30 — Strefa czasowa Caracas.

UTC-04:00 — Czas atlantycki (Kanada).

UTC-03:30 — Strefa czasowa Nowej Fundlandii.

UTC-03:00 — Strefa czasowa Buenos Aires, Salvadoru, Brasilii.

UTC-02:00 — Strefa czasowa Stanów Środkowoatlantyckich.

UTC-01:00 — Strefa czasowa Azorów i Republiki zielonego przylądka.

UTC — Strefa czasowa Dublinu, Edynburgu, Lizbony, Londynu.

UTC+01:00 — Strefa czasowa Amsterdamu, Berlina, Berna, Rzymu, Sztokholmu, Wiednia.

UTC+02:00 — Strefa czasowa Kairu, Aten, Bukaresztu, Ammanu, Bejrutu, Jerozolimy.

UTC+03:00 — Strefa czasowa Kuwejtu, Rijadu, Bagdadu.

UTC+03:30 — Strefa czasowa Teheranu.

UTC+04:00 — Strefa czasowa Moskwy, Petersburgu, Wołgogradu, Tbilisi, Portu Louis.

UTC+04:30 — Strefa czasowa Kabulu.

UTC+05:00 — Strefa czasowa Islamabadu, Karaczi, Taszkentu.

UTC+05:30 — Strefa czasowa Madrasu, Kalkuty, Bombaju, Nowego Delhi.
 UTC+05:45 — Strefa czasowa Katmandu.
 UTC+06:00 — Strefa czasowa Dhaki, Astany, Jekaterynburgu.
 UTC+06:30 — Strefa czasowa Rangun.
 UTC+07:00 — Strefa czasowa Nowosybirsk, Bangkoku, Hanoi, Dżakarty.
 UTC+08:00 — Strefa czasowa Pekinu, Chongqingu, Hongkongu, Urumczy, Singapuru.
 UTC+09:00 — Strefa czasowa Seulu, Irkucka, Osaki, Sapporo, Tokio.
 UTC+09:30 — Strefa czasowa Darwina, Adelaide.
 UTC+10:00 — Strefa czasowa Canberry, Melbourne, Sydney, Brisbane.
 UTC+11:00 — Strefa czasowa Wysp Salomona, Nowej Kaledonii, Władystoku.
 UTC+12:00 — Strefa czasowa Fidzi, Magadanu, Auckland, Wellington.
 UTC+13:00 — Strefa czasowa Nuku'alofa, Samoa.

ntp-server: Podaj adres IP preferowanego serwera NTP.

backup-ntp-server: Podaj adres IP alternatywnego serwera NTP.

fetching-rate: Określ interwał pobierania z serwera NTP.

Krok 3 Skorzystaj z poniższego polecenia, aby zweryfikować informacje o czasie systemowy.

show system-time

Sprawdź czas systemowy.

Skorzystaj z poniższego polecenia, aby zweryfikować informacje dotyczące ustawień trybu serwera NTP.

show system-time ntp

Sprawdź czas systemowy trybu NTP.

Krok 4 **end**
Powróć do trybu privileged EXEC.

Krok 5 **copy running-config startup-config**
Zapisz ustawienia w pliku konfiguracyjnym.

Poniższy schemat przedstawia przykładową konfigurację czasu systemowego za pomocą trybu pobierania czasu z serwera NTP, strefy czasowej jako UTC+08:00, serwera NTP jako 133.100.9.2, alternatywnego serwera NTP jako 139.78.100.163 oraz częstotliwości aktualizacji jako 11.

Switch#configure

Switch(config)#system-time ntp UTC+08:00 133.100.9.2 139.78.100.163 11

Switch(config)#show system-time ntp

Time zone : UTC+08:00

Preferred NTP server: 133.100.9.2

Backup NTP server: 139.78.100.163

Last successful NTP server: 133.100.9.2

Update Rate: 11 hour(s)

Switch(config)#end

Switch#copy running-config startup-config

2.2.4 Konfiguracja czasu letniego

Wykonaj poniższe kroki, aby skonfigurować czas letni:

Krok 1 **configure**

Uruchom tryb konfiguracji globalnej.

Krok 2 Skorzystaj z poniższego polecenia, aby wybrać gotową konfigurację czasu letniego:

system-time dst predefined [USA | Australia | Europe | New-Zealand]

Określ czas letni wybierając skonfigurowany wcześniej harmonogram.

USA | Australia | Europe | New-Zealand: Wybierz tryb czasu letniego.

USA: Od 02:00 drugiej niedzieli marca do 02:00 pierwszej niedzieli listopada.

Australia: Od 02:00 pierwszej niedzieli października do 03:00 pierwszej niedzieli kwietnia.

Europe: Od 01:00 ostatniej niedzieli marca do 01:00 ostatniej niedzieli października.

New Zealand: Od 02:00 ostatniej niedzieli września do 03:00 pierwszej niedzieli kwietnia.

Skorzystaj z poniższego polecenia, aby ustawić tryb cykliczny czasu letniego:

system-time dst recurring { sweek } { sday } { smonth } { stime } { eweek } { eday } { emonth } { etime } [offset]

Określ okres czasu letniego w trybie cyklicznym.

sweek: Podaj tydzień początku czasu letniego. Do wyboru jest 5 wartości: first, second, third, fourth, last (pierwszy, drugi, trzeci, czwarty, ostatni).

sday: Podaj dzień tygodnia początku czasu letniego. Do wyboru jest 7 dni tygodnia: Sun, Mon, Tue, Wed, Thu, Fri, Sat.

smonth: Podaj miesiąc początku czasu letniego. Do wyboru jest 12 miesięcy: Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, Dec.

stime: Podaj godzinę początku czasu letniego w formacie GG:MM.

ewweek: Podaj tydzień końca czasu letniego. Do wyboru jest 5 wartości: first, second, third, fourth, last (pierwszy, drugi, trzeci, czwarty, ostatni).

eday: Podaj dzień tygodnia końca czasu letniego. Do wyboru jest 7 dni tygodnia: Sun, Mon, Tue, Wed, Thu, Fri, Sat.

emonth: Podaj miesiąc końca czasu letniego. Do wyboru jest 12 miesięcy: Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, Dec.

etime: Podaj godzinę końca czasu letniego w formacie GG:MM.

offset: Podaj wartość przesunięcia zegara do przodu. Wartością domyślną jest 60.

Skorzystaj z poniższego polecenia, aby ustawić całkowity okres czasu letniego:

```
system-time dst date { smonth } { sday } { stime } { syear } { emonth } { eday } { etime } { eyear } [ offset ]
```

Określ czas letni, ustawiając jego całkowity okres.

smonth: Podaj miesiąc początku czasu letniego. Do wyboru jest 12 miesięcy: Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, Dec.

sday: Podaj datę początku czasu letniego, wybierając wartość z przedziału 1 - 31.

stime: Podaj godzinę początku czasu letniego w formacie GG:MM.

syear: Podaj rok początkowy dla czasu letniego.

emonth: Podaj miesiąc końca czasu letniego. Do wyboru jest 12 miesięcy: Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, Dec.

eday: Podaj datę końca czasu letniego, wybierając wartość z przedziału 1 - 31.

etime: Podaj godzinę końca czasu letniego w formacie GG:MM.

eyear: Podaj rok końcowy dla czasu letniego.

offset: Podaj wartość przesunięcia zegara do przodu. Wartością domyślną jest 60.

Krok 3	show system-time dst Zweryfikuj informacje dotyczące czasu letniego przełącznika.
Krok 4	end Powróć do trybu privileged EXEC.
Krok 5	copy running-config startup-config Zapisz ustawienia w pliku konfiguracyjnym.

Poniższy schemat przedstawia przykładową konfigurację czasu letniego do Date Mode. Terminem początkowym będzie godzina 01:00 1 sierpnia 2017, a terminem końcowym godzina 01:00 1 września 2017, natomiast wartością przesunięcia 50.

Switch#configure

```
Switch(config)#system-time dst date Aug 1 01:00 2017 Sep 1 01:00 2017 50
```

Switch(config)#show system-time dst

```
DST starts at 01:00:00 on Aug 1 2017
```

```
DST ends at 01:00:00 on Sep 1 2017
```

```
DST offset is 50 minutes
```

```
DST configuration is one-off
```

Switch(config)#end

Switch#copy running-config startup-config

2.2.5 Konfiguracja systemowych parametrów adresu IP

Wykonaj poniższe kroki, aby skonfigurować parametry systemowe adresu IP.

Krok 1	configure Uruchom tryb konfiguracji globalnej.
Krok 2	ip management-vlan { vlan-id } Skonfiguruj sieć VLAN przełącznika. Do interfejsu zarządzania przełącznikiem dostęp będą mogły uzyskać jedynie komputery korzystające z tej sieci VLAN.
Krok 3	interface vlan { vlan-id } Wybierz tryb Interface VLAN. <i>vlan-id</i> : ID sieci VLAN przełącznika.
Krok 4	Automatycznie przydziel adres IP i bramę domyślną interfejsowi zarządzania poprzez serwer DHCP lub BOOTP: ip address-alloc { dhcp bootp } Określ tryb przydziału adresu IP dla interfejsu zarządzania. <i>dhcp</i> : Określ interfejs zarządzania, aby pobrać adres IPv4 z serwera DHCP. <i>bootp</i> : Określ interfejs zarządzania, aby pobrać adres IPv4 z serwera BOOTP. Ręcznie przydziel adres IP i bramę domyślną interfejsowi zarządzania: ip address { ip-addr } { mask } gateway { default-gateway } Skonfiguruj ręcznie adres IP i bramę domyślną dla interfejsu zarządzania. <i>ip-addr</i> : Określ adres IP interfejsu zarządzania. <i>mask</i> : Określ maskę podsieci interfejsu zarządzania. <i>default gateway</i> : Wprowadź bramę domyślną interfejsu zarządzania, jeżeli wybrałeś przydzielanie adresu IP w trybie Static. Brama domyślna to adres IP, na który pakiet zostanie następnie przesłany.
Krok 5	show interface vlan { vlan-id } <i>vlan-id</i> : ID sieci VLAN przełącznika. Zweryfikuj najważniejsze informacje dotyczące interfejsu zarządzania.
Krok 6	end Powróć do trybu privileged EXEC.
Krok 7	copy running-config startup-config Zapisz ustawienia w pliku konfiguracyjnym.

Poniższy schemat przedstawia przykładową konfigurację adresu IP przełącznika jako **192.168.0.10/24** i bramy domyślnej jako **192.168.0.100**.

```
Switch#configure
```

```
Switch(config)#interface vlan 1
```

```
Switch(config-if)#ip address 192.168.0.10 255.255.255.0 gateway 192.168.0.100
```

Połączenie zostanie przerwane. Należy wtedy połączyć się przez Telnet z nowym adresem IP przełącznika: **192.168.0.10**.

```
C:\Users\Administrator>telnet 192.168.0.10
```

```
User:admin
```

```
Password:admin
```

```
Switch>enable
```

```
Switch#show interface vlan 1
```

```
Switch#copy running-config startup-config
```

2.2.6 Konfiguracja systemowych parametrów systemowych adresu IPv6

Wykonaj poniższe kroki, aby skonfigurować systemowe parametry adresu IPv6.

Krok 1	configure Uruchom tryb konfiguracji globalnej.
Krok 2	ip management-vlan { vlan-id} Skonfiguruj sieć VLAN przełącznika. Dostęp do interfejsu zarządzania przełącznikiem będą mogły uzyskać jedynie komputery korzystające z tej sieci VLAN.
Krok 3	interface vlan { vlan-id} Wybierz tryb Interface VLAN. <i>vlan-id</i> : ID sieci VLAN przełącznika.
Krok 4	ipv6 enable Włącz funkcję IPv6 w interfejsie zarządzania.
Krok 5	Skonfiguruj adres lokalny dla łącza IPv6 dla interfejsu zarządzania: Ręcznie skonfiguruj adres lokalny dla łącza IPv6 dla interfejsu zarządzania: ipv6 address ipv6-addr link-local <i>ipv6-addr</i> : Wprowadź adres lokalny dla łącza. Powinien to być standardowy adres IPv6 z prefiksem fe80::/10, w przeciwnym razie polecenie to będzie nieprawidłowe. Automatycznie skonfiguruj adres lokalny dla łącza IPv6 dla interfejsu zarządzania: ipv6 address autoconfig

Krok 6	Skonfiguruj globalny adres IPv6 dla interfejsu zarządzania:
	<p>Automatycznie skonfiguruj globalny adres IPv6 interfejsu za pomocą komunikatu RA: ipv6 address ra Skonfiguruj globalny adres IPv6 zgodnie z prefiksem adresu i innymi parametrami konfiguracji otrzymanymi w komunikacie RA (Router Advertisement).</p> <p>Automatycznie skonfiguruj globalny adres IPv6 interfejsu poprzez serwer DHCPv6: ipv6 address dhcp Włącz funkcję klienta DHCPv6. Gdy funkcja jest włączona, interfejs warstwy 3 podejmie próbę uzyskania adresu IPv6 z serwera DHCPv6.</p> <p>Ręcznie skonfiguruj globalny adres IPv6 interfejsu: ipv6 address ipv6-addr <i>ipv6-addr</i>: Globalny adres IPv6 z prefiksem sieci, np. 3ffe::1/64. ipv6 address ipv6-addr eui-64 Określ globalny adres IPv6 za pomocą extended unique identifier (EUI) w 64 bitach niższego rzędu adresu IPv6. Podaj tylko prefiks sieci; końcowe 64 bity są automatycznie obliczane z adresu MAC przełącznika. To umożliwia przetwarzanie IPv6 na poziomie interfejsu.</p>
Krok 7	show ipv6 interface Zweryfikuj skonfigurowane ustawienia IPv6.
Krok 8	end Powróć do trybu privileged EXEC.
Krok 9	copy running-config startup-config Zapisz ustawienia w pliku konfiguracyjnym.

Poniższy schemat przedstawia przykładowy sposób włączania funkcji IPv6 i konfiguracji parametrów IPv6 interfejsu zarządzania:

Switch#configure

Switch(config)#interface vlan 1

Switch(config-if)#ipv6 enable

Switch(config-if)#ipv6 address autoconfig

Switch(config-if)#ipv6 address dhcp

Switch(config-if)#show ipv6 interface

Vlan2 is up, line protocol is up

IPv6 is enable, Link-Local Address: fe80::20a:ebff:fe13:237b[NOR]

Global Address RA: Disable

Global Address DHCPv6: Enable

Global unicast address(es): ff02::1:ff13:237b

Joined group address(es): ff02::1

ICMP error messages limited to one every 1000 milliseconds

ICMP redirects are enable

MTU is 1500 bytes

ND DAD is enable, number of DAD attempts: 1

ND retrans timer is 1000 milliseconds

ND reachable time is 30000 milliseconds

Switch(config-if)#end

Switch#copy running-config startup-config

3 Zarządzanie kontami użytkowników

Dzięki funkcji zarządzania kontami możesz tworzyć i zarządzać kontami użytkowników logujących się do przełącznika.

3.1 Przez GUI

Do wyboru są cztery typy kont użytkowników, o różnych poziomach dostępu: Admin, Operator, Power User oraz User.

- Admin jest kontem domyślnym i nie można go usunąć. Domyślną nazwą użytkownika i hasłem dla tego konta jest admin. Możesz także tworzyć dodatkowe konta Admin.
- Jeżeli utworzysz konto Operator, Power User lub User, przejdź do sekcji AAA, aby utworzyć hasło dostępu. Te typy użytkowników mogą także korzystać z hasła dostępu, aby zmienić swój poziom dostępu i otrzymać uprawnienia administratora.

3.1.1 Tworzenie kont

Wybierz z menu **SYSTEM > User Management > User Config**, aby wyświetlić poniższą stronę.

Rys. 3-1 Strona konfiguracji kont użytkowników

<input type="checkbox"/>	User ID	Username	Access Level	Operation
<input type="checkbox"/>	1	admin	Admin	

Total: 1

Domyślnie w tabeli znajduje się konto Admin. Możesz kliknąć , aby edytować to konto, ale nie możesz go usunąć.

Utwórz nowe konto użytkownika. Kliknij , a pojawi się poniższe okno.

Rys. 3-2 Dodawanie konta

Wykonaj poniższe kroki, aby utworzyć nowe konto użytkownika.

1) Skonfiguruj poniższe parametry:

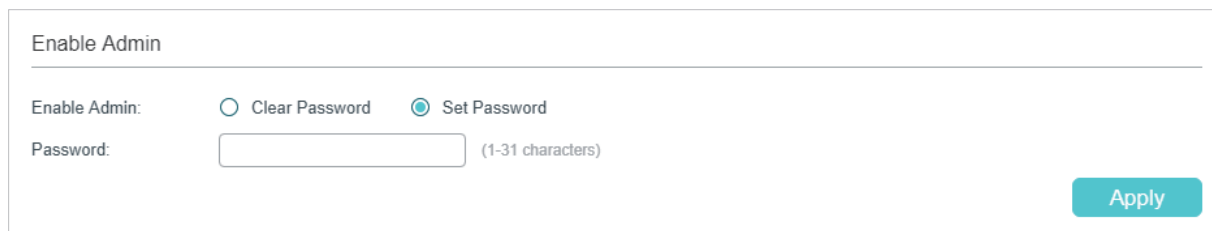
Username	Podaj nazwę użytkownika dla konta. Może ona zawierać maksymalnie 16 znaków, w tym cyfry, litery alfabetu angielskiego lub znaki podkreślenia.
Access Level	Wybierz poziom dostępu. Do wyboru są cztery opcje: Admin: Konto Admin może edytować, zmieniać i przeglądać wszystkie ustawienia funkcji. Operator: Konto Operator może edytować, zmieniać i przeglądać większość ustawień funkcji. Power User: Konto Power User może edytować, zmieniać i przeglądać tylko wybrane ustawienia funkcji. User: Konto User może tylko przeglądać ustawienia, bez możliwości ich edycji lub zmiany.
Password	Podaj hasło dla konta, wprowadzając od 1 do 31 znaków alfanumerycznych. Możesz korzystać z cyfr, liter alfabetu angielskiego (z uwzględnieniem ich wielkości), znaków podkreślenia i szesnastu znaków specjalnych. .
Confirm Password	Wprowadź ponownie hasło.

2) Kliknij **Create**.

3.1.2 Konfiguracja hasła dostępu

Wybierz z menu **SECURITY > AAA > Global Config**, aby wyświetlić poniższą stronę.

Rys. 3-3 Konfiguracja hasła dostępu



Enable Admin

Enable Admin: Clear Password Set Password

Password: (1-31 characters)

Apply

Wykonaj poniższe kroki, aby skonfigurować hasło dostępu:

- 1) Wybierz **Set Password** i wpisz hasło dostępu w polu **Password**.
- 2) Kliknij **Apply**.

Wskazówka:

Zalogowani użytkownicy mogą podać na tej stronie hasło dostępu, aby otrzymać uprawnienia administratora.

3.2 Przez CLI

Do wyboru są cztery typy kont użytkowników, o różnych poziomach dostępu: Admin, Operator, Power User oraz User.

- Admin jest kontem domyślnym i nie można go usunąć. Domyślną nazwą użytkownika i hasłem dla tego konta jest admin. Możesz także tworzyć dodatkowe konta Admin.
- Jeżeli utworzysz konto Operator, Power User lub User, przejdź do sekcji AAA, aby utworzyć hasło dostępu. Te typy użytkowników mogą także korzystać z hasła dostępu, aby zmienić swój poziom dostępu i otrzymać uprawnienia administratora.

3.2.1 Tworzenie kont

Wykonaj poniższe kroki, aby utworzyć konto:

-
- Krok 1 **configure**
- Uruchom tryb konfiguracji globalnej.
-

- Krok 2 Skorzystaj z poniższego polecenia, aby utworzyć konto nieszyfrowane lub szyfrowane symetrycznie.
- ```
user name name { privilege admin | operator | power_user | user } password { [0] password | 7 encrypted-password }
```
- name*: Podaj nazwę użytkownika, która posłuży za login do konta. Nazwa może zawierać maksymalnie 16 znaków, w tym cyfry, litery alfabetu angielskiego i znaki podkreślenia.
- admin | operator | power\_user | user**: Określ poziom dostępu dla użytkownika. Konto Admin może edytować, zmieniać i przeglądać wszystkie ustawienia funkcji. Konto Operator może edytować, zmieniać i przeglądać większość ustawień funkcji. Konto Power User może edytować, zmieniać i przeglądać tylko wybrane ustawienia funkcji. Konto User może tylko przeglądać ustawienia, bez możliwości ich edycji lub zmiany.
- 0: Wybierz typ szyfrowania. 0 oznacza, że podane hasło jest nieszyfrowane i w takiej formie zapisywane jest w pliku konfiguracyjnym. Domyślnie ustawioną wartością jest 0.
- password*: Podaj hasło potrzebne do logowania na konto. Hasło to ciąg od 1 do 32 znaków alfanumerycznych lub symboli, w tym cyfr, liter alfabetu angielskiego (z uwzględnieniem ich wielkości), znaków podkreślenia i szesnaście znaków specjalnych.
- 7: Wybierz typ szyfrowania. 7 oznacza, że hasło jest szyfrowane symetrycznie i w takiej formie zapisywane jest w pliku konfiguracyjnym.
- encrypted-password*: Wprowadź hasło szyfrowane symetrycznie o stałej długości, które możesz skopiować z pliku konfiguracyjnego innego przełącznika. Po skonfigurowaniu hasła szyfrowanego, użyj odpowiedniego hasła nieszyfrowanego, aby ponownie wejść w ten tryb.

Skorzystaj z poniższego polecenia, aby utworzyć konto szyfrowane algorytmem MD5.

```
user name name { privilege admin | operator | power_user | user } secret { [0] password | 5 encrypted-password }
```

Utwórz konto o poziomie dostępu Admin.

*name*: Podaj nazwę użytkownika, która posłuży za login do konta. Nazwa może zawierać maksymalnie 16 znaków, w tym cyfry, litery alfabetu angielskiego i znaków podkreślenia.

**admin | operator | power\_user | user**: Określ poziom dostępu dla użytkownika. Konto Admin może edytować, zmieniać i przeglądać wszystkie ustawienia funkcji. Konto Operator może edytować, zmieniać i przeglądać większość ustawień funkcji. Konto Power User może edytować, zmieniać i przeglądać tylko wybrane ustawienia funkcji. Konto User może tylko przeglądać ustawienia, bez możliwości ich edycji lub zmiany.

0: Wybierz typ szyfrowania. 0 oznacza, że podane hasło jest nieszyfrowane, ale hasło zapisane w pliku konfiguracyjnym ma szyfrowanie MD5. Domyślnie ustawioną wartością jest 0.

*password*: Podaj hasło potrzebne do logowania na konto. Hasło to ciąg od 1 do 32 znaków alfanumerycznych lub symboli, w tym cyfr, liter alfabetu angielskiego (z uwzględnieniem ich wielkości), znaków podkreślenia i szesnaście znaków specjalnych.

5: Wybierz typ szyfrowania. 5 oznacza, że hasło ma szyfrowanie MD5 i w takiej formie zapisywane jest w pliku konfiguracyjnym.

*encrypted-password*: Wprowadź hasło z szyfrowaniem MD5 o stałej długości, które możesz skopiować z pliku konfiguracyjnego innego przełącznika.

- Krok 3 **show user account-list**  
Zweryfikuj szczegóły utworzonych kont.

- Krok 4 **end**  
Powróć do trybu privileged EXEC.

---

Krok 5     **copy running-config startup-config**  
Zapisz ustawienia w pliku konfiguracyjnym.

---

### 3.2.2 Konfiguracja hasła dostępu

Wykonaj poniższe kroki, aby utworzyć konto innego typu:

---

Krok 1     **configure**  
Uruchom tryb konfiguracji globalnej..

---

Krok 2     **aaa enable**  
Włącz globalnie funkcję AAA.

---

Krok 3     Skorzystaj z poniższego polecenia, aby utworzyć hasło dostępu nieszyfrowane lub szyfrowane symetrycznie.

**enable admin password { [ 0 ] password | 7 encrypted-password }**

Utwórz hasło dostępu. Poziom dostępu użytkownika może zmienić się na Admin. Domyślnie to pole jest puste.

**0:** Wybierz typ szyfrowania. 0 oznacza, że podane hasło jest nieszyfrowane i w takiej formie zapisywane jest w pliku konfiguracyjnym. Domyślnie ustawioną wartością jest 0..

**password:** Podaj hasło dostępu. Hasło to ciąg od 1 do 32 znaków alfanumerycznych lub symboli, w tym cyfr, liter alfabetu angielskiego (z uwzględnieniem ich wielkości), znaków podkreślenia i szesnaście znaków specjalnych.

**7:** Wybierz typ szyfrowania. 7 oznacza, że hasło jest szyfrowane symetrycznie i w takiej formie zapisywane jest w pliku konfiguracyjnym.

**encrypted-password:** Wprowadź hasło szyfrowane symetrycznie o stałej długości, które możesz skopiować z pliku konfiguracyjnego innego przełącznika. Po skonfigurowaniu hasła szyfrowanego, użyj odpowiedniego hasła nieszyfrowanego, aby ponownie wejść w ten tryb.

Skorzystaj z poniższego polecenia, aby utworzyć hasło dostępu nieszyfrowane lub szyfrowane algorytmem MD5.

**enable admin secret { [ 0 ] password | 5 encrypted-password }**

Utwórz hasło dostępu. Poziom dostępu użytkownika może zmienić się na Admin. Domyślnie to pole jest puste.

**0:** Wybierz typ szyfrowania. 0 oznacza, że podane hasło jest nieszyfrowane, ale hasło zapisane w pliku konfiguracyjnym ma szyfrowanie MD5. Domyślnie ustawioną wartością jest 0.

**password:** Podaj hasło dostępu. Hasło to ciąg od 1 do 32 znaków alfanumerycznych lub symboli, w tym cyfr, liter alfabetu angielskiego (z uwzględnieniem ich wielkości), znaków podkreślenia i szesnaście znaków specjalnych.

**5:** Wybierz typ szyfrowania. 5 oznacza, że hasło ma szyfrowanie MD5 i w takiej formie zapisywane jest w pliku konfiguracyjnym.

**encrypted-password:** Wprowadź hasło z szyfrowaniem MD5 o stałej długości, które możesz skopiować z pliku konfiguracyjnego innego przełącznika. Po skonfigurowaniu hasła szyfrowanego, użyj odpowiedniego hasła nieszyfrowanego, aby ponownie wejść w ten tryb.

---

---

Krok 4     **show user account-list**  
Zweryfikuj skonfigurowane informacje.

---

Krok 5     **end**  
Powróć do trybu privileged EXEC.

---

Krok 6     **copy running-config startup-config**  
Zapisz ustawienia w pliku konfiguracyjnym.

---

*Wskazówka:*

Zalogowani użytkownicy mogą podać na tej stronie hasło dostępu, aby otrzymać uprawnienia administratorskie.

Poniższy schemat przedstawia przykładowy sposób tworzenia nowych użytkowników o poziomie dostępu konta Operator, ustawiania nazwy użytkownika jako user1, a hasła jako 123, włączania funkcji AAA oraz ustawiania hasła dostępu jako abc123.

**Switch#configure**

**Switch(config)#user name user1 privilege operator password 123**

**Switch(config)#aaa enable**

**Switch(config)#enable admin password abc123**

**Switch(config)#show user account-list**

| Index | User-Name | User-Type |
|-------|-----------|-----------|
| ----- | -----     | -----     |
| 1     | user1     | Operator  |
| 2     | admin     | Admin     |

**Switch(config)#end**

**Switch#copy running-config startup-config**

# 4 Konfiguracja narzędzi systemowych

Narzędzia systemowe umożliwiają:

- konfigurację pliku rozruchowego;
- przywracanie ustawień przełącznika;
- tworzenie kopii zapasowej pliku konfiguracyjnego;
- aktualizację firmware'u;
- konfigurację automatycznej instalacji DHCP;
- restartowanie przełącznika;
- reset przełącznika.

## 4.1 Przez GUI

### 4.1.1 Konfiguracja pliku rozruchowego

Wybierz z menu **SYSTEM > System Tools > Boot Config**, aby wyświetlić poniższą stronę.

Rys. 4-1 Konfiguracja pliku rozruchowego

Boot Config

| <input checked="" type="checkbox"/> | Unit | Current Startup Image | Next Startup Image | Backup Image      | Current Startup Config | Next Startup Config                   | Backup Config                        |
|-------------------------------------|------|-----------------------|--------------------|-------------------|------------------------|---------------------------------------|--------------------------------------|
| <input checked="" type="checkbox"/> | 1    | Image_1.bin           | Image_1.bin        | Image_2.bin       | Config_1.cfg           | Config_1.cfg                          | Config_2.cfg                         |
| Total: 1                            |      |                       |                    | 1 entry selected. |                        | <input type="button" value="Cancel"/> | <input type="button" value="Apply"/> |

Image Table

UNIT1

▼ Current Startup Image

Image Name: image1.bin

Software Version: 3.0.0

Flash Version: 1.3.0

▼ Next Startup Image

Image Name: image1.bin

Software Version: 3.0.0

Flash Version: 1.3.0

▼ Backup Image

Image Name: image2.bin

Software Version: 3.0.0

Flash Version: 1.3.0



Wykonaj poniższe kroki, aby skonfigurować plik rozruchowy:

- 1) W sekcji **Boot Table** wybierz jeden lub więcej modułów i skonfiguruj odpowiednie parametry.

|                        |                                                                                                                                                                                                                                                                    |
|------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Unit                   | Numer modułu.                                                                                                                                                                                                                                                      |
| Current Startup Image  | Aktualny obraz rozruchowy.                                                                                                                                                                                                                                         |
| Next Startup Image     | Wybierz kolejny obraz rozruchowy. Po podłączeniu przełącznika będzie on starał się uruchomić przy pomocy kolejnego obrazu rozruchowego. Kolejny obraz rozruchowy i obraz kopii zapasowej nie mogą być takie same.                                                  |
| Backup Image           | Wybierz obraz kopii zapasowej. Gdy przełącznik nie będzie mógł się uruchomić za pomocą kolejnego obrazu rozruchowego, skorzysta z obrazu kopii zapasowej. Kolejny obraz rozruchowy i obraz kopii zapasowej nie mogą być takie same.                                |
| Current Startup Config | Aktualna konfiguracja rozruchowa.                                                                                                                                                                                                                                  |
| Next Startup Config    | Wybierz kolejną konfigurację rozruchową. Po podłączeniu przełącznika, będzie on starał się uruchomić przy pomocy kolejnej konfiguracji rozruchowej. Kolejna konfiguracja rozruchowa i konfiguracja kopii zapasowej nie mogą być takie same. .                      |
| Backup Config          | Wybierz konfigurację kopii zapasowej. Gdy przełącznik nie będzie mógł się uruchomić za pomocą kolejnej konfiguracji rozruchowej, skorzysta z konfiguracji kopii zapasowej. Kolejna konfiguracja rozruchowa i konfiguracja kopii zapasowej nie mogą być takie same. |

- 2) Kliknij **Apply**.

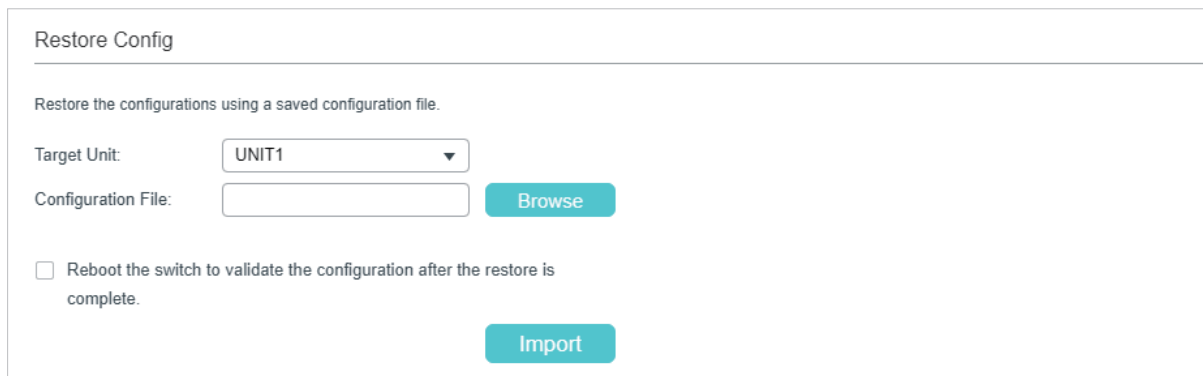
W **Image Table** znajdują się informacje o aktualnym obrazie rozruchowym. Wyświetlane informacje wyglądają następująco:

|                  |                               |
|------------------|-------------------------------|
| Image Name       | Nazwa obrazu.                 |
| Software Version | Wersja oprogramowania obrazu. |
| Flash Version    | Wersja wtyczki Flash obrazu.  |

## 4.1.2 Przywracanie ustawień przełącznika

Wybierz z menu **SYSTEM** > **System Tools** > **Restore Config**, aby wyświetlić poniższą stronę.

Rys. 4-2 Przywracanie konfiguracja przełącznika



Wykonaj poniższe kroki, aby przywrócić aktualną konfigurację przełącznika:

- 1) W sekcji **Restore Config** wybierz moduł, który ma być przywrócony.
- 2) Kliknij **Browse** i wybierz plik konfiguracyjny, który ma być zaimportowany.
- 3) Zdecyduj, czy przełącznik ma się uruchomić ponownie, gdy przywracanie ustawień zostanie ukończony. Zaimportowany obraz będzie obowiązywać dopiero po restarcie przełącznika.
- 4) Kliknij **Import**, aby zaimportować plik konfiguracyjny.

---

 **Uwaga:**

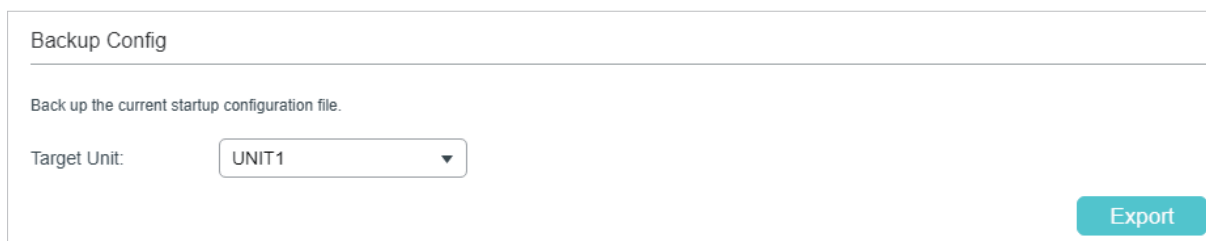
Przywrócenie konfiguracji zajmie trochę czasu. Czekaj, nie wykonując żadnych działań.

---

## 4.1.3 Tworzenie kopii zapasowej pliku konfiguracyjnego

Wybierz z menu **SYSTEM** > **System Tools** > **Backup Config**, aby wyświetlić poniższą stronę.

Rys. 4-3 Tworzenie kopii zapasowej pliku konfiguracyjnego



W sekcji **Config Backup** wybierz jeden moduł i kliknij **Export**, aby wyeksportować plik konfiguracyjny.

---

 **Uwaga:**

Wyeksportowanie konfiguracji może chwilę potrwać. Czekaj, nie wykonując żadnych działań

---

## 4.1.4 Aktualizacja firmware'u

Wybierz z menu **SYSTEM** > **System Tools** > **Firmware Upgrade**, aby wyświetlić poniższą stronę.

Rys. 4-4 Aktualizacja firmware'u

**Firmware Upgrade**

---

You can upgrade the firmware of the switch using the new upgrade file.

Firmware Version: 2.0.0 Build 20181022 Rel.38882(s)

Hardware Version: T2500G-10TS 2.0

Image Name: Backup Image

Firmware File:  Browse

Reboot the switch using the backup image after upgrading is completed.

Upgrade

Na tej stronie znajdują się aktualne informacje dotyczące firmware'u:

|                  |                                                                                             |
|------------------|---------------------------------------------------------------------------------------------|
| Firmware Version | Aktualna wersja firmware'u systemu.                                                         |
| Hardware Version | Aktualna wersja sprzętowa systemu.                                                          |
| Image Name       | Obraz, który ma być zaktualizowany. To działanie będzie miało wpływ wyłącznie na ten obraz. |

Wykonaj poniższe kroki, aby zaktualizować firmware przełącznika:

- 1) Kliknij **Browse** i wybierz odpowiedni plik z aktualizacją firmware'u.
- 2) Zdecyduj, czy przełącznik ma się uruchomić ponownie po zakończeniu aktualizacji. Zaktualizowany firmware będzie obowiązywać dopiero po restarcie przełącznika.
- 3) Kliknij **Upgrade**, aby zaktualizować system.

### Uwaga:

- Aktualizacja przełącznika może chwilę potrwać. Czekaj, nie wykonując żadnych działań.
- Zaleca się zrobić kopię zapasową ustawień przed aktualizacją.

## 4.1.5 Konfiguracja automatycznej instalacji DHCP

Funkcja ta służy do automatycznego pobierania plików konfiguracyjnych i graficznych z serwera TFTP. Wymagana jest dostępność serwera TFTP oraz serwera DHCP, które obsługują opcję 67, 125 oraz 150 w ramach twojej sieci. Po uruchomieniu funkcji automatycznej instalacji przełącznik stara się pozyskać z serwera DHCP informacje o

nazwie pliku konfiguracyjnego, ścieżce pliku graficznego oraz o adresie IP serwera TFTP, a następnie pobiera nowy plik graficzny i konfiguracyjny z serwera TFTP.

Wybierz z menu **SYSTEM > System Tools > DHCP Auto Install**, aby wyświetlić poniższą stronę.

Rys. 4-5 Konfiguracja automatycznej instalacji DHCP

**DHCP Auto Install**

---

DHCP Auto Install:  Enable

Auto Install Persistent Mode:  Enable

Auto Save Mode:  Enable

Auto Reboot Mode:  Enable

Auto Install Retry Count:  (1-3)

Auto Install State: Stopped

Apply

Skonfiguruj poniższe parametry i kliknij **Apply**:

|                              |                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DHCP Auto Install            | Włącz lub wyłącz funkcję automatycznej instalacji DHCP.                                                                                                                                                                                                                                                                                                                                                                                          |
| Auto Install Persistent Mode | Po włączeniu tego trybu przełącznik rozpocznie proces automatycznej instalacji po zakończeniu restartu.                                                                                                                                                                                                                                                                                                                                          |
| Auto Save Mode               | Po włączeniu tego trybu pobrany plik konfiguracyjny zostanie zapisany jako startup configuration file, co oznacza, że konfiguracja ta zostanie wprowadzona po kolejnym restarcie przełącznika.                                                                                                                                                                                                                                                   |
| Auto Reboot Mode             | Po włączeniu tego trybu przełącznik automatycznie się zrestartuje, gdy zakończy się proces instalacji.                                                                                                                                                                                                                                                                                                                                           |
| Auto Install Retry Count     | Określ, ile razy przełącznik może ponowić próbę pobrania pliku konfiguracyjnego lub graficznego z serwera TFTP w ramach jednego cyklu. Jeśli limit zostanie wykorzystany, przełącznik wstrzyma ten mechanizm na 10 minut, po czym ponownie podejmie próbę pozyskania pliku. Proces ten będzie powtarzany do momentu, aż przełącznik pobierze plik graficzny lub konfiguracyjny bądź funkcja automatycznej instalacji zostanie wyłączona ręcznie. |
| Auto Install State           | Stan procesu automatycznej instalacji.                                                                                                                                                                                                                                                                                                                                                                                                           |

#### Uwaga:

- Podczas procesu automatycznej instalacji przełącznik uzyska nowy adres IP z serwera DHCP. W przypadku zamiaru uzyskania dostępu do przełącznika, jego nowy adres IP znajdziesz na serwerze DHCP.
- Jeśli proces automatycznej instalacji nie powiedzie się za pierwszym razem, przełącznik będzie powtarzać go co 10 minut. Mechanizm ten można zatrzymać ręcznie.

## 4.1.6 Restartowanie przełącznika

Istnieją dwie metody restartu przełącznika: restart ręczny i automatyczny po ustawieniu harmonogramu restartu.

### Ręczny restart przełącznika

Wybierz z menu **SYSTEM > System Tools > System Reboot > System Reboot**, aby wyświetlić poniższą stronę.

Rys. 4-6 Ręczny restart przełącznika

System Reboot

Target Unit:

Save the current configuration before reboot

Wykonaj poniższe kroki, aby zrestartować przełącznik:

- 1) W sekcji **System Reboot** wybierz moduł.
- 2) Zdecyduj czy zapisać aktualną konfigurację przed restartem.
- 3) Kliknij **Reboot**.

### Konfiguracja harmonogramu restartu

Wybierz z menu **SYSTEM > System Tools > System Reboot > Reboot Schedule**, aby wyświetlić poniższą stronę.

Rys. 4-1 Konfiguracja harmonogramu restartu

Reboot Schedule Config

Reboot Schedule:  Enable


Time Interval:  minutes (1-43200)

Special Time: Month:  Day:  Year:  Time (HH:MM):

Save the current configuration before reboot

Wykonaj poniższe kroki, aby skonfigurować harmonogram restartu:

- 1) W sekcji **Reboot Schedule Config** wybierz jedną metodę i uzupełnij odpowiednie parametry.

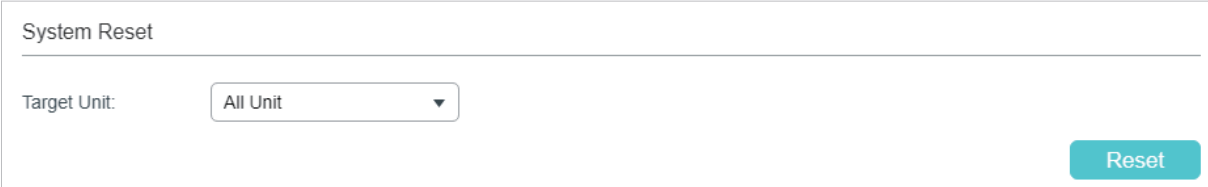
|               |                                                                                                                                                                                                                                                                                                                                                                                                        |
|---------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Time Interval | <p>Podaj wartość interwału. Przełącznik zrestartuje się po upływie tego czasu. Prawidłowe wartości mieszczą się w przedziale 1 - 43200 minut.</p> <p>Aby harmonogram miał charakter cykliczny, kliknij , aby zapisać aktualną konfigurację lub włącz opcję <b>Save the current configuration before reboot</b>.</p> |
| Special Time  | <p>Podaj czas i datę restartu przełącznika.</p> <p><b>Month/Day/Year:</b> Podaj datę restartu przełącznika.</p> <p><b>Time (HH:MM):</b> Podaj czas restartu przełącznika w formacie GG:MM.</p>                                                                                                                                                                                                         |

- 2) Zdecyduj, czy zapisać aktualną konfigurację przed restartem.
- 3) Kliknij **Apply**.

### 4.1.7 Resetowanie przełącznika

Wybierz z menu **SYSTEM > System Tools > System Reset**, aby wyświetlić poniższą stronę.

Rys. 4-7 Resetowanie przełącznika



W sekcji **System Reset** wybierz moduł i kliknij **Reset**. Wszystkie ustawienia przełącznika zostaną przywrócone do wartości domyślnych.

## 4.2 Przez CLI

### 4.2.1 Konfiguracja pliku rozruchowego

Wykonaj poniższe kroki, aby skonfigurować plik rozruchowy:

|        |                                                                                                                                                                                                                                                                                                                                                 |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Krok 1 | <p><b>configure</b></p> <p>Uruchom tryb konfiguracji globalnej.</p>                                                                                                                                                                                                                                                                             |
| Krok 2 | <p><b>boot application filename { image1   image2 } { startup   backup }</b></p> <p>Określ konfigurację pliku rozruchowego. Domyślnie obrazem rozruchowym jest image1.bin, a image2.bin obrazem kopii zapasowej.</p> <p>image1   image2: Wybierz plik obrazu do skonfigurowania.</p> <p>startup   backup: Wybierz właściwości pliku obrazu.</p> |

- 
- Krok 3     **boot config filename { config1 | config2 } { startup | backup }**  
 Określ konfigurację pliku rozruchowego. Domyślnie plikiem konfiguracji rozruchowej jest config1.cfg, a config2.cfg plikiem konfiguracji kopii zapasowej.
- config1 | config2: Wybierz plik konfiguracyjny do dalszej konfiguracji.  
 startup | backup: Określ właściwości pliku konfiguracyjnego.
- 
- Krok 4     **show boot**  
 Zweryfikuj systemową konfigurację pliku rozruchowego.
- 
- Krok 5     **end**  
 Powróć do trybu privileged EXEC.
- 
- Krok 6     **copy running-config startup-config**  
 Zapisz ustawienia w pliku konfiguracyjnym.
- 

Poniższy schemat przedstawia przykładowy sposób ustawiania kolejnego obrazu rozruchowego jako image1, obrazu kopii zapasowej jako image2, kolejnego pliku konfiguracji rozruchowej jako config1 oraz pliku konfiguracji kopii zapasowej jako config2.

### Switch#configure

**Switch(config)#boot application filename image1 startup**

**Switch(config)#boot application filename image2 backup**

**Switch(config)#boot config filename config1 startup**

**Switch(config)#boot config filename config2 backup**

### Switch(config)#show boot

Boot config:

Current Startup Image     - image2.bin

Next Startup Image       - image1.bin

Backup Image             - image2.bin

Current Startup Config   - config2.cfg

Next Startup Config      - config1.cfg

Backup Config            - config2.cfg

### Switch(config)#end

### Switch#copy running-config startup-config

## 4.2.2 Przywracanie konfiguracji przełącznika

Wykonaj poniższe kroki, aby przywrócić konfigurację przełącznika:

Krok 1     **enable**

Uruchom tryb uprzywilejowany.

Krok 2     **copy tftp startup-config ip-address *ip-addr* filename *name***

Pobierz na przełącznik plik konfiguracyjny z serwera TFTP.

*ip-addr*: Podaj adres IP serwera TFTP. Zarówno adres IPv4, jak i adres IPv6 są obsługiwane.

*name*: Podaj nazwę pliku konfiguracyjnego, który ma być pobrany.

### Uwaga:

Aktualizacja przełącznika może trochę potrwać. Czekaj, nie wykonując żadnych działań.

Poniższy schemat przedstawia przykładowy sposób przywracania pliku konfiguracyjnego o nazwie file1 z serwera TFTP za pomocą adresu IP 192.168.0.100.

**Switch>enable**

**Switch#copy tftp startup-config ip-address 192.168.0.100 filename file1**

Start to load user config file.....

Operation OK! Now rebooting system.....

## 4.2.3 Tworzenie kopii zapasowej pliku konfiguracyjnego

Wykonaj poniższe kroki, aby utworzyć w pliku kopię zapasową aktualnej konfiguracji przełącznika:

Krok 1     **enable**

Uruchom tryb uprzywilejowany.

Krok 2     **copy startup-config tftp ip-address *ip-addr* filename *name***

Utwórz kopię zapasową pliku konfiguracyjnego na serwerze TFTP.

*ip-addr*: Podaj adres IP serwera TFTP. Zarówno adres IPv4, jak i adres IPv6 są obsługiwane.

*name*: Podaj nazwę pliku konfiguracyjnego, aby go zapisać.

Poniższy schemat przedstawia przykładowy sposób tworzenia kopii zapasowej pliku konfiguracyjnego o nazwie file2 na serwerze TFTP za pomocą adresu IP 192.168.0.100.

**Switch>enable**

**Switch#copy startup-config tftp ip-address 192.168.0.100 filename file2**

Start to backup user config file.....

Backup user config file OK.



## 4.2.4 Aktualizacja firmware'u

Wykonaj poniższe kroki, aby zaktualizować firmware:

|        |                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Krok 1 | <b>enable</b><br>Uruchom tryb uprzywilejowany.                                                                                                                                                                                                                                                                                                                                                                                         |
| Krok 2 | <b>firmware upgrade ip-address <i>ip-addr</i> filename <i>name</i></b><br>Zaktualizuj obraz kopii zapasowej przełącznika poprzez serwer TFTP. Aby uruchomić system przy użyciu nowego firmware'u, musisz zrestartować przełącznik za pomocą obrazu kopii zapasowej.<br><br><i>ip-addr</i> : Podaj adres IP serwera TFTP. Zarówno adres IPv4, jak i adres IPv6 są obsługiwane.<br><i>name</i> : Podaj nazwę wybranego pliku firmware'u. |
| Krok 3 | Wpisz Y, aby kontynuować, a następnie wpisz Y, aby zrestartować przełącznik za pomocą obrazu kopii zapasowej.                                                                                                                                                                                                                                                                                                                          |

Poniższy schemat przedstawia przykładowy sposób aktualizacji firmware'u za pomocą pliku konfiguracyjnego o nazwie file3.bin. Adresem serwera TFTP jest 190.168.0.100..

**Switch>enable**

**Switch#firmware upgrade ip-address 192.168.0.100 filename file3.bin**

It will only upgrade the backup image. Continue? (Y/N):Y

Operation OK!

Reboot with the backup image? (Y/N):

## 4.2.5 Konfiguracja automatycznej instalacji DHCP

Funkcja ta służy do automatycznego pobierania plików konfiguracyjnych i graficznych z serwera TFTP. Wymagana jest dostępność serwera TFTP oraz serwera DHCP, które obsługują opcję 67, 125 oraz 150 w ramach twojej sieci. Po uruchomieniu funkcji automatycznej instalacji przełącznik stara się pozyskać z serwera DHCP informacje o nazwie pliku konfiguracyjnego, ścieżce pliku graficznego oraz o adresie IP serwera TFTP, a następnie pobiera nowy plik graficzny i konfiguracyjny z serwera TFTP.

Wykonaj poniższe kroki, aby skonfigurować funkcję automatycznej instalacji DHCP.

|        |                                                                                                                                                                                                     |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Krok 1 | <b>configure</b><br>Uruchom tryb konfiguracji globalnej.                                                                                                                                            |
| Krok 2 | <b>boot autoinstall persistent-mode</b><br>Włącz auto install persistent mode. Po zapisaniu konfiguracji przełącznik automatycznie włączy funkcję automatycznej instalacji po zakończeniu restartu. |

|        |                                           |                                                                                                                                                      |
|--------|-------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------|
| Krok 3 | <b>boot autoinstall auto-save</b>         | Włącz auto save mode, a pobrany plik konfiguracyjny zostanie automatycznie zapisany jako startup configuration file (plik konfiguracji początkowej). |
| Krok 4 | <b>boot autoinstall auto-reboot</b>       | Włącz auto reboot mode, a przełącznik automatycznie się zrestartuje po udanym procesie automatycznej instalacji.                                     |
| Krok 5 | <b>boot autoinstall retry-count count</b> | Określ liczbę powtórzeń cyklu automatycznej instalacji, wybierając od 1 do 3. Wartością domyślną jest 1.                                             |
| Krok 6 | <b>boot autoinstall start</b>             | Rozpocznij proces automatycznej instalacji, a przełącznik automatycznie pobierze plik konfiguracyjny i obraz odzyskiwania.                           |
| Krok 7 | <b>end</b>                                | Powróć do trybu privileged EXEC.                                                                                                                     |
| Krok 8 | <b>copy running-config startup-config</b> | Zapisz ustawienia w pliku konfiguracyjnym.                                                                                                           |

 **Uwaga:**

- Podczas procesu automatycznej instalacji przełącznik uzyska nowy adres IP z serwera DHCP. W przypadku zamiaru uzyskania dostępu do przełącznika, jego nowy adres IP znajdziesz na serwerze DHCP.
- Jeśli proces automatycznej instalacji nie powiedzie się za pierwszym razem, przełącznik będzie powtarzać go co 10 minut. Mechanizm ten można zatrzymać ręcznie.

Poniższy schemat przedstawia przykładowy sposób konfiguracji funkcji automatycznej instalacji.

```
Switch#configure
```

```
Switch(config)#boot autoinstall persistent-mode
```

```
Switch(config)#boot autoinstall auto-save
```

```
Switch(config)#boot autoinstall auto-reboot
```

```
Switch(config)#boot autoinstall retry-count 2
```

```
Switch(config)#show boot autoinstall
```

```
Auto Insatll Mode.....Stop
```

```
Auto Insatll Persistent Mode.....Enabled
```

```
Auto Save Mode.....Enabled
```

```
Auto Reboot Mode.....Enabled
```

Auto Insatll Retry Count.....2  
 Auto Insatll sate.....Stopped

## 4.2.6 Restartowanie przełącznika

### Ręczne restartowanie przełącznika

Wykonaj poniższe kroki, aby zrestartować przełącznik:

---

Krok 1     **enable**  
 Uruchom tryb uprzywilejowany.

---

Krok 2     **reboot**  
 Uruchom ponownie przełącznik.

---

### Konfiguracja harmonogramu restartu

Wykonaj poniższe kroki, aby skonfigurować harmonogram restartu:

---

Krok 1     **configure**  
 Uruchom tryb konfiguracji globalnej.

Krok 2     Skorzystaj z poniższego polecenia, aby ustawić interwał restartu:

**reboot-schedule in *interval* [ *save\_before\_reboot* ]**

(Opcjonalnie) Ustaw harmonogram restartu.

*interval*: Podaj wartość interwału. Przełącznik uruchomi się ponownie po upływie tego czasu. Prawidłowe wartości mieszczą się w przedziale 1 - 43200 minut.

**save\_before\_reboot**: Zapisz plik konfiguracyjny przed restartem przełącznika. Aby harmonogram miał charakter cykliczny, dodaj tę część do polecenia.

Skorzystaj z poniższego polecenia, aby ustawić specjalny czas restartu:

**reboot-schedule at *time* [ *date* ] [ *save\_before\_reboot* ]**

(Opcjonalnie) Ustaw harmonogram restartu.

*time*: Podaj czas restartu przełącznika w formacie GG:MM.

*date*: Podaj datę restartu przełącznika w formacie DD/MM/YYYY. Data nie powinna przekraczać okresu najbliższych 30 dni.

**save\_before\_reboot**: Zapisz plik konfiguracyjny przed restartem przełącznika.

Jeżeli nie podasz żadnej daty, przełącznik zrestartuje się zgodnie z czasem, który ustawiłeś. Jeżeli czas, który ustawiłeś jest późniejszy niż czas wykonania polecenia, przełącznik zrestartuje się później w tym samym dniu. W innym wypadku przełącznik zrestartuje się kolejnego dnia.

---

Krok 3     **end**  
 Powróć do trybu privileged EXEC.

---

---

**Krok 4**     **copy running-config startup-config**

Zapisz ustawienia w pliku konfiguracyjnym.

---

Poniższy schemat przedstawia przykładowy sposób ustawienia restartu przełącznika na godzinę 12:00 dnia 15/08/2017.

**Switch#configure****Switch(config)#reboot-schedule at 12:00 15/08/2017 save\_before\_reboot**

Reboot system at 15/08/2017 12:00. Continue? (Y/N): Y

Reboot Schedule Settings

-----

Reboot schedule at 2017-08-15 12:00 (in 25582 minutes)

Save before reboot: Yes

**Switch(config)#end****Switch#copy running-config startup-config**

## 4.2.7 Reset przełącznika

Wykonaj poniższe kroki, aby zresetować przełącznik.

---

**Krok 1**     **enable**

Uruchom tryb uprzywilejowany.

---

**Krok 2**     **reset**

Zresetuj przełącznik. Wszystkie ustawienia przełącznika zostaną przywrócone do wartości fabrycznych.

# 5 Konfiguracja EEE

Wybierz z menu **SYSTEM** > **EEE**, aby wyświetlić poniższą stronę.

Rys. 5-1 Konfiguracja EEE

| UNIT1                               | LAGS | Port   | Status   |
|-------------------------------------|------|--------|----------|
| <input checked="" type="checkbox"/> |      | 1/0/1  | Disabled |
| <input type="checkbox"/>            |      | 1/0/2  | Disabled |
| <input type="checkbox"/>            |      | 1/0/3  | Disabled |
| <input type="checkbox"/>            |      | 1/0/4  | Disabled |
| <input type="checkbox"/>            |      | 1/0/5  | Disabled |
| <input type="checkbox"/>            |      | 1/0/6  | Disabled |
| <input type="checkbox"/>            |      | 1/0/7  | Disabled |
| <input type="checkbox"/>            |      | 1/0/8  | Disabled |
| <input type="checkbox"/>            |      | 1/0/9  | Disabled |
| <input type="checkbox"/>            |      | 1/0/10 | Disabled |

Total: 28      1 entry selected.      Cancel      Apply

Wykonaj poniższe kroki, aby skonfigurować EEE:

- 1) W sekcji **EEE Config** wybierz jeden lub więcej portów, które chcesz skonfigurować.
- 2) Włącz lub wyłącz EEE dla poszczególnych portów.
- 3) Kliknij **Apply**.

## 5.1 Przez CLI

Wykonaj poniższe kroki, aby skonfigurować EEE:

|        |                                                                                                                                                                                                                                          |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Krok 1 | <b>configure</b><br>Uruchom tryb konfiguracji globalnej.                                                                                                                                                                                 |
| Krok 2 | <b>interface { fastEthernet port   range fastEthernet port-list   gigabitEthernet port   range gigabitEthernet port-list   ten-gigabitEthernet port   range ten-gigabitEthernet port-list }</b><br>Uruchom tryb konfiguracji interfejsu. |
| Krok 3 | <b>eee</b><br>Włącz EEE na porcie.                                                                                                                                                                                                       |

---

Krok 4     **end**  
Powróć do trybu privileged EXEC.

---

Krok 5     **copy running-config startup-config**  
Zapisz ustawienia w pliku konfiguracyjnym.

---

Poniższy schemat przedstawia przykładowy sposób włączania funkcji EEE na porcie 1/0/1.

**Switch#config**

**Switch(config)#interface gigabitEthernet 1/0/1**

**Switch(config-if)#eee**

**Switch(config-if)#show interface eee**

Port     EEE status

Gi1/0/1   Enable

Gi1/0/2   Disable

...

**Switch(config-if)#end**

**Switch#copy running-config startup-config**

# 6 Konfiguracja szablonów SDM

## 6.1 Przez GUI

Wybierz z menu **SYSTEM > SDM Template**, aby wyświetlić poniższą stronę.

Rys. 6-1 Konfiguracja szablonu SDM

**SDM Template Config**

---

Current Template: Default

Next Template: Default

Select Next Template:  ▼

[Apply](#)

**SDM Template Table**

---

| SDM Template | IP ACL Rules | MAC ACL Rules | IPv6 ACL Rules | IPv4 Source Guard Entries | IPv6 Source Guard Entries |
|--------------|--------------|---------------|----------------|---------------------------|---------------------------|
| Default      | 100          | 80            | 0              | 253                       | 0                         |
| EnterpriseV4 | 120          | 84            | 0              | 253                       | 0                         |
| EnterpriseV6 | 32           | 32            | 120            | 0                         | 183                       |
| Total: 3     |              |               |                |                           |                           |

W sekcji **SDM Template Config** wybierz jeden szablon i kliknij **Apply**. Ustawienie zostanie wprowadzone po restarcie przełącznika.

|                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Current Template</b>     | Aktualnie obowiązujący szablon.                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Next Template</b>        | Szablon, który będzie obowiązujący po restarcie przełącznika.                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Select Next Template</b> | <p>Wybierz szablon, który będzie obowiązujący po najbliższym restarcie przełącznika.</p> <p><b>Default:</b> Wybierz szablon domyślny. Ten szablon równoważy działanie reguł ACL IP i ACL MAC oraz wpisów ochrony ARP.</p> <p><b>EnterpriseV4:</b> Wybierz szablon enterpriseV4. Ten szablon maksymalizuje zasoby systemowe dla reguł ACL IP i ACL MAC.</p> <p><b>EnterpriseV6:</b> Wybierz szablon enterpriseV6. Ten szablon przydziela zasoby regułom ACL IPv6.</p> |

Tabela szablonów prezentuje przydział zasobów dla każdego z szablonów.

|                     |                                                             |
|---------------------|-------------------------------------------------------------|
| <b>SDM Template</b> | Nazwa szablonów.                                            |
| <b>IP ACL Rules</b> | Liczba reguł ACL IP, w tym reguł ACL warstwy 3 i warstwy 4. |

|                           |                                  |
|---------------------------|----------------------------------|
| MAC ACL Rules             | Liczba reguł ACL warstwy 2.      |
| Combined ACL Rules        | Liczba wszystkich reguł ACL.     |
| IPv6 ACL Rules            | Liczba reguł ACL IPv6.           |
| IPv4 Source Guard Entries | Liczba wpisów IPv4 Source Guard. |
| IPv6 Source Guard Entries | Liczba wpisów IPv6 Source Guard. |

## 6.2 Przez CLI

Wykonaj poniższe kroki, aby skonfigurować szablon SDM:

|        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Krok 1 | <b>configure</b><br>Uruchom tryb konfiguracji globalnej.                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Krok 2 | <b>show sdm prefer { used   default   enterpriseV4   enterpriseV6 }</b><br>Przejrzyj tabelę szablonów. Na tej podstawie wybierzesz najodpowiedniejszy dla swojej sieci szablon.<br><br>used: Przydział zasobów dla aktualnego szablonu.<br><br>default: Przydział zasobów dla szablonu domyślnego.<br><br>enterpriseV4: Przydział zasobów dla szablonu enterpriseV4.<br><br>enterpriseV6: Przydział zasobów dla szablonu enterpriseV6.                                                      |
| Krok 3 | <b>sdm prefer { default   enterpriseV4   enterpriseV6 }</b><br>Wybierz szablon, który będzie obowiązujący po restarcie przełącznika.<br><br>default: Wybierz szablon domyślny. Ten szablon równoważy działanie reguł ACL IP i ACL MAC oraz wpisów ochrony ARP.<br><br>enterpriseV4: Wybierz szablon enterpriseV4. Ten szablon maksymalizuje zasoby systemowe dla reguł ACL IP i ACL MAC.<br><br>enterpriseV6: Wybierz szablon enterpriseV6. Ten szablon przydziela zasoby regułom ACL IPv6. |
| Krok 4 | <b>end</b><br>Powróć do trybu privileged EXEC.                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Krok 5 | <b>copy running-config startup-config</b><br>Zapisz ustawienia w pliku konfiguracyjnym.                                                                                                                                                                                                                                                                                                                                                                                                     |



Poniższy schemat przedstawia przykładowy sposób ustawiania szablonu SDM jako enterpriseV4.

**Switch#config****Switch(config)#show sdm prefer enterpriseV4**

"enterpriseV4" template:

number of IP ACL Rules : 120

number of MAC ACL Rules : 84

number of IPV6 ACL Rules : 0

number of IPV4 Source Guard Entries : 253

number of IPV6 Source Guard Entries : 0

**Switch(config)#sdm prefer enterpriseV4**

Zmiana na szablon "enterpriseV4".

Zmiany ustawień szablonu SDM zostały zapisane, ale nie zostaną wprowadzone do czasu restartu przełącznika.

**Switch(config)#end****Switch#copy running-config startup-config**

# 7 Konfiguracja przedziałów czasowych

Aby skonfigurować przedziały czasowe, wykonaj poniższe kroki:

- 1) Dodaj pozycje z przedziałami czasowymi.
- 2) Skonfiguruj okres wakacyjny.

## 7.1 Przez GUI

### 7.1.1 Dodawanie pozycji z przedziałami czasowymi

Wybierz z menu **SYSTEM > Time Range > Time Range Config** i kliknij  Add, aby wyświetlić poniższą stronę.

Rys. 7-1 Konfiguracja przedziału czasowego

**Time-Range Config**



---

Name:  (1-16 characters)

Holiday:  Exclude  Include

---

**Period Time Config**

 Add  Delete

| <input type="checkbox"/>  | Index | Date | Day | Time | Operation |
|---------------------------|-------|------|-----|------|-----------|
| No entries in this table. |       |      |     |      |           |

Total: 0

Discard
Create

Wykonaj poniższe kroki, aby dodać wpisy z przedziałami czasowymi:

- 1) W sekcji **Time-Range Config** podaj nazwę pozycji i zaznacz tryb Holiday.

|         |                                                                                                                                                                                                                                                                                                                                                                       |
|---------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Name    | Podaj nazwę pozycji.                                                                                                                                                                                                                                                                                                                                                  |
| Holiday | Zaznacz, aby przedział czasowy obowiązywał/nie obowiązywał w okresie wakacyjnym.<br><br><b>Exclude:</b> Przedział czasowy nie będzie obowiązywał w okresie wakacyjnym.<br><br><b>Include:</b> Okres wakacyjny nie będzie miał wpływu na przedział czasowy.<br><br>Aby skonfigurować okres wakacji, zapoznaj się z rozdziałem <i>Konfiguracja okresu wakacyjnego..</i> |

- 2) W sekcji **Period Time Config** kliknij  Add. Pojawi się poniższe okno.

Rys, 7-2 Dodawanie przedziału czasowego

Period Time Config

---

**Date**

From      Month:       Day:       Year:

To          Month:       Day:       Year:

---

**Time**

From:  (Format: HH:MM)

To:  (Format: HH:MM)

---

**Day of Week**

Mon     Tue     Wed     Thu     Fri     Sat     Sun

Skonfiguruj poniższe parametry i kliknij **Create**:

|                    |                                                                               |
|--------------------|-------------------------------------------------------------------------------|
| <b>Date</b>        | Podaj datę początkową i datę końcową tego przedziału czasowego.               |
| <b>Time</b>        | Podaj godzinę początku i godzinę końca dnia.                                  |
| <b>Day of Week</b> | Wybierz dni tygodnia, dla których dany przedział czasowy będzie obowiązujący. |

- 3) W taki sam sposób możesz dodać kolejne pozycje. Końcowy przedział czasowy jest sumą wszystkich przedziałów w tabeli. Kliknij **Create**.

Rys. 7-3 Wynik konfiguracji

### Time-Range Config

Name:  (1-16 characters)

Holiday:  Exclude  Include

---

### Period Time Config

+ Add - Delete

| <input type="checkbox"/> | Index | Date                               | Day                     | Time          | Operation |
|--------------------------|-------|------------------------------------|-------------------------|---------------|-----------|
| <input type="checkbox"/> | 1     | January 1, 2017 - November 1, 2017 | Mon, Tue, Wed, Thu, Fri | 08:00 - 20:00 |           |
| Total: 1                 |       |                                    |                         |               |           |

## 7.1.2 Konfiguracja okresu wakacyjnego

Wybierz z menu **SYSTEM > Time Range > Holiday Config** i kliknij **Add**, aby wyświetlić poniższą stronę.

Rys. 7-1 Konfiguracja okresu wakacyjnego

### Holiday Config

Holiday Name:  (1-31 characters)

Start Date

Month:  Day:

End Date

Month:  Day:

Skonfiguruj poniższe parametry i kliknij **Create**, aby dodać nową pozycję.

|              |                                           |
|--------------|-------------------------------------------|
| Holiday Name | Podaj nazwę pozycji.                      |
| Start Date   | Podaj datę początkową okresu wakacyjnego. |
| End Date     | Podaj datę końcową okresu wakacyjnego.    |

W podobny sposób możesz dodać kolejne pozycje. Końcowy okres wakacyjny to suma wszystkich pozycji.

## 7.2 Przez CLI

### 7.2.1 Dodawanie pozycji z przedziałami czasowymi

Wykonaj poniższe kroki, aby dodać pozycje z przedziałami czasowymi:

|        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Krok 1 | <b>configure</b><br>Uruchom tryb konfiguracji globalnej.                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Krok 2 | <b>time-range <i>name</i></b><br>Utwórz pozycję z przedziałem czasowym.<br><br><i>name</i> : Podaj nazwę pozycji.                                                                                                                                                                                                                                                                                                                                                                                      |
| Krok 3 | <b>holiday { exclude   include }</b><br>Zdecyduj, czy przedział czasowy ma obowiązywać w okresie wakacyjnym.<br><br><i>exclude</i> : Przedział czasowy nie będzie obowiązywał w okresie wakacyjnym.<br><br><i>include</i> : Okres wakacyjny nie będzie miał wpływu na przedział czasowy.<br><br>Aby skonfigurować okres wakacji, zapoznaj się z rozdziałem <i>Konfiguracja okresu wakacyjnego..</i>                                                                                                    |
| Krok 4 | <b>absolute from <i>start-date</i> to <i>end-date</i></b><br>Podaj datę początkową i datę końcową tego przedziału czasowego.<br><br><i>start-date</i> : Podaj datę początkową w formacie MM/DD/RRRR.<br><br><i>end-date</i> : Podaj datę końcową w formacie MM/DD/RRRR.                                                                                                                                                                                                                                |
| Krok 5 | <b>periodic { [start <i>start-time</i> ] [end <i>end-time</i> ] [day-of-the-week <i>week-day</i> ] }</b><br>Wybierz dni tygodnia, dla których dany przedział czasowy będzie obowiązuje.<br><br><i>start-time</i> : Podaj godzinę początku dnia w formacie GG:MM.<br><br><i>end-time</i> : Podaj godzinę końca dnia w formacie GG:MM.<br><br><i>week-day</i> : Podaj dni tygodnia w formacie 1-3, 7. Cyfry 1-7 oznaczają odpowiednio Poniedziałek, Wtorek, Środę, Czwartek, Piątek, Sobotę i Niedzielę. |
| Krok 6 | <b>show time-range</b><br>Sprawdź konfigurację przedziału czasowego.                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Krok 7 | <b>end</b><br>Powróć do trybu privileged EXEC.                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Krok 8 | <b>copy running-config startup-config</b><br>Zapisz ustawienia w pliku konfiguracyjnym.                                                                                                                                                                                                                                                                                                                                                                                                                |

Poniższy schemat przedstawia przykładowy sposób tworzenia pozycji z przedziałem czasowym i ustawiania nazwy jako time1, okresu wakacji do trybu exclude, czasu

całkowitego jako 10/01/2017 - 10/31/2017, a godzinowego jako 8:00 - 20:00 w każdy poniedziałek i wtorek:

**Switch#config**

**Switch(config)#time-range** time1

**Switch(config-time-range)#holiday** exclude

**Switch(config-time-range)#absolute** from 10/01/2017 to 10/31/2017

**Switch(config-time-range)#periodic** start 08:00 end 20:00 day-of-the-week 1,2

**Switch(config-time-range)#show** time-range

Time-range entry: 12 (Inactive)

Time-range entry: time1 (Inactive)

holiday: exclude

number of time slice: 1

01 - 10/01/2017 to 10/31/2017

- 08:00 to 20:00 on 1,2

**Switch(config-time-range)#end**

**Switch#copy** running-config startup-config

## 7.2.2 Konfiguracja okresu wakacyjnego

Wykonaj poniższe kroki, aby skonfigurować okres wakacyjny:

|        |                                                                                                                                                                                                                                                                                  |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Krok 1 | <b>configure</b><br>Uruchom tryb konfiguracji globalnej.                                                                                                                                                                                                                         |
| Krok 2 | <b>holiday</b> <i>name</i> <i>start-date</i> <i>start-date</i> <i>end-date</i> <i>end-date</i><br>Utwórz pozycję.<br><i>name</i> : Podaj nazwę pozycji.<br><i>start-date</i> : Podaj datę początkową w formacie MM/DD.<br><i>end-date</i> : Podaj datę końcową w formacie MM/DD. |
| Krok 3 | <b>show holiday</b><br>Sprawdź konfigurację okresu wakacyjnego.                                                                                                                                                                                                                  |
| Krok 4 | <b>end</b><br>Powróć do trybu privileged EXEC.                                                                                                                                                                                                                                   |
| Krok 8 | <b>copy running-config startup-config</b><br>Zapisz ustawienia w pliku konfiguracyjnym.                                                                                                                                                                                          |

Poniższy schemat przedstawia przykładowy sposób tworzenia pozycji czasu wakacyjnego, ustawiania nazwy pozycji jako holiday1 oraz dat początkowych i końcowych jako 07/01 i 09/01:

**Switch#config**

**Switch(config)#holiday holiday1 start-date 07/01 end-date 09/01**

**Switch(config)#show holiday**

| Index | Holiday Name | Start-End   |
|-------|--------------|-------------|
| ----- | -----        | -----       |
| 1     | holiday1     | 07.01-09.01 |

**Switch(config)#end**

**Switch#copy running-config startup-config**

# Część 3

## Zarządzanie interfejsami

### ROZDZIAŁY

1. Interfejs fizyczny
2. Konfiguracja podstawowych parametrów
3. Konfiguracja funkcji izolacji portów
4. Konfiguracja funkcji Loopback Detection
5. Przykłady konfiguracji



# 1 Interfejs fizyczny

## 1.1 Informacje ogólne

Interfejsy służą do wymiany danych oraz interakcji z interfejsami innych urządzeń sieciowych. Ich klasyfikacja uwzględnia interfejsy fizyczne oraz interfejsy warstwy 3.

- Interfejsy fizyczne to porty znajdujące się na panelu przełącznika. Przekazują pakiety na podstawie tablicy adresów MAC.
- Interfejsy warstwy 3 służą do przekazywania pakietów IPv4 oraz IPv6 z wykorzystaniem statycznych lub dynamicznych protokołów routingu. Interfejsy warstwy 3 można stosować do routingu IP i routingu między sieciami VLAN.

W tej części omówiono konfigurację interfejsów fizycznych.

## 1.2 Obsługiwane funkcje

Przełącznik obsługuje następujące funkcje dla interfejsów fizycznych:

### Parametry podstawowe

Możesz skonfigurować status, tryb prędkości, tryb duplexu, kontrolę przepływu i inne parametry podstawowe portów.

### Izolacja portów

Funkcja umożliwia ograniczenie działania wybranego portu do wysyłania pakietów jedynie do portów ze skonfigurowanej listy portów przesyłających.

### Loopback Detection

Dzięki tej funkcji przełącznik może wykrywać pętle w sieci. Po wykryciu pętli na porcie lub w sieci VLAN przełącznik wyświetli ostrzeżenie na interfejsie zarządzania i zgodnie z ustawieniami zablokuje odpowiedni port lub sieć VLAN.

# 2 Konfiguracja podstawowych parametrów

## 2.1 Przez GUI

Wybierz z menu **L2 FEATURES > Switching > Port > Port Config**, aby wyświetlić poniższą stronę.

Rys. 2-1 Konfiguracja podstawowych parametrów

Port Config

Jumbo:  bytes (1518-9216) Apply

UNIT1 | LAGS

| <input type="checkbox"/>            | Port   | Type   | Description | Status  | Speed | Duplex | Flow Control | LAG |
|-------------------------------------|--------|--------|-------------|---------|-------|--------|--------------|-----|
| <input checked="" type="checkbox"/> | 1/0/1  | Copper |             | Enabled | Auto  | Auto   | Disabled     | --  |
| <input type="checkbox"/>            | 1/0/2  | Copper |             | Enabled | Auto  | Auto   | Disabled     | --  |
| <input type="checkbox"/>            | 1/0/3  | Copper |             | Enabled | Auto  | Auto   | Disabled     | --  |
| <input type="checkbox"/>            | 1/0/4  | Copper |             | Enabled | Auto  | Auto   | Disabled     | --  |
| <input type="checkbox"/>            | 1/0/5  | Copper |             | Enabled | Auto  | Auto   | Disabled     | --  |
| <input type="checkbox"/>            | 1/0/6  | Copper |             | Enabled | Auto  | Auto   | Disabled     | --  |
| <input type="checkbox"/>            | 1/0/7  | Copper |             | Enabled | Auto  | Auto   | Disabled     | --  |
| <input type="checkbox"/>            | 1/0/8  | Copper |             | Enabled | Auto  | Auto   | Disabled     | --  |
| <input type="checkbox"/>            | 1/0/9  | Fiber  |             | Enabled | 1000M | Full   | Disabled     | --  |
| <input type="checkbox"/>            | 1/0/10 | Fiber  |             | Enabled | 1000M | Full   | Disabled     | --  |

Total: 10 1 entry selected. Cancel Apply

Aby skonfigurować parametry podstawowe portów, wykonaj poniższe kroki:

- 1) Skonfiguruj rozmiar MTU ramek Jumbo dla wszystkich portów i kliknij **Apply**.

### Jumbo

Skonfiguruj rozmiar ramek jumbo. Wielkość domyślna to 1518 bajtów.

Z reguły rozmiar MTU (Maximum Transmission Unit) standardowej ramki to 1518 bajtów. Jeżeli chcesz, żeby przełącznik wysyłał ramki o MTU większym niż 1518 bajtów, w tym miejscu możesz ręcznie skonfigurować rozmiar MTU.

- 2) Wybierz co najmniej jeden port do konfiguracji parametrów podstawowych i kliknij **Apply**.

### UNIT/LAGS

Kliknij **UNIT**, aby skonfigurować porty fizyczne. Kliknij **LAGS**, aby przeprowadzić konfigurację LAG.

|              |                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|--------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Type         | Informacja dotyczy typu portu. <b>Copper</b> oznacza port Ethernet, a <b>Fiber</b> oznacza port SFP.                                                                                                                                                                                                                                                                                                                                   |
| Description  | Wprowadź opis portu (opcjonalnie).                                                                                                                                                                                                                                                                                                                                                                                                     |
| Status       | Przy włączonej funkcji port normalnie przekierowuje pakiety. Port nie działa przy wyłączonej opcji. Funkcja jest domyślnie włączona.                                                                                                                                                                                                                                                                                                   |
| Speed        | Wybierz odpowiedni tryb prędkości dla portu. Przy wybraniu opcji <b>Auto</b> port automatycznie negocjuje prędkość z sąsiednim urządzeniem. Opcja <b>Auto</b> jest ustawiona domyślnie. Jeżeli obie strony łączy obsługują autonegocjację, zaleca się wybranie ustawienia <b>Auto</b> .                                                                                                                                                |
| Duplex       | Wybierz odpowiedni tryb duplexu dla portu. Dostępne są trzy opcje: <b>Half</b> (półduplex), <b>Full</b> (pełny duplex) i <b>Auto</b> . Domyślnie ustawiona opcja to <b>Auto</b> .<br><br><b>Half:</b> Port może wysyłać i otrzymywać pakiety, ale nie w tym samym czasie.<br><br><b>Full:</b> Port może jednocześnie wysyłać i otrzymywać pakiety.<br><br><b>Auto:</b> Port automatycznie negocjuje duplex z urządzeniem równorzędnym. |
| Flow Control | Po włączeniu tej opcji, gdy przełącznik będzie przeciążony, wyśle ramkę PAUSE, aby powiadomić urządzenie równorzędne o zaprzestaniu wysyłania danych przez określony czas, co wyeliminuje problem utraty pakietów. Domyślnie opcja jest wyłączona.                                                                                                                                                                                     |

### Uwaga:

Zaleca się ustawić ten sam tryb prędkości i duplexu dla portów na obu stronach łącza.

## 2.2 Przez CLI

Wykonaj poniższe kroki, aby skonfigurować podstawowe parametry portów..

|        |                                                                                                                                                                                                                                                                                                                                                                                                                   |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Krok 1 | <b>configure</b><br>Uruchom tryb konfiguracji globalnej.                                                                                                                                                                                                                                                                                                                                                          |
| Krok 2 | <b>jumbo-size size</b><br>Zmień rozmiar MTU (Maximum Transmission Unit) do obsługi ramek jumbo. Domyślny rozmiar MTU ramek otrzymywanych i wysyłanych dla wszystkich portów wynosi 1518 bajtów. Aby przekazywać ramki jumbo, możesz ręcznie ustawić rozmiar MTU ramek, maksymalna wartość to 9216 bajtów.<br><br><i>size:</i> Skonfiguruj rozmiar MTU ramek jumbo. Może być to wartość między 1518 a 9216 bajtów. |
| Krok 3 | <b>interface { fastEthernet port   range fastEthernet port-list   gigabitEthernet port   range gigabitEthernet port-list   ten-gigabitEthernet port   ten-range gigabitEthernet port-list   port-channel port-channel   range port-channel port-channel-list }</b><br>Uruchom tryb konfiguracji interfejsu.                                                                                                       |

|        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Krok 4 | <p>Skonfiguruj podstawowe parametry portu.</p> <p><b>description <i>string</i></b><br/>Dodaj opis portu.<br/><i>string</i>: Treść opisu portu, zawierająca od 1 do 16 znaków.</p> <p><b>shutdown</b><br/><b>no shutdown</b><br/>Wybierz <b>shutdown</b>, aby wyłączyć port i <b>no shutdown</b>, aby włączyć port. Włączony port normalnie przekierowuje pakiety. Port wyłączony odrzuca otrzymywane pakiety. Domyślnie wszystkie porty są włączone.</p> <p><b>speed { 10   100   1000   10000   auto }</b><br/>Ustaw odpowiedni tryb prędkości dla portu.<br/><b>10   100   1000   10000   auto</b>: Tryb prędkości portu. Dostępne opcje różnią się w zależności od posiadanego urządzenia. Zaleca się ustawić ten sam tryb prędkości i dupleksu dla portu i połączanego z nim urządzenia. W przypadku wybrania opcji auto tryb prędkości wybierany jest na podstawie autonegocjacji.</p> <p><b>duplex { auto   full   half }</b><br/>Ustaw odpowiedni tryb dupleksu dla portu.<br/><b>auto   full   half</b>: Tryb dupleksu dla portu. Zaleca się ustawić ten sam tryb prędkości i dupleksu dla portu i połączanego z nim urządzenia. W przypadku wybrania opcji auto tryb dupleksu wybierany jest na podstawie autonegocjacji.</p> <p><b>flow-control</b><br/>Funkcja kontroli przepływu umożliwi przełącznikowi synchronizację prędkości transmisji danych z urządzeniem równorzędnym, co wyeliminuje problem utraty pakietów. Domyślnie opcja jest wyłączona.</p> |
| Krok 5 | <p><b>show interface configuration [ fastEthernet <i>port</i>   gigabitEthernet <i>port</i>     ten-gigabitEthernet <i>port</i>   port-channel <i>port-channel-id</i> ]</b><br/>Sprawdź konfigurację portu lub konfigurację LAG.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Krok 6 | <p><b>end</b><br/>Wróć do trybu privileged EXEC.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Krok 7 | <p><b>copy running-config startup-config</b><br/>Zapisz ustawienia w pliku konfiguracyjnym.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |

Poniższy przykład prezentuje, jak wprowadzić podstawowe konfiguracje portu 1/0/1, takie jak ustawianie opisu portu, konfiguracja ramki jumbo, ustawianie autonegocjacji prędkości i dupleksu z sąsiadującym portem i włączanie funkcji kontroli przepływu:

```
Switch#configure
```

```
Switch#jumbo-size 9216
```

```
Switch(config)#interface gigabitEthernet 1/0/1
```

```
Switch(config-if)#no shutdown
```

```
Switch(config-if)#description router connection
```

```
Switch(config-if)#speed auto
```

```
Switch(config-if)#duplex auto
```

```
Switch(config-if)#flow-control
```

```
Switch(config-if)#show interface configuration gigabitEthernet 1/0/1
```

| Port    | State  | Speed | Duplex | FlowCtrl | Jumbo   | Description       |
|---------|--------|-------|--------|----------|---------|-------------------|
| -----   | -----  | ----- | -----  | -----    | -----   | -----             |
| Gi1/0/1 | Enable | Auto  | Auto   | Enable   | Disable | router connection |

```
Switch(config-if)#show jumbo-size
```

```
Global jumbo size : 9216
```

```
Switch(config-if)#end
```

```
Switch#copy running-config startup-config
```

# 3 Konfiguracja funkcji izolacji portów

## 3.1 Przez GUI


Funkcja izolacji portów (Port Isolation) służy do ograniczania ilości danych przekazywanych przez port. Izolowany port może wysyłać pakiety jedynie do portów znajdujących się na jego liście (Forwarding Port List).

Wybierz z menu **L2 FEATURES > Switching > Port > Port Isolation**, aby wyświetlić poniższą stronę.

Rys. 3-1 Lista izolacji portów

| Port   | LAG | Forwarding Port List |
|--------|-----|----------------------|
| 1/0/1  | --  | 1/0/1-10,LAG1-8      |
| 1/0/2  | --  | 1/0/1-10,LAG1-8      |
| 1/0/3  | --  | 1/0/1-10,LAG1-8      |
| 1/0/4  | --  | 1/0/1-10,LAG1-8      |
| 1/0/5  | --  | 1/0/1-10,LAG1-8      |
| 1/0/6  | --  | 1/0/1-10,LAG1-8      |
| 1/0/7  | --  | 1/0/1-10,LAG1-8      |
| 1/0/8  | --  | 1/0/1-10,LAG1-8      |
| 1/0/9  | --  | 1/0/1-10,LAG1-8      |
| 1/0/10 | --  | 1/0/1-10,LAG1-8      |

Total: 10

Na powyższej stronie wyświetlana jest lista izolacji portów. Kliknij  **Edit**, aby skonfigurować izolację portów na następnej stronie.

Rys. 3-2 Izolacja portów

Port Isolation Config

---

**Port**

UNIT1
LAGS

Select All
 

1

2

3

4

5

6

7

8

9

10

Selected
  Unselected
  Not Available

---

**Forwarding Port List**

UNIT1
LAGS

Select All
 

1

2

3

4

5

6

7

8

9

10

Selected
  Unselected
  Not Available

Cancel

Apply

Wykonaj poniższe kroki, aby skonfigurować izolację portów:

- 1) W sekcji **Port** wybierz jeden lub wiele portów, które będą izolowane.
- 2) W sekcji **Forwarding Port List** wybierz porty przekazujące lub porty LAG, z którymi izolowane porty będą mogły się komunikować. Można wybrać więcej niż jeden port.
- 3) Kliknij **Apply**.

## 3.2 Przez CLI

Wykonaj poniższe kroki, aby skonfigurować izolację portów:

---

Krok 1      **configure**  
Uruchom tryb konfiguracji globalnej.

---

Configuration Guide ■ 80

|        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Krok 2 | <p><b>interface { fastEthernet <i>port</i>   range fastEthernet <i>port-list</i>   gigabitEthernet <i>port</i>   range gigabitEthernet <i>port-list</i>   ten-gigabitEthernet <i>port</i>   ten-range gigabitEthernet <i>port-list</i>   port-channel <i>port-channel</i>   range port-channel <i>port-channel-list</i> }</b></p> <p>Wybierz izolowany port i wejdź w tryb konfiguracji interfejsu.</p>                                                                         |
| Krok 3 | <p><b>port isolation { [fa-forward-list <i>fa-forward-list</i>] [gi-forward-list <i>gi-forward-list</i>] [te-forward-list <i>te-forward-list</i>] [ po-forward-list <i>po-forward-list</i> ] }</b></p> <p>Dodaj porty lub LAG do listy Forwarding Port List izolowanego portu. Można dodać wiele portów.</p> <p><i>fa-forward-list / gi-forward-list / te-forward-list</i>: Określ przesyłające porty Ethernet.<br/> <i>po-forward-list</i>: Określ przesyłające porty LAG.</p> |
| Krok 4 | <p><b>show port isolation interface { fastEthernet <i>port</i>   gigabitEthernet <i>port</i>   ten-gigabitEthernet <i>port</i>   port-channel <i>port-channel</i> }</b></p> <p>Sprawdź konfigurację izolacji wyznaczonych portów.</p>                                                                                                                                                                                                                                           |
| Krok 5 | <p><b>end</b></p> <p>Wróć do trybu privileged EXEC.</p>                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Krok 6 | <p><b>copy running-config startup-config</b></p> <p>Zapisz ustawienia w pliku konfiguracyjnym.</p>                                                                                                                                                                                                                                                                                                                                                                              |

Poniższy przykład prezentuje, jak dodać porty 1/0/1-3 i LAG 4 do listy przekierowywania portu 1/0/5:

**Switch#configure**

**Switch(config)#interface gigabitEthernet 1/0/5**

**Switch(config-if)#port isolation gi-forward-list 1/0/1-3 po-forward-list 4**

**Switch(config-if)#show port isolation interface gigabitEthernet 1/0/5**

| Port    | LAG | Forward-List  |
|---------|-----|---------------|
| ----    | --- | -----         |
| Gi1/0/5 | N/A | Gi1/0/1-3,Po4 |

**Switch(config-if)#end**

**Switch#copy running-config startup-config**



# 4 Konfiguracja funkcji Loopback Detection

## 4.1 Przez GUI

W celu uniknięcia burzy broadcastowej przed włączeniem funkcji loopback detection zalecamy włączenie funkcji storm control. Szczegółowe informacje dotyczące funkcji storm control znajdziesz w części *Konfiguracja QoS*.

Wybierz z menu **L2 FEATURES > Switching > Port > Loopback Detection**, aby wyświetlić poniższą stronę.

Rys. 4-1 Konfiguracja funkcji Loopback Detection

### Loopback Detection

Loopback Detection Status:  Enable

Detection Interval:  seconds (1-1000)

Auto-recovery Time:  seconds (2-100,000)

Web Refresh Status:  Enable

Web Refresh Interval:  seconds (3-100)

Apply

### Port Config

UNIT1
LAGS

↻ Recovery

| <input type="checkbox"/>            | Port   | Status   | Operation Mode | Recovery Mode | Loop Status | Block Status | Block VLAN | LAG |
|-------------------------------------|--------|----------|----------------|---------------|-------------|--------------|------------|-----|
| <input checked="" type="checkbox"/> | 1/0/1  | Disabled | Alert          | Auto          | ---         | ---          | --         | --- |
| <input type="checkbox"/>            | 1/0/2  | Disabled | Alert          | Auto          | ---         | ---          | --         | --- |
| <input type="checkbox"/>            | 1/0/3  | Disabled | Alert          | Auto          | ---         | ---          | --         | --- |
| <input type="checkbox"/>            | 1/0/4  | Disabled | Alert          | Auto          | ---         | ---          | --         | --- |
| <input type="checkbox"/>            | 1/0/5  | Disabled | Alert          | Auto          | ---         | ---          | --         | --- |
| <input type="checkbox"/>            | 1/0/6  | Disabled | Alert          | Auto          | ---         | ---          | --         | --- |
| <input type="checkbox"/>            | 1/0/7  | Disabled | Alert          | Auto          | ---         | ---          | --         | --- |
| <input type="checkbox"/>            | 1/0/8  | Disabled | Alert          | Auto          | ---         | ---          | --         | --- |
| <input type="checkbox"/>            | 1/0/9  | Disabled | Alert          | Auto          | ---         | ---          | --         | --- |
| <input type="checkbox"/>            | 1/0/10 | Disabled | Alert          | Auto          | ---         | ---          | --         | --- |

Total: 28
1 entry selected.

Cancel
Apply

Wykonaj poniższe kroki, aby skonfigurować funkcję Loopback Detection:

- 1) W sekcji **Loopback Detection** włącz funkcję loopback detection i skonfiguruj parametry globalne, następnie kliknij **Apply**.

|                           |                                                                                                                                                                                                                                                           |
|---------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Loopback Detection Status | Włącz funkcję Loopback Detection globalnie.                                                                                                                                                                                                               |
| Detection Interval        | Ustaw odstęp między wysyłaniem pakietów wykrywania pętli zwrotnych (loopback detection), w sekundach.<br><br>Wartość musi zawierać się w zakresie od 1 do 1000, wartość domyślna to 30.                                                                   |
| Auto-recovery Time        | Skonfiguruj globalnie czas przywracania. Zablokowany port w trybie Auto Recovery zostanie automatycznie przywrócony do normalnego stanu po wygaśnięciu czasu automatycznego przywracania. Wartość może wynosić od 2 do 100,000 s, wartość domyślna to 90. |
| Web Refresh Status        | Przy włączonej funkcji przełącznik będzie w odpowiednim momencie odświeżał sieć. Funkcja jest domyślnie wyłączona.                                                                                                                                        |
| Web Refresh Interval      | Jeżeli opcja Web Refresh Status jest włączona, ustaw odstęp odświeżania, między 3 a 100 s. Wartość domyślna to 6 s.                                                                                                                                       |

- 2) W sekcji **Port Config** wybierz co najmniej jeden port do konfiguracji parametrów wykrywania pętli zwrotnych. Kliknij **Apply**.

|                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Status         | Włącz funkcję Loopback Detection dla portu.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Operation Mode | Po wykryciu pętli zwrotnej na porcie wybierz tryb działania:<br><br><b>Alert:</b> Stan Loop poinformuje, czy na odpowiadającym porcie wykryto pętlę. Jest to ustawienie domyślne.<br><br><b>Port Based:</b> Poza wyświetlaniem ostrzeżeń przełącznik zablokuje również port, na którym wykryto pętlę.<br><br><b>VLAN-Based:</b> Jeżeli wykryto pętlę w sieci VLAN portu, przełącznik wyświetli ostrzeżenia, jak również zablokuje daną sieć VLAN. Ruch z innych sieci VLAN może być w dalszym ciągu normalnie przekierowywany przez port. |
| Recovery Mode  | Jeżeli wybierzesz tryb działania <b>Port Based</b> lub <b>VLAN-Based</b> , musisz również skonfigurować tryb odzyskiwania dla zablokowanego portu:<br><br><b>Auto:</b> Po wygaśnięciu czasu automatycznego odzyskiwania zablokowany port będzie automatycznie przywracany do stanu normalnego. Jest to ustawienie domyślne.<br><br><b>Manual:</b> Wymagane jest ręczne zwolnienie zablokowanego portu. Kliknij <b>Recovery</b> , aby zwolnić wybrany port.                                                                                |

- 3) Sprawdź dane funkcji Loopback Detection (opcjonalnie).

|              |                                        |
|--------------|----------------------------------------|
| Loop Status  | Pokazuje, czy na porcie wykryto pętlę. |
| Block Status | Pokazuje, czy port jest zablokowany.   |
| Block VLAN   | Pokazuje zablokowane sieci VLAN.       |

## 4.2 Przez CLI

Wykonaj poniższe kroki, aby skonfigurować funkcję Loopback Detection:

|        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Krok 1 | <b>configure</b><br>Uruchom tryb konfiguracji globalnej..                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Krok 2 | <b>loopback-detection</b><br>Włącz funkcję Loopback Detection globalnie. Domyślnie funkcja jest wyłączona.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Krok 3 | <b>loopback-detection interval <i>interval-time</i></b><br>Ustaw odstęp wysyłania pakietów wykrywania pętli zwrotnych, aby umożliwić wykrycie pętli w sieci.<br><i>interval-time</i> : Odstęp czasu, w jakim wysyłane są pakiety wykrywania pętli. Wartość może wynosić od 1 do 1000 s. Wartość domyślna to 30 s.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Krok 4 | <b>loopback-detection recovery-time <i>recovery-time</i></b><br>Ustaw czas automatycznego przywracania, po którym zablokowany port w trybie Auto Recovery może automatycznie powrócić do stanu normalnego.<br><i>recovery-time</i> : Ustaw interwał wykrywania na czas między 2 a 100,000 s. Wartość domyślna to 90.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Krok 5 | <b>interface { fastEthernet <i>port</i>   range fastEthernet <i>port-list</i>   gigabitEthernet <i>port</i>   range gigabitEthernet <i>port-list</i>   ten-gigabitEthernet <i>port</i>   ten-range gigabitEthernet <i>port-list</i>   port-channel <i>port-channel</i>   range port-channel <i>port-channel-list</i> }</b><br>Uruchom tryb konfiguracji interfejsu.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Krok 6 | <b>loopback-detection</b><br>Włącz funkcję Loopback Detection dla portu. Domyślnie funkcja jest wyłączona.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Krok 7 | <b>loopback-detection config process-mode { alert   port-based   vlan-based } recovery-mode { auto   manual }</b><br>Ustaw tryb przetwarzania na wypadek wykrycia na porcie pętli zwrotnej. Dostępne są trzy tryby.<br><br><i>alert</i> : Po wykryciu pętli zwrotnej przełącznik jedynie wyświetli ostrzeżenia. Jest to ustawienie domyślne.<br><br><i>port-based</i> : Przełącznik wyświetli ostrzeżenia i zablokuje port, na którym wykryto pętlę.<br><br><i>vlan-based</i> : Przełącznik wyświetli ostrzeżenia i zablokuje VLAN portom, na którym wykryto pętlę.<br><br>Ustaw tryb odzyskiwania dla zablokowanego portu. Dostępne są dwa tryby.<br><br><i>auto</i> : Po wygaśnięciu czasu automatycznego odzyskiwania zablokowany port będzie automatycznie przywracany do stanu normalnego i na nowo zacznie wykrywać pętlę w sieci.<br><br><i>manual</i> : Wymagane jest ręczne zwolnienie zablokowanego portu. Aby przywrócić wybrany port, możesz użyć polecenia 'loopback-detection recover'. |
| Krok 8 | <b>show loopback-detection global</b><br>Sprawdź konfigurację globalną funkcji Loopback Detection.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |

|         |                                                                                                                                                                                                                                                 |
|---------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Krok 9  | <b>show loopback-detection interface { fastEthernet <i>port</i>   gigabitEthernet <i>port</i>   ten-gigabitEthernet <i>port</i>   port-channel <i>port-channel</i> }</b><br>Sprawdź konfigurację funkcji Loopback Detection na wybranym porcie. |
| Krok 10 | <b>end</b><br>Powróć do trybu privileged EXEC.                                                                                                                                                                                                  |
| Krok 11 | <b>copy running-config startup-config</b><br>Zapisz ustawienia w pliku konfiguracyjnym.                                                                                                                                                         |

Poniższy przykład przedstawia, jak włączyć funkcję Loopback Detection globalnie (zachowaj parametry domyślne):

**Switch#configure**

**Switch(config)#loopback-detection**

**Switch(config)#show loopback-detection global**

Loopback detection global status : enable

Loopback detection interval : 30s

Loopback detection recovery time : 3 intervals

**Switch(config-if)#end**

**Switch#copy running-config startup-config**

Poniższy przykład prezentuje, jak włączyć funkcję Loopback Detection dla portu 1/0/3, ustawić tryb przetwarzania na alert i tryb odzyskiwania na auto:

**Switch#configure**

**Switch(config)#interface gigabitEthernet 1/0/3**

**Switch(config-if)#loopback-detection**

**Switch(config-if)#loopback-detection config process-mode alert recovery-mode auto**

**Switch(config-if)#show loopback-detection interface gigabitEthernet 1/0/3**

| Port    | Enable | Process Mode | Recovery Mode | Loopback | Block | LAG  |
|---------|--------|--------------|---------------|----------|-------|------|
| ----    | -----  | -----        | -----         | -----    | ----- | ---- |
| Gi1/0/3 | enable | alert        | auto          | N/A      | N/A   | N/A  |

**Switch(config-if)#end**

**Switch#copy running-config startup-config**

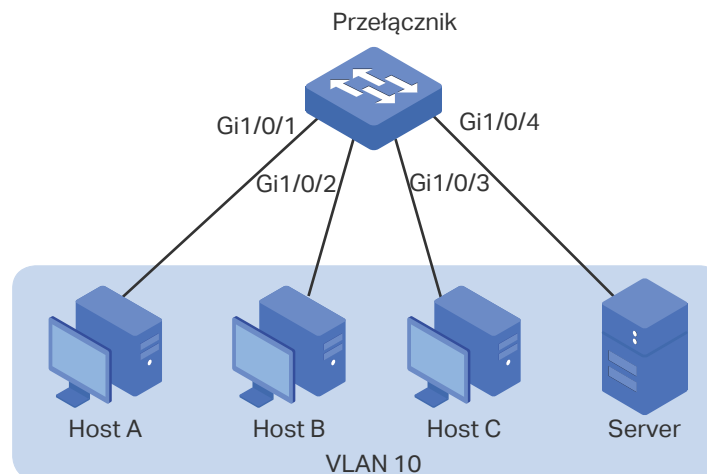
# 5 Przykłady konfiguracji

## 5.1 Przykładowa konfiguracja izolacji portu

### 5.1.1 Wymagania sieciowe

Jak pokazano na poniższym schemacie, z przełącznikiem, w ramach sieci VLAN 10, połączone są trzy hosty oraz serwer. Bez zmiany ustawień sieci VLAN Host A nie ma zezwolenia na komunikację z innymi hostami, może się komunikować wyłącznie z serwerem, nawet jeśli zmieni się adres MAC lub adres IP Hosta A.

Rys. 5-1 Topologia sieci



### 5.1.2 Schemat konfiguracji

Aby spełnić ten warunek, należy skonfigurować funkcję izolacji portów. Ustaw port 1/0/4 jako jedyny port przekazujący do portu 1/0/1, co uniemożliwi Hostowi A przekazywanie pakietów do innych hostów.

Ponieważ komunikacja jest dwukierunkowa, jeśli chcesz, aby Host A i serwer komunikowały się normalnie, musisz również ustawić port 1/0/1 jako port przekazujący do 1/0/4.

W poniższych podrozdziałach opisano dwa sposoby przeprowadzenia procedury konfiguracji: przez GUI oraz przez CLI.

### 5.1.3 Przez GUI

- 1) Wybierz z menu **L2 FEATURES > Switching > Port > Port Isolation**, aby wyświetlić poniższą stronę. Pokaże się lista izolacji portów.

Rys. 5-2 Lista izolacji portów

| Port Isolation Config                         |     |                      |  |
|-----------------------------------------------|-----|----------------------|--|
| UNIT1 <span style="float: right;">Edit</span> |     |                      |  |
| Port                                          | LAG | Forwarding Port List |  |
| 1/0/1                                         | --  | 1/0/1-10,LAG1-8      |  |
| 1/0/2                                         | --  | 1/0/1-10,LAG1-8      |  |
| 1/0/3                                         | --  | 1/0/1-10,LAG1-8      |  |
| 1/0/4                                         | --  | 1/0/1-10,LAG1-8      |  |
| 1/0/5                                         | --  | 1/0/1-10,LAG1-8      |  |
| 1/0/6                                         | --  | 1/0/1-10,LAG1-8      |  |
| 1/0/7                                         | --  | 1/0/1-10,LAG1-8      |  |
| 1/0/8                                         | --  | 1/0/1-10,LAG1-8      |  |
| 1/0/9                                         | --  | 1/0/1-10,LAG1-8      |  |
| 1/0/10                                        | --  | 1/0/1-10,LAG1-8      |  |

Total: 10

- 2) Kliknij na powyższej stronie **Edit**, aby wyświetlić poniższą stronę. Ustaw port 1/0/1 jako port izolowany, a port 1/0/4 jako port przekazujący. Kliknij **Apply**.

Rys. 5-3 Konfiguracja funkcji izolacji portów

Port Isolation Config

**Port**

Select All

UNIT1

LAGS

Selected

Unselected

Not Available

**Forwarding Port List**

Select All

UNIT1

LAGS

Selected

Unselected

Not Available

Cancel

Apply

- 3) Ustaw port 1/0/4 jako port izolowany i port 1/0/1 jako port przekazujący. Kliknij **Apply**.

Rys. 5-4 Konfiguracja funkcji izolacji portów

Port Isolation Config

**Port**

---

Select All

UNIT1

1

2

3

4

5

6

7

8

LAGS

9

10

Selected

Unselected

Not Available

---

**Forwarding Port List**

Select All

UNIT1

1

2

3

4

5

6

7

8

LAGS

9

10

Selected

Unselected

Not Available

Cancel

Apply

- 4) Kliknij Save, aby zapisać ustawienia.

## 5.1.4 Przez CLI

```
Switch#configure
Switch(config)#interface gigabitEthernet 1/0/1
Switch(config-if)#port isolation gi-forward-list 1/0/4
Switch(config-if)#exit
Switch(config)#interface gigabitEthernet 1/0/4
Switch(config-if)#port isolation gi-forward-list 1/0/1
Switch(config-if)#end
Switch#copy running-config startup-config
```

## Sprawdzanie konfiguracji

```
Switch#show port isolation interface
```

| Port    | LAG | Forward-List     |
|---------|-----|------------------|
| ----    | --- | -----            |
| Gi1/0/1 | N/A | Gi1/0/4          |
| Gi1/0/2 | N/A | Gi1/0/1-10,Po1-8 |
| Gi1/0/3 | N/A | Gi1/0/1-10,Po1-8 |
| Gi1/0/4 | N/A | Gi1/0/1          |
| .....   |     |                  |

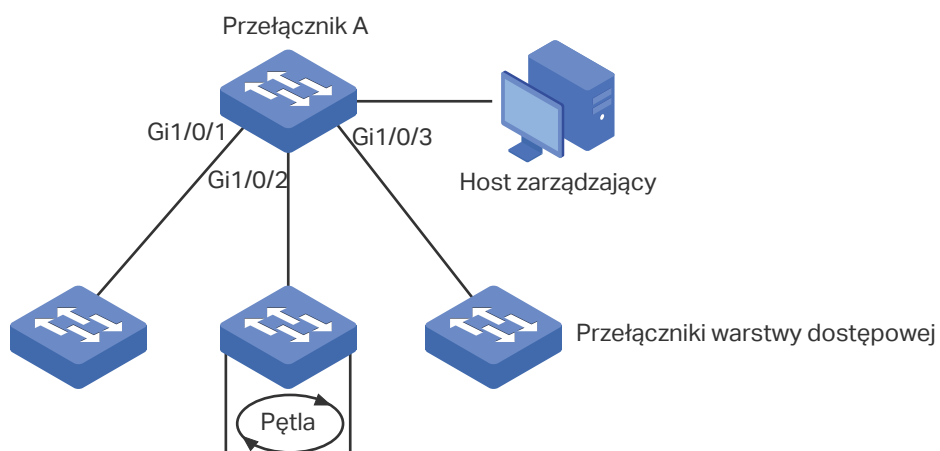
## 5.2 Przykładowa konfiguracja funkcji Loopback Detection

### 5.2.1 Wymagania sieciowe

Jak pokazano na poniższym schemacie, przełącznik A to przełącznik warstwy konwergencji, łączący się z kilkoma przełącznikami warstwy dostępowej. W wyniku pojawienia się nieprawidłowości w działaniu przełącznika warstwy dostępowej tworzą się pętle. Pojawienie się pętli na przełączniku warstwy dostępowej prowadzi do występowania burz broadcastowych na przełączniku A lub nawet w całej sieci, co powoduje nadmierny ruch i zmniejszenie wydajności sieci.

W celu zmniejszenia negatywnych skutków burz broadcastowych użytkownicy mogą wykrywać pętle w sieci poprzez przełącznik A oraz okresowo blokować porty, na których wykryta zostanie pętla.

Rys. 5-5 Topologia sieci





## 5.2.2 Schemat konfiguracji

Włącz funkcję loopback detection na portach 1/0/1-3 i skonfiguruj SNMP, aby otrzymywać powiadomienia w formie komunikatów trap. Szczegółowe informacje o SNMP znajdują się w części *Konfiguracja SNMP*. W tym rozdziale omawiamy jak skonfigurować funkcję loopback detection i monitorować wyniki wykrywania poprzez interfejs zarządzania przełącznika.

W poniższych podrozdziałach opisano dwa sposoby przeprowadzenia procedury konfiguracji: przez GUI oraz przez CLI.

### 5.2.3 Przez GUI

- 1) Wybierz z menu **L2 FEATURES > Switching > Port > Loopback Detection**, aby wyświetlić stronę konfiguracji.
- 2) W części **Loopback Detection** włącz funkcję loopback detection oraz globalnie uruchom web refresh. Pozostałe parametry pozostaw bez zmian i kliknij **Apply**.

Rys. 5-6 Konfiguracja globalna

| Loopback Detection                   |                                                     |
|--------------------------------------|-----------------------------------------------------|
| Loopback Detection Status:           | <input checked="" type="checkbox"/> Enable          |
| Detection Interval:                  | <input type="text" value="20"/> seconds (1-1000)    |
| Auto-recovery Time:                  | <input type="text" value="90"/> seconds (2-100,000) |
| Web Refresh Status:                  | <input checked="" type="checkbox"/> Enable          |
| Web Refresh Interval:                | <input type="text" value="6"/> seconds (3-100)      |
| <input type="button" value="Apply"/> |                                                     |

- 3) W części **Port Config** włącz porty 1/0/1-3, ustaw operation mode jako **Port-Based**, aby port był blokowany po wykryciu pętli oraz pozostaw recovery mode na ustawieniu **Auto**, aby port był automatycznie przywracany do stanu normalnego po upływie czasu automatycznego przywracania. Kliknij **Apply**.

Rys. 5-7 Konfiguracja portów

Port Config

UNIT1 LAGS Recovery

| <input type="checkbox"/>            | Port   | Status   | Operation Mode | Recovery Mode | Loop Status | Block Status | Block VLAN | LAG |
|-------------------------------------|--------|----------|----------------|---------------|-------------|--------------|------------|-----|
| <input checked="" type="checkbox"/> | 1/0/1  | Enabled  | Port Based     | Auto          | ---         | ---          | --         | --- |
| <input checked="" type="checkbox"/> | 1/0/2  | Enabled  | Port Based     | Auto          | ---         | ---          | --         | --- |
| <input checked="" type="checkbox"/> | 1/0/3  | Enabled  | Port Based     | Auto          | ---         | ---          | --         | --- |
| <input type="checkbox"/>            | 1/0/4  | Disabled | Alert          | Auto          | ---         | ---          | --         | --- |
| <input type="checkbox"/>            | 1/0/5  | Disabled | Alert          | Auto          | ---         | ---          | --         | --- |
| <input type="checkbox"/>            | 1/0/6  | Disabled | Alert          | Auto          | ---         | ---          | --         | --- |
| <input type="checkbox"/>            | 1/0/7  | Disabled | Alert          | Auto          | ---         | ---          | --         | --- |
| <input type="checkbox"/>            | 1/0/8  | Disabled | Alert          | Auto          | ---         | ---          | --         | --- |
| <input type="checkbox"/>            | 1/0/9  | Disabled | Alert          | Auto          | ---         | ---          | --         | --- |
| <input type="checkbox"/>            | 1/0/10 | Disabled | Alert          | Auto          | ---         | ---          | --         | --- |

Total: 10 3 entries selected. Cancel **Apply**

- 4) Na powyższej stronie możesz sprawdzić wyniki wykrywania. Diagnoza dla **Loop status** oraz **Block status** wyświetla się odpowiednio po prawej stronie każdego z portów.

## 5.2.4 Przez CLI

- 1) Włącz globalnie funkcję loopback detection i skonfiguruj detection interval oraz recovery time.

```
Switch#configure
```

```
Switch(config)#loopback-detection
```

```
Switch(config)#loopback-detection interval 30
```

```
Switch(config)#loopback-detection recovery-time 3
```

- 2) Włącz funkcję loopback detection na portach 1/0/1-3 i ustaw process mode oraz recovery mode.

```
Switch(config)#interface range gigabitEthernet 1/0/1-3
```

```
Switch(config-if-range)#loopback-detection
```

```
Switch(config-if-range)#loopback-detection config process-mode port-based
recovery-mode auto
```

```
Switch(config-if-range)#end
```

```
Switch#copy running-config startup-config
```

## Sprawdzanie konfiguracji

Sprawdź konfigurację globalną:

```
Switch#show loopback-detection global
Loopback detection global status : enable
Loopback detection interval: 30 s
Loopback detection recovery time : 90 s
```

Sprawdź konfigurację funkcji loopback detection na portach:

```
Switch#show loopback-detection interface
```

| Port    | Enable | Process Mode | Recovery Mode | Loopback | Block | LAG |
|---------|--------|--------------|---------------|----------|-------|-----|
| Gi1/0/1 | enable | port-based   | auto          | N/A      | N/A   | N/A |
| Gi1/0/2 | enable | port-based   | auto          | N/A      | N/A   | N/A |
| Gi1/0/3 | enable | port-based   | auto          | N/A      | N/A   | N/A |

# Część 4

## Konfiguracja LAG

### ROZDZIAŁY

1. Grupy agregacji łączy (LAG)
2. Konfiguracja LAG
3. Przykład konfiguracji

# 1 Grupy agregacji łączy (LAG)

## 1.1 Informacje ogólne

Funkcja LAG (Link Aggregation Group) umożliwia połączenie ze sobą wielu portów fizycznych przełącznika w jedną logiczną całość, co pozwala uzyskać większą przepustowość oraz niezawodność połączeń.

## 1.2 Obsługiwane funkcje

Funkcję LAG można skonfigurować na dwa sposoby: jako statyczne LAG i dynamiczne LACP (Link Aggregation Control Protocol).

### Statyczne LAG

Porty muszą być dodawane ręcznie do LAG.

### LACP

Przełącznik korzysta z protokołu LACP, aby wdrożyć dynamiczną agregację i dezagregację łączy poprzez wymianę pakietów LACP z urządzeniem równorzędnym. Protokół LACP zwiększa elastyczność konfiguracji LAG.

## 2 Konfiguracja LAG

Aby przeprowadzić proces konfiguracji LAG, wykonaj poniższe kroki:

- 1) Skonfiguruj globalny algorytm równoważenia obciążenia pasma.
- 2) Skonfiguruj statyczne LAG lub LACP.

### Wskazówki dotyczące konfiguracji

- Upewnij się, że obie strony łącza agregacji pracują w tym samym trybie LAG. Np., jeżeli lokalna strona pracuje w trybie LACP, urządzenie równorzędne też musi mieć ustawiony tryb LACP.
- Upewnij się, że urządzenia po obu stronach łącza agregacji korzystają z tych samych numerów portów fizycznych, o tych samych prędkościach, trybie duplexu, ramce jumbo i kontroli przepływu.
- Jeden port może być jednocześnie dodany do więcej niż jednego łącza agregacji.
- LACP nie obsługuje połączeń w trybie półduplexu.
- Jedno statyczne LAG obsługuje do 8 portów. Wszystkie te porty korzystają po równo z dostępnej przepustowości. Jeżeli aktywne łącze napotka błąd, pozostałe aktywne łącza dzielą przepustowość równomiernie.
- Jedno LACP LAG obsługuje wiele portów, ale tylko osiem z nich może działać w tym samym czasie. Pozostałe porty są portami alternatywnymi. Korzystając z protokołu LACP, przełączniki negocjują parametry i wybierają porty pracujące. Gdy na pracującym porcie wystąpi błąd, port alternatywny o najwyższym priorytecie zastępuje go i rozpoczyna przesyłanie danych.
- Dla funkcji takich jak IGMP Snooping, 802.1Q VLAN, MAC VLAN, protokół VLAN, VLAN-VPN, GVRP, Voice VLAN, STP, QoS, DHCP Snooping i kontrola przepustowości, port LAG korzysta z konfiguracji LAG, a nie z ustawień własnych. Konfiguracja portu obowiązuje dopiero po opuszczeniu LAG.
- Port uruchomiony poprzez Port Security, Port Mirror, filtrowanie adresów MAC lub 802.1X nie może być dodany do LAG, a port LAG nie może być uruchomiony za pomocą tych funkcji.

## 2.1 Przez GUI

### 2.1.1 Konfiguracja algorytmu równoważenia obciążenia pasma

Wybierz z menu **L2 FEATURES > Switching > LAG > LAG Table**, aby wyświetlić poniższą stronę.

Rys. 2-1 Konfiguracja globalna

Global Config

Hash Algorithm: SRC MAC+DST MAC

Apply

LAG Table

| <input type="checkbox"/> | Group ID | Description | Members | Operation |
|--------------------------|----------|-------------|---------|-----------|
| <input type="checkbox"/> | 1        | Active LACP | --      |           |

Total: 1

W sekcji **Global Config** wybierz algorytm równoważenia obciążenia pasma (Hash Algorithm) i kliknij **Apply**.

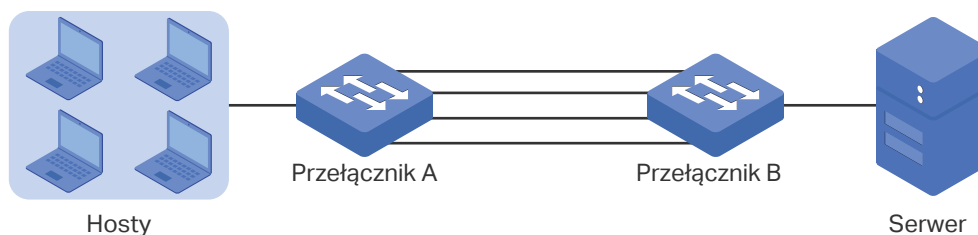
|                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Hash Algorithm</b> | <p>Wybierz algorytm Hash, aby przełącznik mógł wybierać porty do przesyłania odebranych pakietów. W ten sposób przepływ danych jest równomierny, a obciążenie pasma zrównoważone. Do wyboru są trzy możliwości:</p> <p><b>SRC MAC:</b> Obliczenia są oparte na źródłowych adresach MAC pakietów.</p> <p><b>DST MAC:</b> Obliczenia są oparte na docelowych adresach MAC pakietów.</p> <p><b>SRC MAC+DST MAC:</b> Obliczenia są oparte na źródłowych i docelowych adresach MAC pakietów.</p> <p><b>SRC IP:</b> Obliczenia są oparte na źródłowych adresach IP pakietów.</p> <p><b>DST IP:</b> Obliczenia są oparte na docelowych adresach IP pakietów.</p> <p><b>SRC IP+DST IP:</b> Obliczenia są oparte na źródłowych i docelowych adresach IP pakietów.</p> |
|-----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

#### Wskazówki:

- Algorytm równoważenia obciążenia pasma obowiązuje tylko dla ruchu wychodzącego. Jeżeli strumień danych nie jest dobrze współdzielony przez łącza, zmień algorytm interfejsu wychodzącego.
- Wybierz prawidłowy algorytm równoważenia obciążenia, aby uniknąć przesyłania strumienia danych tylko na jednym fizycznym łączu. Np. gdy przełącznik A odbiera pakiety od kilku hostów i przesyła je do serwera ze stałym adresem MAC,

ustaw algorytm jako "SRC MAC", aby umożliwić przełącznikowi A wybranie portu przesyłającego w oparciu o źródłowy adres MAC odebranych pakietów.

Rys. 2-2 Konfiguracja algorytmu Hash



## 2.1.2 Konfiguracja trybu statycznego LAG lub LACP

Dla jednego portu można wybrać tylko jeden tryb LAG: statyczny LAG lub LACP. Upewnij się, że obie strony łącza korzystają z tego samego trybu LAG.

### ■ Konfiguracja do statycznego LAG

Wybierz z menu **L2 FEATURES > Switching > LAG > Static LAG**, aby wyświetlić poniższą stronę.

Rys. 2-3 Statyczny LAG

**LAG Config**

---

Group ID:

Description: --

Port:  (Format: 1/0/1, input or choose below)

UNIT1

Selected

Unselected

Not Available

Wykonaj poniższe kroki, aby skonfigurować statyczny LAG:

1) Wybierz LAG do konfiguracji.

|             |                                                 |
|-------------|-------------------------------------------------|
| Group ID    | Wybierz LAG do konfiguracji jako statyczny LAG. |
| Description | Tryb LAG.                                       |

2) Wybierz porty LAG. Jest tutaj wiele opcji.

3) Kliknij **Apply**.



 **Uwaga:**

Usunięcie wszystkich portów spowoduje usunięcie LAG..

■ **Konfiguracja do LACP**

Wybierz z menu **L2 FEATURES > Switching > LAG > LACP**, aby wyświetlić poniższą stronę.

Rys. 2-4 Konfiguracja LACP

Global Config

---

System Priority:  (0-65535) Apply

LACP Config

UNIT1

| <input type="checkbox"/> | Port   | Status   | Group ID | Port Priority | Mode    | LAG |
|--------------------------|--------|----------|----------|---------------|---------|-----|
| <input type="checkbox"/> | 1/0/1  | Disabled | 0        | 32768         | Passive | --- |
| <input type="checkbox"/> | 1/0/2  | Disabled | 0        | 32768         | Passive | --- |
| <input type="checkbox"/> | 1/0/3  | Disabled | 0        | 32768         | Passive | --- |
| <input type="checkbox"/> | 1/0/4  | Disabled | 0        | 32768         | Passive | --- |
| <input type="checkbox"/> | 1/0/5  | Disabled | 0        | 32768         | Passive | --- |
| <input type="checkbox"/> | 1/0/6  | Disabled | 0        | 32768         | Passive | --- |
| <input type="checkbox"/> | 1/0/7  | Disabled | 0        | 32768         | Passive | --- |
| <input type="checkbox"/> | 1/0/8  | Disabled | 0        | 32768         | Passive | --- |
| <input type="checkbox"/> | 1/0/9  | Disabled | 0        | 32768         | Passive | --- |
| <input type="checkbox"/> | 1/0/10 | Disabled | 0        | 32768         | Passive | --- |

Total: 10

Wykonaj poniższe kroki, aby skonfigurować LACP:

1) Określ priorytety dla przełącznika i kliknij **Apply**.

**System Priority**

Określ priorytety dla przełącznika, pamiętając, że im mniejsza wartość, tym wyższy priorytet.

Aby zachować zgodność portów po obu stronach, priorytet jednego urządzenia może być wyższy niż priorytet drugiego urządzenia. Urządzenie o wyższym priorytecie określi porty aktywne, a drugie urządzenie wybierze porty aktywne spośród portów zidentyfikowanych przez urządzenie pierwsze. Jeżeli obie strony mają tę samą wartość priorytetu, urządzenie o niższym adresie MAC uznawane jest za urządzenie o wyższym priorytecie.

2) Wybierz porty LAG i skonfiguruj odpowiednie parametry. Kliknij **Apply**.

|                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Group ID                | <p>Podaj grupowe ID LAG. Pamiętaj, że nie możesz tutaj wpisać grupowego ID innego statycznego LAG.</p> <p>Prawidłowa wartość grupowego ID zależy od maksymalnej liczby LAG obsługiwanych przez przełącznik. Np. jeżeli przełącznik obsługuje do 14 LAG, prawidłowa wartość waha się od 1 do 14.</p>                                                                                                                                                                                                                                    |
| Port Priority (0-65535) | <p>Określ priorytety portów, pamiętając, że im niższa wartość, tym wyższy priorytet.</p> <p>Port o wyższym priorytecie w LAG zostanie wybrany jako port aktywny do przesyłu danych. Maksymalnie 8 portów może pracować w tym samym czasie. Jeżeli dwa porty mają tę samą wartość priorytetu, port o niższym numerze poru uznawany jest za port o wyższym priorytecie.</p>                                                                                                                                                              |
| Mode                    | <p>Wybierz tryb LACP dla portu.</p> <p>W trybie LACP przełącznik korzysta z LACPDU (Link Aggregation Control Protocol Data Unit) do negocjacji parametrów z urządzeniem równorzędnym. W ten sposób obie strony wybierają porty aktywne i tworzą łącze agregacji. W trybie LACP można ustalić czy dany port ma służyć do przesyłu LACPDU. Do wyboru są dwa tryby:</p> <p><b>Passive:</b> Port prześle LACPDU przed odebraniem LACPDU od urządzenia równorzędnego.</p> <p><b>Active:</b> Port podejmie inicjatywę przesłania LACPDU.</p> |
| Status                  | <p>Włącz funkcję LACP portu. Domyślnie ta funkcja jest wyłączona.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |

## 2.2 Przez CLI

### 2.2.1 Konfiguracja algorytmu równoważenia obciążenia pasma

Wykonaj poniższe kroki, aby skonfigurować algorytm równoważenia obciążenia pasma:

|        |                                                                     |
|--------|---------------------------------------------------------------------|
| Krok 1 | <p><b>configure</b></p> <p>Uruchom tryb konfiguracji globalnej.</p> |
|--------|---------------------------------------------------------------------|

|        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Krok 2 | <p><b>port-channel load-balance { src-mac   dst-mac   src-dst-mac   src-ip   dst-ip   src-dst-ip }</b></p> <p>Wybierz algorytm Hash, aby przełącznik mógł wybierać porty do przesyłania odebranych pakietów. W ten sposób przepływ danych jest równomierny, a obciążenie pasma zrównoważone. Do wyboru są trzy możliwości.</p> <p><b>src-mac:</b> Obliczenia są oparte na źródłowych adresach MAC pakietów.</p> <p><b>dst-mac:</b> Obliczenia są oparte na docelowych adresach MAC pakietów.</p> <p><b>src-dst-mac:</b> Obliczenia są oparte na źródłowych i docelowych adresach MAC pakietów.</p> <p><b>src-ip:</b> Obliczenia są oparte na źródłowych adresach IP pakietów.</p> <p><b>dst-ip:</b> Obliczenia są oparte na docelowych adresach IP pakietów.</p> <p><b>src-dst-ip:</b> Obliczenia są oparte na źródłowych i docelowych adresach IP pakietów.</p> |
| Krok 3 | <p><b>show etherchannel load-balance</b></p> <p>Zweryfikuj konfigurację algorytmu równoważenia obciążenia pasma.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Krok 4 | <p><b>end</b></p> <p>Powrót do trybu privileged EXEC.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Krok 5 | <p><b>copy running-config startup-config</b></p> <p>Zapisz ustawienia w pliku konfiguracyjnym.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |

Poniższy schemat przedstawia przykładowy sposób ustawiania trybu globalnego równoważenia obciążenia pasma jako src-dst-mac:

**Switch#configure**

**Switch(config)#port-channel load-balance src-dst-mac**

**Switch(config)#show etherchannel load-balance**

EtherChannel Load-Balancing Configuration: src-dst-mac

EtherChannel Load-Balancing Addresses Used Per-Protocol:

Non-IP: Source XOR Destination MAC address

IPv4: Source XOR Destination MAC address

IPv6: Source XOR Destination MAC address

**Switch(config)#end**

**Switch#copy running-config startup-config**

## 2.2.2 Konfiguracja trybu statycznego LAG lub LACP

Dla jednego portu można wybrać tylko jeden tryb LAG: statyczny LAG lub LACP. Upewnij się, że obie strony łącza korzystają z tego samego trybu LAG.

## ■ Konfiguracja statycznego LAG

Wykonaj poniższe kroki, aby skonfigurować tryb statycznego LAG:

|        |                                                                                                                                                                                                                                                                                   |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Krok 1 | <b>configure</b><br>Uruchom tryb konfiguracji globalnej.                                                                                                                                                                                                                          |
| Krok 2 | <b>interface {fastEthernet <i>port</i>   range fastEthernet <i>port-list</i>   gigabitEthernet <i>port</i>   range gigabitEthernet <i>port-list</i>   ten-gigabitEthernet <i>port</i>   range ten-gigabitEthernet <i>port-list</i> }</b><br>Uruchom tryb konfiguracji interfejsu. |
| Krok 3 | <b>channel-group <i>num</i> mode on</b><br>Dodaj port do statycznego LAG.<br><br><i>num</i> : Grupowy ID LAG.                                                                                                                                                                     |
| Krok 4 | <b>show etherchannel <i>num</i> summary</b><br>Zweryfikuj konfigurację statycznego LAG.<br><br><i>num</i> : Grupowy ID LAG.                                                                                                                                                       |
| Krok 5 | <b>end</b><br>Powróć do trybu privileged EXEC.                                                                                                                                                                                                                                    |
| Krok 6 | <b>copy running-config startup-config</b><br>Zapisz ustawienia w pliku konfiguracyjnym.                                                                                                                                                                                           |

Poniższy schemat przedstawia przykładowy sposób dodawania portów 1/0/5-8 do LAG 2 i ustawiania trybu jako statyczne LAG:

**Switch#configure**

**Switch(config)#interface range gigabitEthernet 1/0/5-8**

**Switch(config-if-range)#channel-group 2 mode on**

**Switch(config-if-range)#show etherchannel 2 summary**

```

Flags: D - down P - bundled in port-channel U - in use
 I - stand-alone H - hot-standby(LACP only) s - suspended
 R - layer3 S - layer2 f - failed to allocate aggregator
 u - unsuitable for bundling w - waiting to be aggregated d - default port
Group Port-channel Protocol Ports
----- ----- - -----
2 Po2(S) - Gi1/0/5(D) Gi1/0/6(D) Gi1/0/7(D) Gi1/0/8(D)

```

**Switch(config-if-range)#end**

**Switch#copy running-config startup-config**

## ■ Konfiguracja LACP

Wykonaj poniższe kroki, aby skonfigurować tryb LACP:

|        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Krok 1 | <p><b>configure</b></p> <p>Uruchom tryb konfiguracji globalnej.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Krok 2 | <p><b>lACP system-priority <i>pri</i></b></p> <p>Określ priorytety dla przełącznika.</p> <p>Aby zachować zgodność portów po obu stronach, priorytet jednego urządzenia może być wyższy niż priorytet drugiego urządzenia. Urządzenie o wyższym priorytecie określi porty aktywne, a drugie urządzenie wybierze porty aktywne, spośród portów zidentyfikowanych przez urządzenie pierwsze. Jeżeli obie strony mają tę samą wartość priorytetu, urządzenie o niższym adresie MAC uznawane jest za urządzenie o wyższym priorytecie.</p> <p><i>pri</i>: Priorytet systemowy. Prawidłowa wartość waha się od 0 do 65535, a wartością domyślną jest 32768. Im mniejsza wartość, tym wyższy priorytet urządzenia.</p> |
| Krok 3 | <p><b>interface {fastEthernet <i>port</i>   range fastEthernet <i>port-list</i>   gigabitEthernet <i>port</i>   range gigabitEthernet <i>port-list</i>   ten-gigabitEthernet <i>port</i>   range ten-gigabitEthernet <i>port-list</i> }</b></p> <p>Uruchom tryb konfiguracji interfejsu.</p>                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Krok 4 | <p><b>channel-group <i>num</i> mode { active   passive }</b></p> <p>Dodaj port do LAG i ustaw tryb LACP.</p> <p><i>num</i>: Grupowy ID LAG.</p> <p><b>mode</b>: Tryb LAG. Wybierz jeden z trybów LACP: active lub passive.</p> <p>W trybie LACP przełącznik korzysta z LACPDU (Link Aggregation Control Protocol Data Unit) do negocjacji parametrów z urządzeniem równorzędnym. W ten sposób obie strony wybierają porty aktywne i tworzą łącze agregacji. W trybie LACP można ustalić czy dany port ma służyć do przesyłu LACPDU.</p> <p><i>passive</i>: Port nie prześle LACPDU przed odebraniem LACPDU od urządzenia równorzędnego.</p> <p><i>active</i>: Port podejmie inicjatywę przesłania LACPDU.</p>   |
| Krok 5 | <p><b>lACP port-priority <i>pri</i></b></p> <p>Określ priorytet portów. Port o wyższym priorytecie w LAG zostanie wybrany jako port aktywny do przesyłu danych. Jeżeli dwa porty mają tę samą wartość priorytetu, port o niższym numerze portu uznawany jest za port o wyższym priorytecie.</p> <p><i>pri</i>: Priorytet portu. Prawidłowa wartość waha się od 0 do 65535, a wartością domyślną jest 32768. Im mniejsza wartość, tym wyższy priorytet portu.</p>                                                                                                                                                                                                                                                |
| Krok 6 | <p><b>show lACP sys-id</b></p> <p>Zweryfikuj priorytety systemu globalnego.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Krok 7 | <p><b>show lACP internal</b></p> <p>Zweryfikuj konfigurację LACP lokalnego przełącznika.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |

---

Krok 8      **end**  
Powróć do trybu privileged EXEC.

---

Krok 9      **copy running-config startup-config**  
Zapisz ustawienia w pliku konfiguracyjnym.

---

Poniższy schemat przedstawia przykładowy sposób ustawiania priorytetu przełącznika jako 2:

**Switch#configure**

**Switch(config)#lcp system-priority 2**

**Switch(config)#show lcp sys-id**

2, 000a.eb13.2397

**Switch(config)#end**

**Switch#copy running-config startup-config**

Poniższy schemat przedstawia przykładowy sposób dodawania portów 1/0/1-4 do LAG 6, ustawiania trybu jako LACP oraz trybu wysyłania LACPDU jako active:

**Switch#configure**

**Switch(config)#interface range gigabitEthernet 1/0/1-4**

**Switch(config-if-range)#channel-group 6 mode active**

**Switch(config-if-range)#show lcp internal**

Flags: S - Device is requesting Slow LACPDU

      F - Device is requesting Fast LACPDU

      A - Device is in active mode

      P - Device is in passive mode

Channel group 6

| Port    | Flags | State | LACP Port Priority | Admin Key | Oper Key | Port Number | Port State |
|---------|-------|-------|--------------------|-----------|----------|-------------|------------|
| Gi1/0/1 | SA    | Up    | 32768              | 0x6       | 0x4b1    | 0x1         | 0x7d       |
| Gi1/0/2 | SA    | Down  | 32768              | 0x6       | 0        | 0x2         | 0x45       |
| Gi1/0/3 | SA    | Down  | 32768              | 0x6       | 0        | 0x3         | 0x45       |
| Gi1/0/4 | SA    | Down  | 32768              | 0x6       | 0        | 0x4         | 0x45       |

**Switch(config-if-range)#end**

**Switch#copy running-config startup-config**

# 3 Przykład konfiguracji

## 3.1 Wymagania sieciowe

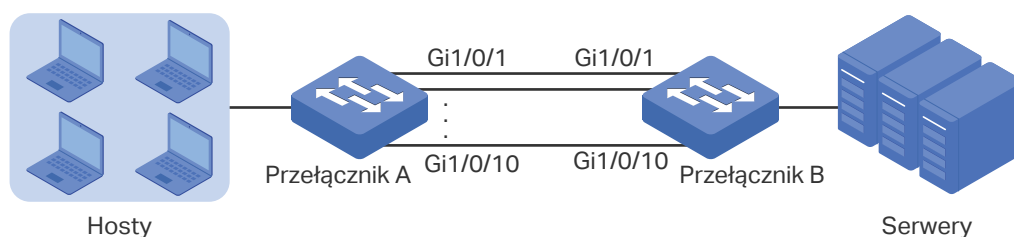
Jak pokazano na poniższym schemacie, hosty i serwery połączone są z przełącznikiem A i przełącznikiem B, które obciążone są intensywnym ruchem sieciowym. Aby uzyskać większe prędkości i wyższą wydajność transmisji danych, użytkownicy powinni postawić na poprawę przepustowości oraz redundancji łącza pomiędzy tymi przełącznikami.

## 3.2 Schemat konfiguracji

Funkcja LAG umożliwia połączenie ze sobą wielu portów fizycznych przełącznika w jedną logiczną całość, co pozwala uzyskać większą przepustowość oraz niezawodność połączeń. W tym przypadku posłużymy się przykładem LACP.

Zgodnie z poniższym schematem w jedną logiczną grupę agregacji połączyć można osiem portów fizycznych, aby przesyłać dane pomiędzy dwoma przełącznikami i odpowiednio łączyć porty należące do grupy. Dodatkowe dwa łącza redundantne mogą służyć jako łącza alternatywne. Aby uniknąć zatorów w ruchu między serwerami a przełącznikiem B, należy także skonfigurować na nich LAG, co pozwoli na zwiększenie przepustowości łącza. W poniższym przykładzie omawiamy przede wszystkim konfigurację LAG pomiędzy dwoma przełącznikami.

Rys. 3-1 Topologia sieci



Podsumowując, konfiguracja przebiega w następujący sposób:

- 1) Zakładając, że po obu stronach znajduje się kilka urządzeń, skonfiguruj algorytm równoważenia obciążenia pasma jako 'SRC MAC+DST MAC'.
- 2) Określ priorytet systemowy przełączników. W tym przykładzie jako urządzenie dominujące wybieramy przełącznik A i nadajemy mu wyższy priorytet systemowy.
- 3) Dodaj porty 1/0/1-10 do LAG i ustaw tryb jako LACP.
- 4) Ustaw niższy priorytet dla portów 1/0/9-10, aby pełniły funkcję portów alternatywnych. Gdy któryś z portów 1/0/1-8 ulegnie awarii, porty alternatywne automatycznie przejmą jego transmisję danych.

W poniższych podrozdziałach opisano dwa sposoby przeprowadzenia procedury konfiguracji: przez GUI oraz przez CLI.

### 3.3 Przez GUI

Ustawienia przełącznika A i przełącznika B są takie same. W poniższym przykładzie omawiamy ustawienia przełącznika A.

- 1) Wybierz z menu **L2 FEATURES > Switching > LAG > LAG Table**, aby wyświetlić poniższą stronę. Ustaw algorytm Hash jako 'SRC MAC+DST MAC'.

Rys. 3-2 Konfiguracja globalna

Global Config

Hash Algorithm: SRC MAC+DST MAC ▼

Apply

- 2) Wybierz z menu **L2 FEATURES > Switching > LAG > LACP Config**, aby wyświetlić poniższą stronę. W części **Global Config** ustaw priorytet systemowy przełącznika A jako **0** i kliknij **Apply**. Pamiętaj, aby upewnić się, że wartość priorytetu systemowego przełącznika B jest wyższy niż 0.

Rys. 3-3 Konfiguracja priorytetu systemowego

Global Config

System Priority: 0 (0-65535)

Apply

- 3) W części **LACP Table** zaznacz porty 1/0/1-10 i ustaw dla każdego z nich wartości status, group ID, port priority oraz mode tak, jak pokazano poniżej.

Rys. 3-4 Konfiguracja LACP

LACP Config

UNIT1

| <input type="checkbox"/> | Port   | Status  | Group ID | Port Priority | Mode   | LAG |
|--------------------------|--------|---------|----------|---------------|--------|-----|
| <input type="checkbox"/> | 1/0/1  | Enabled | 1        | 0             | Active | --- |
| <input type="checkbox"/> | 1/0/2  | Enabled | 1        | 0             | Active | --- |
| <input type="checkbox"/> | 1/0/3  | Enabled | 1        | 0             | Active | --- |
| <input type="checkbox"/> | 1/0/4  | Enabled | 1        | 0             | Active | --- |
| <input type="checkbox"/> | 1/0/5  | Enabled | 1        | 0             | Active | --- |
| <input type="checkbox"/> | 1/0/6  | Enabled | 1        | 0             | Active | --- |
| <input type="checkbox"/> | 1/0/7  | Enabled | 1        | 0             | Active | --- |
| <input type="checkbox"/> | 1/0/8  | Enabled | 1        | 0             | Active | --- |
| <input type="checkbox"/> | 1/0/9  | Enabled | 1        | 1             | Active | --- |
| <input type="checkbox"/> | 1/0/10 | Enabled | 1        | 2             | Active | --- |

Total: 10

- 4) Kliknij , aby zapisać ustawienia.



## 3.4 Przez CLI

Ustawienia przełącznika A i przełącznika B są takie same. W poniższym przykładzie omawiamy ustawienia przełącznika A.

- 1) Ustaw algorytm równoważenia obciążenia pasma jako "src-dst-mac".

```
Switch#configure
```

```
Switch(config)#port-channel load-balance src-dst-mac
```

- 2) Ustaw priorytet systemowy przełącznika A jako 0. Pamiętaj, aby upewnić się, że wartość priorytetu systemowego przełącznika B jest wyższy niż 0.

```
Switch(config)#lacp system-priority 0
```

- 3) Dodaj porty 1/0/1-8 do LAG 1 i ustaw tryb jako LACP. Następnie ustaw priorytet portu jako 0, aby porty były aktywne.

```
Switch(config)#interface range gigabitEthernet 1/0/1-8
```

```
Switch(config-if-range)#channel-group 1 mode active
```

```
Switch(config-if-range)#lacp port-priority 0
```

```
Switch(config-if-range)#exit
```

- 4) Dodaj port 1/0/9 do LAG 1 i ustaw tryb jako LACP. Następnie ustaw priorytet portu jako 1, aby pełnił funkcję portu alternatywnego. Gdy któryś z aktywnych portów ulegnie awarii, port ten będzie miał pierwszeństwo działania jako port aktywny.

```
Switch(config)#interface gigabitEthernet 1/0/9
```

```
Switch(config-if)#channel-group 1 mode active
```

```
Switch(config-if)#lacp port-priority 1
```

```
Switch(config-if)#exit
```

- 5) Dodaj port 1/0/10 do LAG 1 i ustaw tryb jako LACP. Następnie ustaw priorytet portu jako 2, aby pełnił funkcję portu alternatywnego. Priorytet tego portu będzie niższy niż portu 1/0/9.

```
Switch(config)#interface gigabitEthernet 1/0/10
```

```
Switch(config-if)#channel-group 1 mode active
```

```
Switch(config-if)#lacp port-priority 2
```

```
Switch(config-if)#end
```

```
Switch#copy running-config startup-config
```

### Sprawdzanie konfiguracji

Sprawdzanie priorytetu systemowego:

```
Switch#show lacp sys-id
```

0, 000a.eb13.2397

Sprawdzanie konfiguracji LACP:

Switch#show lacp internal

Flags: S - Device is requesting Slow LACPDUs

F - Device is requesting Fast LACPDUs

A - Device is in active mode

P - Device is in passive mode

Channel group 1

| Port     | Flags | State | LACP Port Priority | Admin Key | Oper Key | Port Number | Port State |
|----------|-------|-------|--------------------|-----------|----------|-------------|------------|
| Gi1/0/1  | SA    | Down  | 0                  | 0x1       | 0        | 0x1         | 0x45       |
| Gi1/0/2  | SA    | Down  | 0                  | 0x1       | 0        | 0x2         | 0x45       |
| Gi1/0/3  | SA    | Down  | 0                  | 0x1       | 0        | 0x3         | 0x45       |
| Gi1/0/4  | SA    | Down  | 0                  | 0x1       | 0        | 0x4         | 0x45       |
| Gi1/0/5  | SA    | Down  | 0                  | 0x1       | 0        | 0x5         | 0x45       |
| Gi1/0/6  | SA    | Down  | 0                  | 0x1       | 0        | 0x6         | 0x45       |
| Gi1/0/7  | SA    | Down  | 0                  | 0x1       | 0        | 0x7         | 0x45       |
| Gi1/0/8  | SA    | Down  | 0                  | 0x1       | 0        | 0x8         | 0x45       |
| Gi1/0/9  | SA    | Down  | 1                  | 0x1       | 0        | 0x9         | 0x45       |
| Gi1/0/10 | SA    | Down  | 2                  | 0x1       | 0        | 0xa         | 0x45       |

# Część 5

## Konfiguracja DDM

### ROZDZIAŁy

1. Informacje ogólne
2. Konfiguracja DDM

# 1 Informacje ogólne

Funkcja DDM (Digital Diagnostic Monitoring) służy do monitorowania stanu modułów SFP podłączonych do portów SFP przełącznika. Użytkownik może automatycznie wyłączać monitorowany port SFP, gdy określone parametry przekroczą dozwoloną wartość alarmową lub wartość ostrzegawczą. Monitorowane parametry to m.in.: temperatura, napięcie, bias, moc nadajnika (Tx power) i moc wymagana przez odbiornik (Rx power).

## 2 Konfiguracja DDM

Aby przeprowadzić proces konfiguracji DDM, wykonaj poniższe kroki:

- 1) Włącz DDM na porcie SFP i skonfiguruj warunki wyłączenia portu.
- 2) Ustaw wartość ostrzegawczą lub wartość alarmową.

### 2.1 Przez GUI

#### 2.1.1 Konfiguracja globalna DDM

Wybierz z menu **L2 FEATURES > Switching > DDM > DDM Config** i zaznacz określony port SFP, aby wyświetlić poniższą stronę.

Rys. 2-1 Konfiguracja globalna DDM

| Port Config                         |        |                   |          |                                                                            |
|-------------------------------------|--------|-------------------|----------|----------------------------------------------------------------------------|
| <input type="checkbox"/>            | Port   | DDM Status        | Shutdown | LAG                                                                        |
| <input checked="" type="checkbox"/> | 1/0/9  | Enabled           | None     | --                                                                         |
| <input type="checkbox"/>            | 1/0/10 | Enabled           | None     | --                                                                         |
| Total: 2                            |        | 1 entry selected. |          | <input type="button" value="Cancel"/> <input type="button" value="Apply"/> |

Wykonaj poniższe kroki, aby skonfigurować parametry DDM portów SFP:

- 1) W części **Port Config** zaznacz co najmniej jeden port SFP, aby skonfigurować jego parametry DDM.

|            |                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DDM Status | Włącz lub wyłącz funkcję DDM na porcie SFP.                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Shutdown   | Określ, czy port ma być wyłączany, gdy przekroczona zostanie wartość alarmowa lub wartość ostrzegawcza.<br><br><b>Alarm:</b> Gdy przekroczona zostanie wartość alarmowa, port zostanie wyłączony.<br><br><b>Warning:</b> Gdy przekroczona zostanie wartość ostrzegawcza, port zostanie wyłączony.<br><br><b>None:</b> Port nie zostanie wyłączony nawet wtedy, gdy przekroczona zostanie wartość alarmowa lub ostrzegawcza. Opcja ta jest domyślnie włączona. |
| LAG        | Numer LAG, do którego należy port.                                                                                                                                                                                                                                                                                                                                                                                                                            |

- 2) Kliknij **Apply**.

## 2.1.2 Konfiguracja wartości progowych

### Uwaga:

Wartości progowe parametrów powinny być zgodne z następującą regułą: High Alarm  $\geq$  High Warning  $\geq$  Low Warning  $\geq$  Low Alarm.

Wybierz z menu **L2 FEATURES > Switching > DDM > Threshold Config**, aby wyświetlić poniższą stronę.

#### ■ Konfiguracja wartości progowych temperatury

Rys. 2-2 Konfiguracja wartości progowych temperatury

| Temperature                         |        |                                 |                                |                                   |                                  |                                       |                                      |
|-------------------------------------|--------|---------------------------------|--------------------------------|-----------------------------------|----------------------------------|---------------------------------------|--------------------------------------|
| <input type="checkbox"/>            | Port   | High Alarm<br>(-128-127.996 °C) | Low Alarm<br>(-128-127.996 °C) | High Warning<br>(-128-127.996 °C) | Low Warning<br>(-128-127.996 °C) | LAG                                   |                                      |
| <input checked="" type="checkbox"/> | 1/0/9  | --                              | --                             | --                                | --                               | --                                    |                                      |
| <input type="checkbox"/>            | 1/0/10 | --                              | --                             | --                                | --                               | --                                    |                                      |
| Total: 2                            |        | 1 entry selected.               |                                |                                   |                                  | <input type="button" value="Cancel"/> | <input type="button" value="Apply"/> |

Wykonaj poniższe kroki, aby skonfigurować wartości progowe temperatury dla DDM:

- 1) W tabeli **Temperature** zaznacz co najmniej jeden port SFP, aby skonfigurować jego wartości progowe temperatury.

|              |                                                                                                                                                                                                                               |
|--------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| High Alarm   | Określ najwyższą dopuszczalną wartość alarmową temperatury. Po przekroczeniu tego progu zainicjowane zostanie określone działanie. Prawidłowa wartość musi mieścić się w przedziale -128 - 127,996.                           |
| Low Alarm    | Określ najniższą dopuszczalną wartość alarmową temperatury. Po odnotowaniu wartości niższej niż ustalony próg zainicjowane zostanie określone działanie. Prawidłowa wartość musi mieścić się w przedziale -128 - 127,996.     |
| High Warning | Określ najwyższą dopuszczalną wartość ostrzegawczą temperatury. Po przekroczeniu tego progu zainicjowane zostanie określone działanie. Prawidłowa wartość musi mieścić się w przedziale -128 - 127,996.                       |
| Low Warning  | Określ najniższą dopuszczalną wartość ostrzegawczą temperatury. Po odnotowaniu wartości niższej niż ustalony próg zainicjowane zostanie określone działanie. Prawidłowa wartość musi mieścić się w przedziale -128 - 127,996. |
| LAG          | Numer LAG, do którego należy port.                                                                                                                                                                                            |

- 2) Kliknij **Apply**.

## ■ Konfiguracja wartości progowych napięcia

Rys. 2-3 Konfiguracja wartości progowych napięcia

| Voltage                             |        |                            |                           |                              |                             |        |       |
|-------------------------------------|--------|----------------------------|---------------------------|------------------------------|-----------------------------|--------|-------|
| <input type="checkbox"/>            | Port   | High Alarm<br>(0-6.5535 V) | Low Alarm<br>(0-6.5535 V) | High Warning<br>(0-6.5535 V) | Low Warning<br>(0-6.5535 V) | LAG    |       |
| <input checked="" type="checkbox"/> | 1/0/9  | ---                        | ---                       | ---                          | ---                         | --     |       |
| <input type="checkbox"/>            | 1/0/10 | ---                        | ---                       | ---                          | ---                         | --     |       |
| Total: 2                            |        | 1 entry selected.          |                           |                              |                             | Cancel | Apply |

Wykonaj poniższe kroki, aby skonfigurować wartości progowe napięcia dla DDM:

- 1) W tabeli **Voltage** zaznacz co najmniej jeden port SFP, aby skonfigurować jego wartości progowe napięcia.

|                     |                                                                                                                                                                                                                        |
|---------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>High Alarm</b>   | Określ najwyższą dopuszczalną wartość alarmową napięcia. Po przekroczeniu tego progu zainicjowane zostanie określone działanie. Prawidłowa wartość musi mieścić się w przedziale 0 - 6,5535.                           |
| <b>Low Alarm</b>    | Określ najniższą dopuszczalną wartość alarmową napięcia. Po odnotowaniu wartości niższej niż ustalony próg zainicjowane zostanie określone działanie. Prawidłowa wartość musi mieścić się w przedziale 0 - 6,5535.     |
| <b>High Warning</b> | Określ najwyższą dopuszczalną wartość ostrzegawczą napięcia. Po przekroczeniu tego progu zainicjowane zostanie określone działanie. Prawidłowa wartość musi mieścić się w przedziale 0 - 6,5535.                       |
| <b>Low Warning</b>  | Określ najniższą dopuszczalną wartość ostrzegawczą napięcia. Po odnotowaniu wartości niższej niż ustalony próg zainicjowane zostanie określone działanie. Prawidłowa wartość musi mieścić się w przedziale 0 - 6,5535. |
| <b>LAG</b>          | Numer LAG, do którego należy port.                                                                                                                                                                                     |

- 2) Kliknij **Apply**.

## ■ Konfiguracja wartości progowych bias

Rys. 2-4 Konfiguracja wartości progowych bias

| Bias Current                        |        |                          |                         |                            |                           |        |       |
|-------------------------------------|--------|--------------------------|-------------------------|----------------------------|---------------------------|--------|-------|
| <input type="checkbox"/>            | Port   | High Alarm<br>(0-131 mA) | Low Alarm<br>(0-131 mA) | High Warning<br>(0-131 mA) | Low Warning<br>(0-131 mA) | LAG    |       |
| <input checked="" type="checkbox"/> | 1/0/9  | ---                      | ---                     | ---                        | ---                       | --     |       |
| <input type="checkbox"/>            | 1/0/10 | ---                      | ---                     | ---                        | ---                       | --     |       |
| Total: 2                            |        | 1 entry selected.        |                         |                            |                           | Cancel | Apply |

Wykonaj poniższe kroki, aby skonfigurować wartości progowe bias dla DDM:

- 1) W tabeli **Bias Current** zaznacz co najmniej jeden port SFP, aby skonfigurować jego wartości progowe bias.

|              |                                                                                                                                                                                                                 |
|--------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| High Alarm   | Określ najwyższą dopuszczalną wartość alarmową bias. Po przekroczeniu tego progu zainicjowane zostanie określone działanie. Prawidłowa wartość musi mieścić się w przedziale 0 - 131.                           |
| Low Alarm    | Określ najniższą dopuszczalną wartość alarmową bias. Po odnotowaniu wartości niższej niż ustalony próg zainicjowane zostanie określone działanie. Prawidłowa wartość musi mieścić się w przedziale 0 - 131.     |
| High Warning | Określ najwyższą dopuszczalną wartość ostrzegawczą bias. Po przekroczeniu tego progu zainicjowane zostanie określone działanie. Prawidłowa wartość musi mieścić się w przedziale 0 - 131..                      |
| Low Warning  | Określ najniższą dopuszczalną wartość ostrzegawczą bias. Po odnotowaniu wartości niższej niż ustalony próg zainicjowane zostanie określone działanie. Prawidłowa wartość musi mieścić się w przedziale 0 - 131. |
| LAG          | Numer LAG, do którego należy port.                                                                                                                                                                              |

- 2) Kliknij **Apply**.

#### ■ Konfiguracja wartości progowych mocy wymaganej przez odbiornik

Rys. 2-5 Konfiguracja wartości progowych mocy wymaganej przez odbiornik

| RX Power                            |        |                             |                            |                               |                              |                                       |                                      |
|-------------------------------------|--------|-----------------------------|----------------------------|-------------------------------|------------------------------|---------------------------------------|--------------------------------------|
| <input type="checkbox"/>            | Port   | High Alarm<br>(0-6.5535 mW) | Low Alarm<br>(0-6.5535 mW) | High Warning<br>(0-6.5535 mW) | Low Warning<br>(0-6.5535 mW) | LAG                                   |                                      |
| <input checked="" type="checkbox"/> | 1/0/9  | --                          | --                         | --                            | --                           | --                                    |                                      |
| <input type="checkbox"/>            | 1/0/10 | --                          | --                         | --                            | --                           | --                                    |                                      |
| Total: 2                            |        | 1 entry selected.           |                            |                               |                              | <input type="button" value="Cancel"/> | <input type="button" value="Apply"/> |

Wykonaj poniższe kroki, aby skonfigurować wartości progowe mocy wymaganej przez odbiornik dla DDM:

- 1) W tabeli **RX Power** zaznacz co najmniej jeden port SFP, aby skonfigurować jego wartości progowe mocy wymaganej przez odbiornik.

|            |                                                                                                                                                                                                                                          |
|------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| High Alarm | Określ najwyższą dopuszczalną wartość alarmową mocy wymaganej przez odbiornik. Po przekroczeniu tego progu zainicjowane zostanie określone działanie. Prawidłowa wartość musi mieścić się w przedziale 0 - 6,5535.                       |
| Low Alarm  | Określ najniższą dopuszczalną wartość alarmową mocy wymaganej przez odbiornik. Po odnotowaniu wartości niższej niż ustalony próg zainicjowane zostanie określone działanie. Prawidłowa wartość musi mieścić się w przedziale 0 - 6,5535. |



|              |                                                                                                                                                                                                                                              |
|--------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| High Warning | Określ najwyższą dopuszczalną wartość ostrzegawczą mocy wymaganej przez odbiornik. Po przekroczeniu tego progu zainicjowane zostanie określone działanie. Prawidłowa wartość musi mieścić się w przedziale 0 - 6,5535.                       |
| Low Warning  | Określ najniższą dopuszczalną wartość ostrzegawczą mocy wymaganej przez odbiornik. Po odnotowaniu wartości niższej niż ustalony próg zainicjowane zostanie określone działanie. Prawidłowa wartość musi mieścić się w przedziale 0 - 6,5535. |
| LAG          | Numer LAG, do którego należy port.                                                                                                                                                                                                           |

2) Kliknij **Apply**.

#### ■ Konfiguracja wartości progowych mocy nadajnika

Rys. 2-6 Konfiguracja wartości progowych mocy nadajnika

| TX Power                            |        |                             |                            |                               |                              |                                       |                                      |
|-------------------------------------|--------|-----------------------------|----------------------------|-------------------------------|------------------------------|---------------------------------------|--------------------------------------|
| <input type="checkbox"/>            | Port   | High Alarm<br>(0-6.5535 mW) | Low Alarm<br>(0-6.5535 mW) | High Warning<br>(0-6.5535 mW) | Low Warning<br>(0-6.5535 mW) | LAG                                   |                                      |
| <input checked="" type="checkbox"/> | 1/0/9  | --                          | --                         | --                            | --                           | --                                    |                                      |
| <input type="checkbox"/>            | 1/0/10 | --                          | --                         | --                            | --                           | --                                    |                                      |
| Total: 2                            |        | 1 entry selected.           |                            |                               |                              | <input type="button" value="Cancel"/> | <input type="button" value="Apply"/> |

Wykonaj poniższe kroki, aby skonfigurować wartości progowe mocy nadajnika dla DDM:

1) W tabeli **TX Power** zaznacz co najmniej jeden port SFP, aby skonfigurować jego wartości progowe mocy nadajnika.

|              |                                                                                                                                                                                                                              |
|--------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| High Alarm   | Określ najwyższą dopuszczalną wartość alarmową mocy nadajnika. Po przekroczeniu tego progu zainicjowane zostanie określone działanie. Prawidłowa wartość musi mieścić się w przedziale 0 - 6,5535.                           |
| Low Alarm    | Określ najniższą dopuszczalną wartość alarmową mocy nadajnika. Po odnotowaniu wartości niższej niż ustalony próg zainicjowane zostanie określone działanie. Prawidłowa wartość musi mieścić się w przedziale 0 - 6,5535.     |
| High Warning | Określ najwyższą dopuszczalną wartość ostrzegawczą mocy nadajnika. Po przekroczeniu tego progu zainicjowane zostanie określone działanie. Prawidłowa wartość musi mieścić się w przedziale 0 - 6,5535.                       |
| Low Warning  | Określ najniższą dopuszczalną wartość ostrzegawczą mocy nadajnika. Po odnotowaniu wartości niższej niż ustalony próg zainicjowane zostanie określone działanie. Prawidłowa wartość musi mieścić się w przedziale 0 - 6,5535. |
| LAG          | Numer LAG, do którego należy port.                                                                                                                                                                                           |

2) Kliknij **Apply**.

## 2.1.3 Sprawdzanie stanu DDM

Wybierz z menu **L2 FEATURES > Switching > DDM > DDM Status**, aby wyświetlić poniższą stronę.

Rys. 2-7 Sprawdzanie stanu DDM

| DDM Status |                  |             |                   |               |               |                |                |            |
|------------|------------------|-------------|-------------------|---------------|---------------|----------------|----------------|------------|
| Port       | Temperature (°C) | Voltage (V) | Bias Current (mA) | TX Power (mW) | RX Power (mW) | Transmit Fault | Loss of Signal | Data Ready |
| 1/0/9      | --               | --          | --                | --            | --            | --             | --             | --         |
| 1/0/10     | --               | --          | --                | --            | --            | --             | --             | --         |
| Total: 2   |                  |             |                   |               |               |                |                |            |

Tabela **Port Config** zawiera wszystkie aktualne parametry modułu SFP podłączonego do portu SFP.

|                |                                                                                                     |
|----------------|-----------------------------------------------------------------------------------------------------|
| Temperature    | Aktualna wartość temperatury modułu SFP podłączonego do portu.                                      |
| Voltage        | Aktualna wartość napięcia modułu SFP podłączonego do portu.                                         |
| Bias Current   | Aktualna wartość bias modułu SFP podłączonego do portu.                                             |
| Tx Power       | Aktualna wartość mocy nadajnika modułu SFP podłączonego do portu.                                   |
| Rx Power       | Aktualna wartość mocy wymaganej przez odbiornik modułu SFP podłączonego do portu.                   |
| Data Ready     | Określa, czy moduł SFP jest zdolny do działania. Uwzględnia dwie wartości: True i False.            |
| Loss of Signal | Informuje o utracie sygnału lokalnego modułu SFP. Uwzględnia dwie wartości: True i False.           |
| Transmit Fault | Informuje o utracie sygnału zdalnego modułu SFP. Uwzględnia trzy wartości: True, False i No Signal. |

## 2.2 Przez CLI

### 2.2.1 Konfiguracja globalna DDM

Wykonaj poniższe kroki, aby włączyć funkcję DDM na określonych portach SFP:

|        |                                                          |
|--------|----------------------------------------------------------|
| Krok 1 | <b>configure</b><br>Uruchom tryb konfiguracji globalnej. |
|--------|----------------------------------------------------------|

|        |                                                                                                                                                                                                                                                                                    |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Krok 2 | <b>interface { fastEthernet <i>port</i>   range fastEthernet <i>port-list</i>   gigabitEthernet <i>port</i>   range gigabitEthernet <i>port-list</i>   ten-gigabitEthernet <i>port</i>   range ten-gigabitEthernet <i>port-list</i> }</b><br>Uruchom tryb konfiguracji interfejsu. |
| Krok 3 | <b>ddm state enable</b><br>Włącz DDM na tym porcie SFP.                                                                                                                                                                                                                            |
| Krok 4 | <b>show ddm configuration state</b><br>Wyświetl stan DDM portu SFP.                                                                                                                                                                                                                |
| Krok 5 | <b>end</b><br>Powróć do trybu privileged EXEC.                                                                                                                                                                                                                                     |
| Krok 6 | <b>copy running-config startup-config</b><br>Zapisz ustawienia w pliku konfiguracyjnym.                                                                                                                                                                                            |

Poniższy schemat przedstawia przykładowy sposób włączania DDM na porcie 1/0/9 SFP:

**Switch#configure**

**Switch(config)#interface gigabitEthernet 1/0/9**

**Switch(config-if)#ddm state enable**

**Switch(config-if)#show ddm configuration state**

|         | DDM Status | Shutdown |
|---------|------------|----------|
| Gi1/0/9 | Enable     | None     |

...

**Switch(config-if)#end**

**Switch#copy running-config startup-config**

## 2.2.2 Konfiguracja wyłączenia portów dla DDM

Wykonaj poniższe kroki, aby skonfigurować ustawienia wyłączenia portów SFP, gdy przekroczona zostanie wartość alarmowa lub ostrzegawcza:

|        |                                                          |
|--------|----------------------------------------------------------|
| Krok 1 | <b>configure</b><br>Uruchom tryb konfiguracji globalnej. |
|--------|----------------------------------------------------------|

---

|        |                                                                                                                                                                                                                                                                                                |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Krok 2 | <b>interface { fastEthernet <i>port</i>   range fastEthernet <i>port-list</i>   gigabitEthernet <i>port</i>   range gigabitEthernet <i>port-list</i>   ten-gigabitEthernet <i>port</i>   range ten-gigabitEthernet <i>port-list</i> }</b><br>Uruchom tryb konfiguracji interfejsu.             |
| Krok 3 | <b>ddm shutdown { none   warning   alarm }</b><br>none: Port nie zostanie wyłączony po przekroczeniu wartości alarmowej lub ostrzegawczej.<br>warning: Port zostanie wyłączony po przekroczeniu wartości ostrzegawczej.<br>alarm: Port zostanie wyłączony po przekroczeniu wartości alarmowej. |
| Krok 4 | <b>show ddm configuration state</b><br>Wyświetl stan portów SFP dla DDM.                                                                                                                                                                                                                       |
| Krok 5 | <b>end</b><br>Powróć do trybu privileged EXEC.                                                                                                                                                                                                                                                 |
| Krok 6 | <b>copy running-config startup-config</b><br>Zapisz ustawienia w pliku konfiguracyjnym.                                                                                                                                                                                                        |

---

Poniższy schemat przedstawia przykładowy sposób ustawiania wyłączenia portu 1/0/25 SFP po przekroczeniu wartości ostrzegawczej.

**Switch#configure**

**Switch(config)#interface gigabitEthernet 1/0/25**

**Switch(config-if)#ddm shutdown warning**

**Switch(config-if)#show ddm configuration state**

|          | DDM Status | Shutdown |
|----------|------------|----------|
| Gi1/0/25 | Enable     | Warning  |

...

**Switch(config-if)#end**

**Switch#copy running-config startup-config**

### 2.2.3 Konfiguracja wartości progowych

- Konfiguracja wartości progowych temperatury

Wykonaj poniższe kroki, aby skonfigurować wartości progowe temperatury na określonym porcie SFP dla DDM.

---

|        |                                                          |
|--------|----------------------------------------------------------|
| Krok 1 | <b>configure</b><br>Uruchom tryb konfiguracji globalnej. |
|--------|----------------------------------------------------------|

---

|        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Krok 2 | <b>interface { fastEthernet <i>port</i>   range fastEthernet <i>port-list</i>   gigabitEthernet <i>port</i>   range gigabitEthernet <i>port-list</i>   ten-gigabitEthernet <i>port</i>   range ten-gigabitEthernet <i>port-list</i> }</b><br>Uruchom tryb konfiguracji interfejsu.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Krok 3 | <b>ddm temperature_threshold { high_alarm   high_warning   low_alarm   low_warning } value</b><br><br><i>high_alarm</i> : Określ najwyższą dopuszczalną wartość alarmową. Po przekroczeniu tego progu zainicjowane zostanie określone działanie.<br><br><i>high_warning</i> : Określ najwyższą dopuszczalną wartość ostrzegawczą. Po przekroczeniu tego progu zainicjowane zostanie określone działanie.<br><br><i>low_alarm</i> : Określ najniższą dopuszczalną wartość alarmową mocy nadajnika. Po odnotowaniu wartości niższej niż ustalony próg zainicjowane zostanie określone działanie.<br><br><i>low_warning</i> : Określ najniższą dopuszczalną wartość ostrzegawczą mocy nadajnika. Po odnotowaniu wartości niższej niż ustalony próg zainicjowane zostanie określone działanie.<br><br><i>value</i> : Wprowadź wartość progową wyrażoną w stopniach Celsjusza. Prawidłowa wartość musi mieścić się w przedziale -128 - 127,996. |
| Krok 4 | <b>show ddm configuration temperature</b><br>Wyświetl wartości progowe temperatur na portach SFP dla DDM.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Krok 5 | <b>end</b><br>Powróć do trybu privileged EXEC.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Krok 6 | <b>copy running-config startup-config</b><br>Zapisz ustawienia w pliku konfiguracyjnym.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |

Poniższy schemat przedstawia przykładowy sposób ustawiania na porcie 1/0/10 najwyższej wartości alarmowej temperatury na poziomie 110 stopni Celsjusza.

**Switch#configure**

**Switch(config)#interface gigabitEthernet 1/0/10**

**Switch(config-if)#ddm temperature\_threshold high\_alarm 110**

**Switch(config-if)#show ddm configuration temperature**

Temperature Threshold(Celsius) :

|          | High Alarm | Low Alarm | High Warning | Low Warning |
|----------|------------|-----------|--------------|-------------|
| Gi1/0/10 | 110.000000 | --        | --           | --          |

...

**Switch(config-if)#end**

**Switch#copy running-config startup-config**

- Konfiguracja wartości progowych napięcia

Wykonaj poniższe kroki, aby skonfigurować wartości progowe napięcia na określonym porcie SFP dla DDM.

|        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Krok 1 | <b>configure</b><br>Uruchom tryb konfiguracji globalnej.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Krok 2 | <b>interface { fastEthernet port   range fastEthernet port-list   gigabitEthernet port   range gigabitEthernet port-list   ten-gigabitEthernet port   range ten-gigabitEthernet port-list }</b><br>Uruchom tryb konfiguracji interfejsu..                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Krok 3 | <b>ddm voltage_threshold { high_alarm   high_warning   low_alarm   low_warning } value</b><br><br><p><b>high_alarm:</b> Określ najwyższą dopuszczalną wartość alarmową. Po przekroczeniu tego progu zainicjowane zostanie określone działanie.</p> <p><b>high_warning:</b> Określ najwyższą dopuszczalną wartość ostrzegawczą. Po przekroczeniu tego progu zainicjowane zostanie określone działanie.</p> <p><b>low_alarm:</b> Określ najniższą dopuszczalną wartość alarmową mocy nadajnika. Po odnotowaniu wartości niższej niż ustalony próg zainicjowane zostanie określone działanie.</p> <p><b>low_warning:</b> Określ najniższą dopuszczalną wartość ostrzegawczą mocy nadajnika. Po odnotowaniu wartości niższej niż ustalony próg zainicjowane zostanie określone działanie.</p> <p><b>value:</b> Wprowadź wartość progową wyrażoną w woltach (V). Prawidłowa wartość musi mieścić się w przedziale 0 - 6,5535.</p> |
| Krok 4 | <b>show ddm configuration voltage</b><br>Wyświetl wartości progowe napięcia na portach SFP dla DDM.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Krok 5 | <b>end</b><br>Powróć do trybu privileged EXEC.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Krok 6 | <b>copy running-config startup-config</b><br>Zapisz ustawienia w pliku konfiguracyjnym.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |

Poniższy schemat przedstawia przykładowy sposób ustawiania na porcie 1/0/10 najwyższej wartości alarmowej napięcie na poziomie 5 V.

**Switch#configure**

**Switch(config)#interface gigabitEthernet 1/0/10**

**Switch(config-if)#ddm vlotage\_threshold high\_alarm 5**

**Switch(config-if)#show ddm configuration voltage**

Voltage Threshold(V) :

|          | High Alarm | Low Alarm | High Warning | Low Warning |
|----------|------------|-----------|--------------|-------------|
| Gi1/0/10 | 5.000000   | --        | --           | --          |

...

**Switch(config-if)#end****Switch#copy running-config startup-config**

- Konfiguracja wartości progowych bias

Wykonaj poniższe kroki, aby skonfigurować wartości progowe bias na określonym porcie SFP dla DDM.

|        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Krok 1 | <b>configure</b><br>Uruchom tryb konfiguracji globalnej.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Krok 2 | <b>interface { fastEthernet <i>port</i>   range fastEthernet <i>port-list</i>   gigabitEthernet <i>port</i>   range gigabitEthernet <i>port-list</i>   ten-gigabitEthernet <i>port</i>   range ten-gigabitEthernet <i>port-list</i> }</b><br>Uruchom tryb konfiguracji interfejsu..                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Krok 3 | <b>ddm bias_current_threshold { high_alarm   high_warning   low_alarm   low_warning } <i>value</i></b><br><br><i>high_alarm</i> : Określ najwyższą dopuszczalną wartość alarmową. Po przekroczeniu tego progu zainicjowane zostanie określone działanie.<br><br><i>high_warning</i> : Określ najwyższą dopuszczalną wartość ostrzegawczą. Po przekroczeniu tego progu zainicjowane zostanie określone działanie.<br><br><i>low_alarm</i> : Określ najniższą dopuszczalną wartość alarmową mocy nadajnika. Po odnotowaniu wartości niższej niż ustalony próg zainicjowane zostanie określone działanie.<br><br><i>low_warning</i> : Określ najniższą dopuszczalną wartość ostrzegawczą mocy nadajnika. Po odnotowaniu wartości niższej niż ustalony próg zainicjowane zostanie określone działanie.<br><br><i>value</i> : Wprowadź wartość progową wyrażoną w miliamperach (mA). Prawidłowa wartość musi mieścić się w przedziale 0 - 131. |
| Krok 4 | <b>show ddm configuration bias_current</b><br>Wyświetl wartości progowe bias na portach SFP dla DDM.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Krok 5 | <b>end</b><br>Powróć do trybu privileged EXEC.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Krok 6 | <b>copy running-config startup-config</b><br>Zapisz ustawienia w pliku konfiguracyjnym.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |

Poniższy schemat przedstawia przykładowy sposób ustawiania na porcie 1/0/10 najwyższej wartości alarmowej bias na poziomie 120 mA.

**Switch#configure****Switch(config)#interface gigabitEthernet 1/0/10****Switch(config-if)#ddm vltage\_threshold high\_alarm 120****Switch(config-if)#show ddm configuration bias\_current**

Voltage Threshold(V) :

|          | High Alarm | Low Alarm | High Warning | Low Warning |
|----------|------------|-----------|--------------|-------------|
| Gi1/0/10 | 120.000000 | --        | --           | --          |

...

**Switch(config-if)#end**

**Switch#copy running-config startup-config**

- Konfiguracja wartości progowych mocy wymaganej przez odbiornik

Wykonaj poniższe kroki, aby skonfigurować wartości progowe mocy wymaganej przez odbiornik na określonym porcie SFP dla DDM.

|        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Krok 1 | <b>configure</b><br>Uruchom tryb konfiguracji globalnej.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Krok 2 | <b>interface { fastEthernet port   range fastEthernet port-list   gigabitEthernet port   range gigabitEthernet port-list   ten-gigabitEthernet port   range ten-gigabitEthernet port-list }</b><br>Uruchom tryb konfiguracji interfejsu..                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Krok 3 | <b>ddm rx_power_threshold { high_alarm   high_warning   low_alarm   low_warning } value</b><br><br><b>high_alarm:</b> Określ najwyższą dopuszczalną wartość alarmową. Po przekroczeniu tego progu zainicjowane zostanie określone działanie.<br><br><b>high_warning:</b> Określ najwyższą dopuszczalną wartość ostrzegawczą. Po przekroczeniu tego progu zainicjowane zostanie określone działanie.<br><br><b>low_alarm:</b> Określ najniższą dopuszczalną wartość alarmową mocy nadajnika. Po odnotowaniu wartości niższej niż ustalony próg zainicjowane zostanie określone działanie.<br><br><b>low_warning:</b> Określ najniższą dopuszczalną wartość ostrzegawczą mocy nadajnika. Po odnotowaniu wartości niższej niż ustalony próg zainicjowane zostanie określone działanie.<br><br><b>value:</b> Wprowadź wartość progową wyrażoną w miliwatach (mW). Prawidłowa wartość musi mieścić się w przedziale 0 - 6,5535. |
| Krok 4 | <b>show ddm configuration rx_power</b><br>Wyświetl wartości progowe mocy wymaganej przez odbiornik na portach SFP dla DDM.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Krok 5 | <b>end</b><br>Powróć do trybu privileged EXEC.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Krok 6 | <b>copy running-config startup-config</b><br>Zapisz ustawienia w pliku konfiguracyjnym.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |

Poniższy schemat przedstawia przykładowy sposób ustawiania na porcie 1/0/10 najwyższej wartości alarmowej mocy wymaganej przez odbiornik na poziomie 6 mW.

**Switch#configure**



```
Switch(config)#interface gigabitEthernet 1/0/10
```

```
Switch(config-if)#ddm rx_power_threshold high_alarm 6
```

```
Switch(config-if)#show ddm configuration rx_power
```

Rx Power Threshold(mW) :

|          | High Alarm | Low Alarm | High Warning | Low Warning |
|----------|------------|-----------|--------------|-------------|
| Gi1/0/10 | 6.000000   | --        | --           | --          |

...

```
Switch(config-if)#end
```

```
Switch#copy running-config startup-config
```

- Konfiguracja wartości progowych mocy nadajnika

Wykonaj poniższe kroki, aby skonfigurować wartości progowe mocy nadajnika na określonym porcie SFP dla DDM.

|        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Krok 1 | <p><b>configure</b></p> <p>Uruchom tryb konfiguracji globalnej.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Krok 2 | <p><b>interface { fastEthernet <i>port</i>   range fastEthernet <i>port-list</i>   gigabitEthernet <i>port</i>   range gigabitEthernet <i>port-list</i>   ten-gigabitEthernet <i>port</i>   range ten-gigabitEthernet <i>port-list</i> }</b></p> <p>Uruchom tryb konfiguracji interfejsu..</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Krok 3 | <p><b>ddm tx_power_threshold { high_alarm   high_warning   low_alarm   low_warning } <i>value</i></b></p> <p><b>high_alarm:</b> Określ najwyższą dopuszczalną wartość alarmową. Po przekroczeniu tego progu zainicjowane zostanie określone działanie.</p> <p><b>high_warning:</b> Określ najwyższą dopuszczalną wartość ostrzegawczą. Po przekroczeniu tego progu zainicjowane zostanie określone działanie.</p> <p><b>low_alarm:</b> Określ najniższą dopuszczalną wartość alarmową mocy nadajnika. Po odnotowaniu wartości niższej niż ustalony próg zainicjowane zostanie określone działanie.</p> <p><b>low_warning:</b> Określ najniższą dopuszczalną wartość ostrzegawczą mocy nadajnika. Po odnotowaniu wartości niższej niż ustalony próg zainicjowane zostanie określone działanie.</p> <p><b><i>value:</i></b> Wprowadź wartość progową wyrażoną w miliwatach (mW). Prawidłowa wartość musi mieścić się w przedziale 0 - 6,5535..</p> |
| Krok 4 | <p><b>show ddm configuration tx_power</b></p> <p>Wyświetl wartości progowe mocy nadajnika na portach SFP dla DDM.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Krok 5 | <p><b>end</b></p> <p>Powrót do trybu privileged EXEC.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |

---

Krok 6      **copy running-config startup-config**  
Zapisz ustawienia w pliku konfiguracyjnym.

---

Poniższy schemat przedstawia przykładowy sposób ustawiania na porcie 1/0/10 najwyższej wartości alarmowej mocy nadajnika na poziomie 6 mW.

**Switch#configure**

**Switch(config)#interface gigabitEthernet 1/0/10**

**Switch(config-if)#ddm tx\_power\_threshold high\_alarm 6**

**Switch(config-if)#show ddm configuration tx\_power**

Tx Power Threshold(mW) :

|          | High Alarm | Low Alarm | High Warning | Low Warning |
|----------|------------|-----------|--------------|-------------|
| Gi1/0/10 | 6.000000   | --        | --           | --          |

...

**Switch(config-if)#end**

**Switch#copy running-config startup-config**

## 2.2.4 Przeglądanie konfiguracji DDM

Wykonaj poniższej kroki, aby zyskać wgląd w konfigurację DDM.

---

Krok 1      **configure**  
Uruchom tryb konfiguracji globalnej.

---

Krok 2      **show ddm configuration { state | temperature | voltage | bias\_current | tx\_power | rx\_power }**  
state: Stan konfiguracji DDM.  
temperature: Wartości progowe temperatury dla DDM.  
voltage: Wartości progowe napięcia dla DDM.  
bias\_current: Wartości progowe bias dla DDM.  
tx\_power: Wartości progowe mocy nadajnika dla DDM.  
rx\_power: Wartości progowe mocy wymaganej przez odbiornik dla DDM.

---

Krok 5      **end**  
Powróć do trybu privileged EXEC.

---

---

Krok 6      **copy running-config startup-config**  
Zapisz ustawienia w pliku konfiguracyjnym.

---

Poniższy schemat przedstawia przykładowy sposób wyświetlania wartości progowych mocy wymaganej przez odbiornik na portach SFP.

**Switch#configure**

**Switch(config)#show ddm configuration rx\_power**

Rx Power Threshold(mW) :

|          | High Alarm | Low Alarm | High Warning | Low Warning |
|----------|------------|-----------|--------------|-------------|
| Gi1/0/9  | 6.000000   | --        | --           | --          |
| Gi1/0/10 | --         | --        | --           | --          |

**Switch(config)#end**

## 2.2.5 Sprawdzanie stanu DDM

Wykonaj poniższe kroki, aby wyświetlić stan DDM, czyli funkcji umożliwiającej monitorowanie parametrów modułów SFP podłączonych do portów SFP przełącznika.

---

Krok 1      **configure**  
Uruchom tryb konfiguracji globalnej.

---

Krok 2      **show ddm status**  
Wyświetl wszystkie monitorowane parametry modułów SFP.

---

Krok 3      **end**  
Powróć do trybu privileged EXEC.

---

Poniższy schemat przedstawia przykładowy sposób sprawdzania stanu portów SFP dla DDM.

**Switch#configure**

**Switch(config)#show ddm status**

|              | Temperature(C) | Voltage(V) | Bias Current(mA) | Tx Power(mW) |
|--------------|----------------|------------|------------------|--------------|
| Rx Power(mW) | Data Ready     | Rx Los     | Tx Fault         |              |
| Gi1/0/9      | --             | --         | --               | --           |
| --           | --             | --         | --               | --           |
| Gi1/0/10     | --             | --         | --               | --           |
| --           | --             | --         | --               | --           |

**Switch(config)#end**

# Część 6

## Zarządzanie tablicą adresów MAC

### ROZDZIAŁY

1. Tablica adresów MAC
2. Konfiguracja adresów MAC
3. Konfiguracja zabezpieczeń
4. Przykład konfiguracji zabezpieczeń

# 1 Tablica adresów MAC

## 1.1 Informacje ogólne

Tablica adresów MAC zawiera informacje o adresach, z których przełącznik korzysta do przesyłania pakietów. Jak pokazano poniżej, tablica zawiera listę wpisów mapowanych adresów MAC, identyfikatory sieci VLAN oraz numery portów. Wpisy te są dodawane ręcznie lub przełącznik uczy się ich automatycznie. W oparciu o mapowanie portów na adresy MAC przełącznik może przysyłać pakiety tylko na powiązanych portach.

Tabela 1-1 Tablica adresów MAC

| MAC Address       | VLAN ID | Port | Type    | Aging Status |
|-------------------|---------|------|---------|--------------|
| 00:00:00:00:00:01 | 1       | 1    | Dynamic | Aging        |
| 00:00:00:00:00:01 | 1       | 2    | Static  | No-Aging     |
| ...               |         |      |         |              |

## 1.2 Obsługiwane funkcje

Tablica adresów przełącznika zawiera adresy dynamiczne, adresy statyczne i umożliwia filtrowanie adresów. Wpisy możesz odpowiednio dodawać i usuwać. Ponadto możesz także skonfigurować wysyłanie komunikatów trap oraz ustawić limit adresów MAC w sieci VLAN, by zwiększyć bezpieczeństwo ruchu sieciowego.

### Konfiguracja adresów

- Adres dynamiczny

Adresy dynamiczne to adresy, których przełącznik uczy się automatycznie. Przełącznik regularnie pozbywa się adresów, które nie są już używane. Przełącznik usuwa wpisy adresów MAC powiązanych z urządzeniami sieciowymi, jeżeli dane urządzenia w trakcie czasu starzenia adresów nie wysłały żadnego pakietu. W razie potrzeby możesz samodzielnie określić czas starzenia się adresów.

- Adres statyczny

Adresy statyczne dodawane są do tablicy adresów ręcznie i nie starzeją się. Dla stosunkowo stałych połączeń, np. często odwiedzanego serwera, możesz ręcznie ustawić adres MAC serwera jako statyczny - zwiększy to wydajność przesyłania przełącznika.

- Filtrowanie adresów

Filtrowanie adresów umożliwia wyznaczenie pakietów z określonymi źródłowymi lub docelowymi adresami MAC, które będą odrzucane przez przełącznik.

## Konfiguracja zabezpieczeń

- Konfiguracja wysyłania komunikatów trap

Skonfigurowanie komunikatów trap i protokołu SNMP (Simple Network Management Protocol) umożliwia monitorowanie i otrzymywanie powiadomień o korzystaniu z tablicy adresów MAC oraz o wykrytych zmianach adresów MAC. Można na przykład tak skonfigurować ustawienia, aby przełącznik wysyłał powiadomienia, gdy nauczy się nowego adresu MAC, co pozwoli administratorom sieci na uzyskanie informacji o nowych użytkownikach w sieci.

- Ustawianie limitu adresów MAC w sieciach VLAN

Aby ustawić limit adresów MAC zapamiętywanych w określonych sieciach VLAN należy skonfigurować ustawienia zabezpieczeń VLAN. Przełącznik przestanie uczyć się nowych adresów, gdy liczba zapamiętanych adresów przekroczy ustawiony limit. Zapobiega to wykorzystywaniu tablicy adresów przez pakiety rozgłoszeniowe, generowane w wyniku ataku na adres MAC.

## 2 Konfiguracja adresów MAC

Tablica adresów MAC umożliwia:


- dodawanie wpisów statycznych adresów MAC;
- zmianę czasu starzenia się adresów MAC;
- dodawanie wpisów filtrowania adresów;
- wyświetlanie wpisów tablicy adresów

### 2.1 Przez GUI

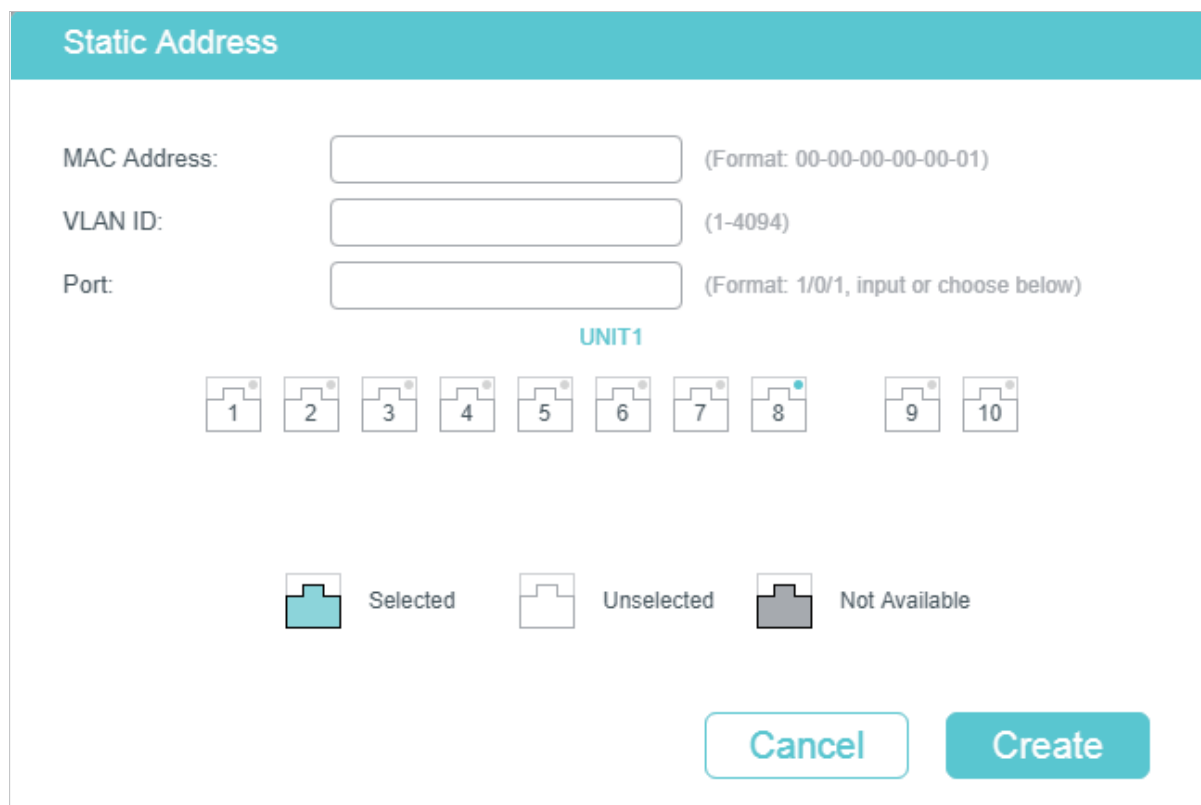
#### 2.1.1 Dodawanie wpisów statycznych adresów MAC

Możesz dodać do tabeli wpisy statycznych adresów MAC ręcznie, wyznaczając wybrane adresy MAC lub wiążąc wpisy dynamicznych adresów MAC.

- Ręczne dodawanie adresów MAC

Wybierz z menu **L2 FEATURES > Switching > MAC Address > Static Address** i kliknij  **Add**, aby wyświetlić poniższą stronę.

Rys. 2-1 Ręczne dodawanie adresów MAC



**Static Address**

MAC Address:  (Format: 00-00-00-00-00-01)

VLAN ID:  (1-4094)

Port:  (Format: 1/0/1, input or choose below)

**UNIT1**

1 2 3 4 5 6 7 8 9 10

Selected Unselected Not Available

Cancel Create

Wykonaj poniższe kroki, aby dodać wpis statycznego adresu MAC:

1) Wprowadź adres MAC, VLAN ID i wybierz port, aby połączyć je w jeden wpis adresu.

|             |                                                                                                                                                                                                                                                                                                                                                                                                        |
|-------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| MAC Address | Wprowadź statyczny adres MAC, który będzie dodany do wpisu statycznego adresu MAC.                                                                                                                                                                                                                                                                                                                     |
| VLAN ID     | Wyznacz istniejącą sieć VLAN, w której odbierane są pakiety z określonymi adresami MAC.                                                                                                                                                                                                                                                                                                                |
| Port        | Wyznacz port, do którego pakiety z określonymi adresami MAC są przekierowywane. Port musi należeć do wyznaczonej sieci VLAN.<br><br>Po dodaniu statycznego adresu MAC, przełącznik nie może prawidłowo przekierowywać pakietów, jeżeli numer odpowiadającego portu adresu MAC jest nieprawidłowy lub zmieniono połączony port (lub urządzenie). Należy odpowiednio zresetować wpis adresu statycznego. |

2) Kliknij **Create**.

#### ■ Wiązanie wpisów adresu dynamicznego

Jeżeli wpisy adresu dynamicznego są często używane, możesz powiązać wpisy jako wpisy statyczne.

Wybierz z menu **L2 FEATURES > Switching > MAC Address > Dynamic Address**, aby wyświetlić poniższą stronę.

Rys. 2-2 Wiązanie wpisów dynamicznego adresu MAC

**Aging Config**

Auto Aging:  Enable

Aging Time:  seconds (10-630)

[Apply](#)

---

**Dynamic Address Table**

All

| <input type="checkbox"/>            | MAC Address       | VLAN ID | Port   | Type    | Aging Status |
|-------------------------------------|-------------------|---------|--------|---------|--------------|
| <input checked="" type="checkbox"/> | 30-B5-C2-BD-04-6E | 1       | 1/0/22 | Dynamic | Aging        |
| <input type="checkbox"/>            | 00-0A-EB-13-23-97 | 1       | 1/0/22 | Dynamic | Aging        |
| <input type="checkbox"/>            | 00-0A-EB-13-23-7B | 1       | 1/0/22 | Dynamic | Aging        |
| <input type="checkbox"/>            | C4-6E-1F-BF-72-51 | 1       | 1/0/22 | Dynamic | Aging        |
| <input type="checkbox"/>            | 00-19-66-35-E1-B0 | 1       | 1/0/22 | Dynamic | Aging        |

Total: 5 1 entry selected.

Wykonaj poniższe kroki, aby powiązać wpisy dynamicznego adresu MAC:

1) W sekcji **Dynamic Address Table** wybierz wpisy adresów MAC.

2) Kliknij **Bind**. Wybrane wpisy zmienią typ na wpisy statycznego adresu MAC.



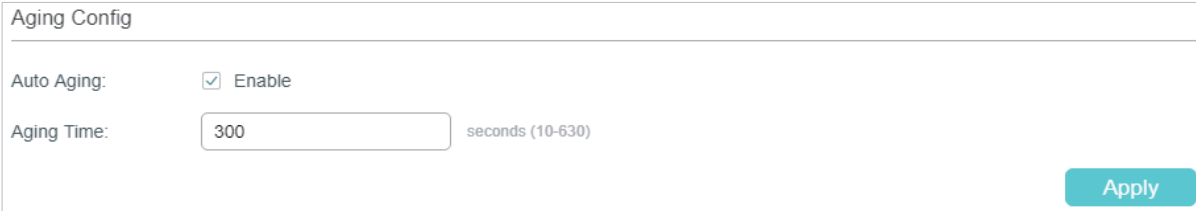
### Uwaga:

- W obrębie jednej sieci VLAN adresu ustawionego jako statyczny nie można już ustawić jako adres filtrowania i vice versa.
- Adresy multicast lub broadcast nie mogą być ustawione jako adresy statyczne.
- Porty w grupach LAG (Link Aggregation Group) nie są obsługiwane w konfiguracji adresów statycznych.

## 2.1.2 Zmiana czasu utraty ważności wpisów adresów dynamicznych

Wybierz z menu **L2 FEATURES > Switching > MAC Address > Dynamic Address**, aby wyświetlić poniższą stronę.

Rys. 2-3 Zmiana czasu utraty ważności wpisów adresów dynamicznych




Wykonaj poniższe kroki, aby zmienić czas utraty ważności wpisów adresów dynamicznych:

- 1) W sekcji **Aging Config** włącz Auto Aging i wprowadź wybraną długość okresu.

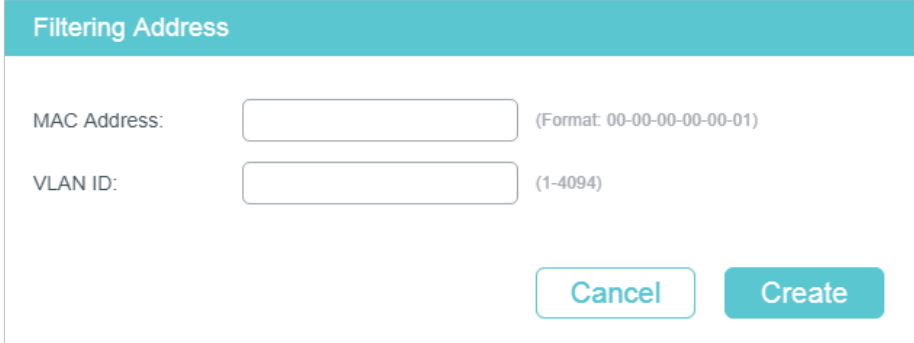
|            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Auto Aging | Włącz Auto Aging. Przełącznik będzie automatycznie aktualizował tablicę dynamicznych adresów, zgodnie z mechanizmem starzenia. Funkcja jest domyślnie włączona.                                                                                                                                                                                                                                                                                                                   |
| Aging Time | Ustaw długość okresu, przez który po ostatnim użyciu lub aktualizacji wpis dynamiczny pozostaje na tablicy adresów MAC. Wartość musi zawierać się między 10 a 630 s. Wartość domyślna to 300.<br><br>Krótki czas utraty ważności sprawdzi się w sieciach, których topologia często się zmienia. Długi czas utraty ważności jest odpowiedni w stabilnych sieciach. W przypadku braku pewności w kwestii wybrania najlepszego ustawienia, zaleca się zachowanie wartości domyślnej. |

- 2) Kliknij **Apply**.

## 2.1.3 Dodawanie wpisów filtrowania adresów MAC

Wybierz z menu **L2 FEATURES > Switching > MAC Address > Filtering Address** i kliknij  **Add**, aby wyświetlić poniższą stronę.

Rys. 2-4 Dodawanie wpisów filtrowania adresów MAC



Wykonaj poniższe kroki, aby dodać wpisy filtrowania adresów MAC:

1) Wprowadź adres MAC i VLAN ID.

|             |                                                                                                         |
|-------------|---------------------------------------------------------------------------------------------------------|
| MAC Address | Wyznacz adres MAC, który będzie wykorzystywany przez przełącznik do filtrowania otrzymywanych pakietów. |
| VLAN ID     | Wyznacz sieć VLAN, w której pakiety o wyznaczonym adresie MAC są odrzucane.                             |


2) Kliknij **Create**.

### Uwaga:


- W obrębie jednej sieci VLAN adresu ustawionego jako statyczny nie można już ustawić jako adres filtrowania i vice versa.
- Adresy multicast lub broadcast nie mogą być ustawione jako adresy filtrowania.

## 2.1.4 Wyświetlanie wpisów tablicy adresów

Możesz wyświetlać wpisy na tablicy adresów MAC, aby sprawdzać poprzednie działania i dane adresu.

Wybierz z menu **L2 FEATURES > Switching > MAC Address > Address Table** i kliknij  **Search**, aby wyświetlić poniższą stronę.

Rys. 2-5 Wyświetlanie wpisów tablicy adresów

Address Table  Search ^

---

MAC Address  (Format: 00-00-00-00-00-01)

VLAN ID  (1-4094)

Type  Dynamic  Static  Filter

Port

---

| MAC Address       | VLAN ID | Port  | Type    | Aging Status |
|-------------------|---------|-------|---------|--------------|
| 30-B5-C2-BD-20-CC | 1       | 1/0/8 | Dynamic | Aging        |
| 00-0A-EB-13-23-97 | 1       | 1/0/8 | Dynamic | Aging        |
| 00-0A-EB-13-23-7B | 1       | 1/0/8 | Dynamic | Aging        |
| 30-B5-C2-BD-20-5C | 1       | 1/0/8 | Dynamic | Aging        |
| 00-0A-EB-13-A2-02 | 1       | 1/0/8 | Dynamic | Aging        |
| C4-6E-1F-BF-72-51 | 1       | 1/0/8 | Dynamic | Aging        |
| 00-19-66-35-E1-B0 | 1       | 1/0/8 | Dynamic | Aging        |

Total: 7

## 2.2 Przez CLI

### 2.2.1 Dodawanie wpisów statycznych adresów MAC

Wykonaj poniższe kroki, aby dodać wpisy statycznych adresów MAC:

**Krok 1**     **configure**

Wejść w tryb konfiguracji globalnej.

**Krok 2**     **mac address-table static *mac-addr* vid *vid* interface { fastEthernet *port* | gigabitEthernet *port* | ten-gigabitEthernet *port* }**

Powiąz adres MAC, VLAN i port, aby dodać adres statyczny do VLAN.

*mac-addr*: Wprowadź adres MAC. Pakiety z tym adresem docelowym otrzymane w wyznaczonej sieci VLAN są przekierowywane do wyznaczonego portu. Format to xx:xx:xx:xx:xx:xx, np. 00:00:00:00:00:01.

*vid*: Wyznacz istniejącą sieć VLAN, w której odbierane są pakiety z określonym adresem MAC.

*port*: Wyznacz port, do którego przesyłane są pakiety z określonym adresem MAC. Port musi należeć do wyznaczonej sieci VLAN.

Krok 3 **end**  
Wróć do trybu privileged EXEC.

Krok 4 **copy running-config startup-config**  
Zapisz ustawienia w pliku konfiguracyjnym.

 **Uwaga:**

- W obrębie jednej sieci VLAN adresu ustawionego jako statyczny nie można już ustawić jako adres filtrowania i vice versa.
- Adresy multicast lub broadcast nie mogą być ustawione jako adresy statyczne.
- Porty w grupach LAG (Link Aggregation Group) nie są obsługiwane w konfiguracji adresów statycznych.

Poniższy przykład prezentuje, jak dodać wpis statycznego adresu MAC dla adresu 00:02:58:4f:6c:23, VLAN 10 i portu 1. Jeżeli pakiet jest odebrany w sieci VLAN 10 z tym adresem jako docelowym, pakiet zostanie przekierowany jedynie do portu 1/0/1.

**Switch#configure**

**Switch(config)# mac address-table static 00:02:58:4f:6c:23 vid 10 interface gigabitEthernet 1/0/1**

**Switch(config)#show mac address-table static**

MAC Address Table

```

MAC VLAN Port Type Aging

00:02:58:4f:6c:23 10 Gi1/0/1 config static no-aging

```

Total MAC Addresses for this criterion: 1

**Switch(config)#end**

**Switch#copy running-config startup-config**

## 2.2.2 Zmiana czasu utraty ważności wpisów adresów dynamicznych

Wykonaj poniższe kroki, aby zmienić czas utraty ważności wpisów adresów dynamicznych:

Krok 1 **configure**  
Wejść w tryb konfiguracji globalnej.

**Krok 2    mac address-table aging-time aging-time**

Ustaw czas utraty ważności adresów dla wpisów adresów dynamicznych.

*aging-time*: Ustaw długość okresu, przez który po ostatnim użyciu lub aktualizacji wpis dynamiczny pozostaje w tablicy adresów MAC. Wartość musi zawierać się między 10 a 630 s. Wartość 0 oznacza wyłączoną funkcję Auto Aging. Wartość domyślna to 300. W przypadku braku pewności w kwestii wybrania najlepszego ustawienia, zaleca się zachowanie wartości domyślnej.

**Krok 3    end**

Wróć do trybu privileged EXEC.

**Krok 4    copy running-config startup-config**

Zapisz ustawienia w pliku konfiguracyjnym.

Poniższy przykład prezentuje zmianę czasu utraty ważności na 500 s. Wpis dynamiczny pozostaje na tablicy adresów MAC przez 500 s od użycia lub aktualizacji wpisu.

**Switch#configure**

**Switch(config)# mac address-table aging-time 500**

**Switch(config)#show mac address-table aging-time**

Aging time is 500 sec.

**Switch(config)#end**

**Switch#copy running-config startup-config**

## 2.2.3 Dodawanie wpisów filtrowania adresów MAC

Wykonaj poniższe kroki, aby dodać wpisy filtrowania adresów MAC:

**Krok 1    configure**

Wejdź w tryb konfiguracji globalnej.

**Krok 2    mac address-table filtering mac-addr vid vid**

Dodaj adres filtrowania do sieci VLAN.

*mac-addr*: Określ adres MAC, który będzie wykorzystywany przez przełącznik do filtrowania otrzymywanych pakietów. Pakiety z tym adresem źródłowym lub docelowym będą odrzucane przez przełącznik. Format to xx:xx:xx:xx:xx:xx, np. 00:00:00:00:00:01.

*vid*: Określ istniejącą sieć VLAN, w której pakiety z określonym adresem MAC będą odrzucane.

**Krok 3    end**

Wróć do trybu privileged EXEC.

**Krok 4    copy running-config startup-config**

Zapisz ustawienia w pliku konfiguracyjnym.

 **Uwaga:**

- W obrębie jednej sieci VLAN adresu ustawionego jako statyczny nie można już ustawić jako adres filtrowania i vice versa.
- Adresy multicast lub broadcast nie mogą być ustawione jako adresy filtrowania.

Poniższy przykład przedstawia dodawanie adresu filtrowania MAC 00:1e:4b:04:01:5d do VLAN 10. Przy tym ustawieniu przełącznik będzie odrzucał pakiet odbierany w sieci VLAN 10 z tym adresem jako źródłowym lub docelowym.

**Switch#configure**

**Switch(config)# mac address-table filtering 00:1e:4b:04:01:5d vid 10**

**Switch(config)#show mac address-table filtering**

MAC Address Table

```

MAC VLAN Port Type Aging
--- -
00:1e:4b:04:01:5d 10 filter no-aging
```

Total MAC Addresses for this criterion: 1

**Switch(config)#end**

**Switch#copy running-config startup-config**

# 3 Konfiguracja zabezpieczeń

Konfiguracja zabezpieczeń tablicy adresów MAC umożliwia:

- konfigurację komunikatów trap;
- ograniczanie liczby adresów MAC w ramach sieci VLAN

## 3.1 Przez GUI

### 3.1.1 Konfiguracja komunikatów trap

Wybierz z menu **L2 FEATURES > Switching > MAC Address > MAC Notification**, aby wyświetlić poniższą stronę.

Rys. 3-1 Konfiguracja komunikatów trap

**MAC Notification Global Config**

Global Status:  Enable

Table Full Notification:  Enable

Notification Interval:  seconds (1-1000)

[Apply](#)

---

**MAC Notification Port Config**

**UNIT1**

| <input type="checkbox"/>            | Port   | Learned Mode Change | New MAC Learned |
|-------------------------------------|--------|---------------------|-----------------|
| <input checked="" type="checkbox"/> | 1/0/1  | Disabled            | Disabled        |
| <input type="checkbox"/>            | 1/0/2  | Disabled            | Disabled        |
| <input type="checkbox"/>            | 1/0/3  | Disabled            | Disabled        |
| <input type="checkbox"/>            | 1/0/4  | Disabled            | Disabled        |
| <input type="checkbox"/>            | 1/0/5  | Disabled            | Disabled        |
| <input type="checkbox"/>            | 1/0/6  | Disabled            | Disabled        |
| <input type="checkbox"/>            | 1/0/7  | Disabled            | Disabled        |
| <input type="checkbox"/>            | 1/0/8  | Disabled            | Disabled        |
| <input type="checkbox"/>            | 1/0/9  | Disabled            | Disabled        |
| <input type="checkbox"/>            | 1/0/10 | Disabled            | Disabled        |

Total: 10      1 entry selected.

[Cancel](#)   [Apply](#)

Wykonaj poniższe kroki, aby skonfigurować komunikaty trap:

- 1) W sekcji **MAC Notification Global Config** włącz tę funkcję, skonfiguruj odpowiednie opcje i kliknij **Apply**.

|                         |                                                                                                                                                     |
|-------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|
| Global Status           | Włącz globalnie funkcję powiadomień MAC.                                                                                                            |
| Table Full Notification | Włączenie Table Full Notification spowoduje wygenerowanie powiadomienia, gdy tablica będzie pełna, a następnie wysłanie go do hosta zarządzającego. |
| Notification Interval   | Określ wartość interwału powiadomień. Jest to interwał, który reguluje wysyłanie powiadomień o nowych adresach MAC zapamiętanych na przełączniku.   |

- 2) W sekcji **MAC Notification Port Config** zaznacz co najmniej jeden port, aby skonfigurować stan powiadomień. Kliknij **Apply**.

|                     |                                                                                                                                                                                                   |
|---------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Learned Mode Change | Włączenie Learned Mode Change sprawi, że gdy zapamiętany tryb określonego portu ulegnie zmianie, wygenerowane zostanie powiadomienie, które następnie zostanie przesłane do hosta zarządzającego. |
| New MAC Learned     | Włączenie New MAC Learned sprawi, że gdy określony port nauczy się nowego adresu MAC, wygenerowane zostanie powiadomienie, które następnie zostanie przesłane do hosta zarządzającego.            |

- 3) Skonfiguruj SNMP i ustaw hosta zarządzającego. Szczegółowe informacje o konfiguracji SNMP znajdują się w części [Konfiguracja SNMP](#).

### 3.1.2 Ograniczanie liczby adresów MAC zapamiętywanych w sieciach VLAN

Wybierz z menu **L2 FEATURES > Switching > MAC Address > MAC VLAN Security**, aby wyświetlić poniższą stronę.

Rys. 3-1 Konfiguracja trybu zabezpieczeń MAC VLAN

MAC VLAN Security Config

MAC VLAN Security Mode:  Drop  Forward Apply

MAC VLAN Security Table

+ Add - Delete

| <input type="checkbox"/>  | VLAN ID | Max Learned Number | Current Learned Number | Operation |
|---------------------------|---------|--------------------|------------------------|-----------|
| No entries in this table. |         |                    |                        |           |
| Total: 0                  |         |                    |                        |           |

Wykonaj poniższe kroki, aby ustawić limit liczby adresów MAC w sieciach VLAN:

- 1) W sekcji **MAC VLAN Security Config** wybierz tryb zabezpieczeń dla wszystkich sieci VLAN.

|      |                                                                                                                    |
|------|--------------------------------------------------------------------------------------------------------------------|
| Drop | Pakiety o nowych źródłowych adresach MAC w sieci VLAN będą odrzucane, gdy przekroczony zostanie limit adresów MAC. |
|------|--------------------------------------------------------------------------------------------------------------------|



|         |                                                                                                                                    |
|---------|------------------------------------------------------------------------------------------------------------------------------------|
| Forward | Pakiety o nowych źródłowych adresach MAC będą przesyłane, ale nie będą zapamiętywane, gdy przekroczony zostanie limit adresów MAC. |
|---------|------------------------------------------------------------------------------------------------------------------------------------|

- 2) W sekcji **MAC VLAN Security Table** kliknij Add, aby wyświetlić poniższą stronę. Wprowadź wartości VLAN ID oraz Max Learned Number, aby wprowadzić ograniczenie liczby adresów MAC zapamiętywanych w określonej sieci VLAN.

Rys. 3-1 Ograniczanie liczby adresów MAC w sieciach VLAN

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| VLAN ID            | Określ sieć VLAN, dla której chcesz ograniczyć liczbę adresów MAC.                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Max Learned Number | Ustal maksymalną liczbę adresów MAC w danej sieci VLAN. Prawidłowa wartość musi mieścić się w przedziale 0 - 8192.<br><br>Możesz kontrolować dostępną powierzchnię na tablicy adresów, ustawiając maksymalną liczbę adresów MAC zapamiętywanych w sieciach VLAN. Jednak podanie nieprawidłowej liczby maksymalnej może być przyczyną niepożądanych przeciążeń sieci lub zmarnowanego miejsca na tablicy adresów. Z tego względu upewnij się przed ustawieniem limitu, że znasz topologię sieci oraz ustawienia systemowe przełącznika. |

- 3) Kliknij **Create**.

## 3.2 Przez CLI

### 3.2.1 Konfiguracja komunikatów trap

Wykonaj poniższe kroki, aby skonfigurować komunikaty trap:

|        |                                                                                                                                                                                                                                                                                                           |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Krok 1 | <b>configure</b><br>Uruchom tryb konfiguracji globalnej.                                                                                                                                                                                                                                                  |
| Krok 2 | <b>mac address-table notification global-status {enable   disable}</b><br>Globalne włączanie powiadomień MAC.<br>enable   disable: Włącz lub wyłącz MAC Notification globally.                                                                                                                            |
| Krok 3 | <b>mac address-table notification table-full-status [enable   disable]</b><br>Włącz opcję Table Full Notification (opcjonalnie).<br>enable   disable: Włączenie Table Full Notification spowoduje wygenerowanie powiadomienia, gdy tablica będzie pełna, a następnie wysłanie go do hosta zarządzającego. |

|        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Krok 4 | <p><b>mac address-table notification interval <i>time</i></b></p> <p>Określ wartość interwału powiadomień. Jest to interwał, który reguluje wysyłanie powiadomień o nowych adresach MAC zapamiętanych na przełączniku.</p> <p><i>time</i>: Określ sekundową wartość interwału powiadomień, wybierając z przedziału 1 - 1000. Domyślną wartością jest 1 sekunda.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Krok 5 | <p><b>interface { fastEthernet <i>port</i>   range fastEthernet <i>port-list</i>   gigabitEthernet <i>port</i>   range gigabitEthernet <i>port-list</i>   ten-gigabitEthernet <i>port</i>   ten-range gigabitEthernet <i>port-list</i> }</b></p> <p>Skonfiguruj komunikaty trap dla określonego portu.</p> <p><i>port/ port-list</i>: Numer lub lista portów Ethernet, dla których chcesz skonfigurować komunikaty trap.</p>                                                                                                                                                                                                                                                                                                                                                                                    |
| Krok 6 | <p><b>mac address-table notification {[learn-mode-change enable   disable] [new-mac-learned enable   disable]}</b></p> <p>Włączanie learn-mode-change, exceed-max-learned lub new-MAC-learned komunikatów trap dla określonego portu.</p> <p><i>enable   disable</i>: Włącz lub wyłącz learn-mode-change, exceed-max-learned lub new-MAC-learned komunikatów trap dla określonego portu.</p> <p><b>learn-mode-change</b>: W przypadku włączenia learn-mode-change, gdy tryb uczenia danego portu ulegnie zmianie, powiadomienie zostanie wygenerowane, a następnie przesłane do hosta zarządzającego.</p> <p><b>new-mac-learned</b>: W przypadku włączenia new-mac-learned, gdy dany port nauczy się nowego adresu MAC, powiadomienie zostanie wygenerowane, a następnie przesłane do hosta zarządzającego.</p> |
| Krok 7 | <p><b>end</b></p> <p>Powrót do trybu privileged EXEC.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Krok 8 | <p><b>copy running-config startup-config</b></p> <p>Zapisz ustawienia w pliku konfiguracyjnym.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |

Komunikaty trap zostały skonfigurowane. W celu otrzymywania powiadomień konieczne jest włączenie funkcji SNMP i ustawienie hosta zarządzającego. Szczegółowe informacje dotyczące konfiguracji SNMP znajdziesz w części [Konfiguracja SNMP](#).

Poniższy schemat przedstawia przykładowy sposób włączania new-MAC-learned komunikatu trap dla portu 1 oraz ustawienia interwału jako 10 sekund. Po skonfigurowaniu funkcji SNMP przełącznik co 10 sekund będzie łączył powiadomienia o nowych adresach i wysyłać je do hosta zarządzającego.

### Switch#configure

```
Switch(config)#mac address-table notification global-status enable
```

```
Switch(config)#mac address-table notification interval 10
```

```
Switch(config)#interface gigabitEthernet 1/0/1
```

```
Switch(config-if)#mac address-table notification new-mac-learned enable
```

```
Switch(config-if)#show mac address-table notification interface gigabitEthernet 1/0/1
```

```
Mac Notification Global Config
```

Notification Global Status : enable

Table Full Notification Status: disable

Notification Interval : 10

| Port    | LrnMode Change | New Mac Learned |
|---------|----------------|-----------------|
| ----    | -----          | -----           |
| Gi1/0/1 | disable        | enable          |

**Switch(config-if)#end**

**Switch#copy running-config startup-config**

### 3.2.2 Ograniczanie liczby adresów MAC w sieciach VLAN

Wykonaj poniższe kroki, aby ograniczyć liczbę adresów MAC w sieciach VLAN:

|        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Krok 1 | <b>configure</b><br>Uruchom tryb konfiguracji globalnej.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Krok 2 | <b>mac address-table vlan-security mode {drop   forward}</b><br>Ustaw tryb zabezpieczeń VLAN dla wszystkich sieci VLAN.<br><br><i>drop   forward:</i> Tryb, który jest uruchamiany na przełączniku po przekroczeniu maksymalnej liczby adresów MAC danej sieci VLAN.<br><i>drop:</i> Pakiety o nowych źródłowych adresach MAC w sieci VLAN będą odrzucane, gdy przekroczony zostanie limit adresów MAC danej sieci VLAN.<br><i>forward:</i> Pakiety o nowych źródłowych adresach MAC będą przesyłane, ale nie będą zapamiętywane, gdy przekroczony zostanie limit adresów MAC danej sieci VLAN. |
| Krok 3 | <b>mac address-table vlan-security vid vid max-learn num</b><br>Skonfiguruj maksymalną liczbę adresów MAC w danej sieci VLAN i wybierz tryb, który będzie uruchamiany na przełączniku po przekroczeniu ustalonego limitu.<br><br><i>vid:</i> Określ sieć VLAN, dla której chcesz ograniczyć liczbę adresów MAC.<br><i>num:</i> Ustal maksymalną liczbę adresów MAC w danej sieci VLAN. Prawidłowa wartość musi mieścić się w przedziale 0 - 8192.                                                                                                                                               |
| Krok 4 | <b>end</b><br>Powróć do trybu privileged EXEC.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Krok 5 | <b>copy running-config startup-config</b><br>Zapisz ustawienia w pliku konfiguracyjnym.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |

Poniższy schemat przedstawia przykładowy sposób ograniczania liczby adresów MAC do 100 w sieci VLAN 10 i konfiguracji przełącznika tak, aby odrzucał pakiety o nowych źródłowych adresach MAC po przekroczeniu limitu.

**Switch#configure**

**Switch(config)#mac address-table vlan-security mode drop**

```
Switch(config)#mac address-table vlan-security vid 10 max-learn 100
```

```
Switch(config)#show mac address-table vlan-security vid 10
```

| VlanId | Max-learn | Current-learn | Status |
|--------|-----------|---------------|--------|
| -----  | -----     | -----         | -----  |
| 10     | 100       | 0             | Drop   |

```
Switch(config)#end
```

```
Switch#copy running-config startup-config
```

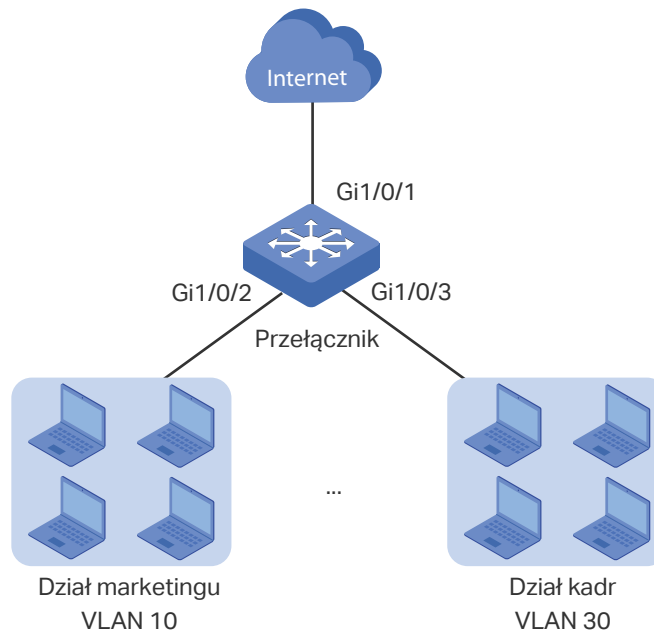
# 4 Przykład konfiguracji zabezpieczeń

## 4.1 Wymagania sieciowe

Z siecią firmową połączonych jest kilka działów, tak jak przedstawiono to na rys. 4-1. Dział marketingu, który jest połączony z siecią VLAN 10, ma następujące wymagania sieciowe:

- Wyeliminowanie możliwości nielegalnego uzyskania dostępu do systemu sieci i ataków na adresy MAC poprzez ograniczenie liczby użytkowników do 100.
- Wsparcie administratora sieci poprzez wysyłanie powiadomień o nowych użytkownikach, którzy uzyskali dostęp do sieci.

Rys. 4-1 Topologia sieci



## 4.2 Schemat konfiguracji

W celu ograniczenia liczby użytkowników i tym samym zapobiegnięciu nielegalnemu uzyskiwaniu dostępu oraz atakom na adresy MAC zaleca się skonfigurować zabezpieczenia VLAN.

Konfiguracja powiadomień MAC oraz funkcji SNMP pozwala na monitorowanie interfejsu, z którego korzysta dział marketingu. Włączenie powiadomień new-MAC-learned oraz funkcji SNMP umożliwia administratorowi sieci otrzymywanie powiadomień o dołączeniu do sieci nowych użytkowników.

W poniższych podrozdziałach opisano dwa sposoby przeprowadzenia procedury konfiguracji: przez GUI oraz przez CL.

## 4.3 Przez GUI

- 1) Wybierz z menu **L2 FEATURES > Switching > MAC Address > MAC VLAN Security** i kliknij **Add**, aby wyświetlić poniższą stronę. Ustaw maksymalną liczbę adresów w sieci VLAN 10 jako 100, wybierz tryb drop i kliknij **Create**.

Rys. 4-2 Konfiguracja zabezpieczeń VLAN

VLAN Security Config

VLAN ID:  (1-4094)

Max Learned Number:  (0-8192)

- 2) Wybierz z menu **L2 FEATURES > Switching > MAC Address > MAC Notification**, aby wyświetlić poniższą stronę. Włącz Global Status, ustaw notification interval jako 10 sekund i kliknij **Apply**. Następnie włącz new-mac-learned trap na porcie 1/0/2 i kliknij **Apply**.

Rys. 4-3 Konfiguracja New-MAC-learned komunikatów trap

MAC Notification Global Config

Global Status:  Enable

Table Full Notification:  Enable


Notification Interval:  seconds (1-1000)

MAC Notification Port Config

UNIT1

| <input type="checkbox"/>            | Port   | Learned Mode Change | New MAC Learned |
|-------------------------------------|--------|---------------------|-----------------|
| <input type="checkbox"/>            | 1/0/1  | Disabled            | Disabled        |
| <input checked="" type="checkbox"/> | 1/0/2  | Disabled            | Enabled         |
| <input type="checkbox"/>            | 1/0/3  | Disabled            | Disabled        |
| <input type="checkbox"/>            | 1/0/4  | Disabled            | Disabled        |
| <input type="checkbox"/>            | 1/0/5  | Disabled            | Disabled        |
| <input type="checkbox"/>            | 1/0/6  | Disabled            | Disabled        |
| <input type="checkbox"/>            | 1/0/7  | Disabled            | Disabled        |
| <input type="checkbox"/>            | 1/0/8  | Disabled            | Disabled        |
| <input type="checkbox"/>            | 1/0/9  | Disabled            | Disabled        |
| <input type="checkbox"/>            | 1/0/10 | Disabled            | Disabled        |

Total: 10 1 entry selected.

- 3) Kliknij  **Save**, aby zapisać ustawienia.
- 4) Włącz funkcję SNMP i ustaw hosta zarządzającego. Szczegółowe informacje dotyczące konfiguracji SNMP znajdują się w części *Konfiguracja SNMP*.

## 4.4 Przez CLI

- 1) Ustaw maksymalną liczbę adresów MAC w sieci VLAN 10 jako 100 i wybierz tryb drop.

```
Switch#configure
```

```
Switch(config)#mac address-table vlan-security mode drop
```

```
Switch(config)#mac address-table vlan-security vid 10 max-learn 100
```

- 2) Skonfiguruj new-MAC-learned trap na porcie 1/0/2 i ustaw notification interval jako 10 sekund.

```
Switch(config)#mac address-table notification global-status enable
```

```
Switch(config)#mac address-table notification interval 10
```

```
Switch(config)#interface gigabitEthernet 1/0/2
```

```
Switch(config-if)#mac address-table notification new-mac-learned enable
```

```
Switch(config-if)#end
```

```
Switch#copy running-config startup-config
```

- 3) Skonfiguruj funkcję SNMP i ustaw hosta zarządzającego. Szczegółowe informacje dotyczące konfiguracji SNMP znajdują się w części *Konfiguracja SNMP*.

### Sprawdzanie konfiguracji

Sprawdzanie konfiguracji zabezpieczeń VLAN.

```
Switch#show mac address-table vlan-security vid 10
```

| VlanId | Max-learn | Current-learn | Status |
|--------|-----------|---------------|--------|
| 10     | 100       | 0             | Drop   |

Sprawdzanie konfiguracji powiadomień MAC na porcie 1/0/2.

```
Switch#show mac address-table notification interface gigabitEthernet 1/0/2
```

| Port    | LrnMode Change | New Mac Learned |
|---------|----------------|-----------------|
| Gi1/0/2 | disable        | enable          |

# Część 7

## Konfiguracja 802.1Q VLAN

### ROZDZIAŁY

1. Informacja ogólne
2. Konfiguracja 802.1Q VLAN
3. Przykład konfiguracji



# 1 Informacje ogólne

VLAN (Virtual Local Area Network) to technika sieci, która rozwiązuje problemy z transmisją w sieciach lokalnych. Stosowana jest najczęściej w następujących przypadkach:

- W celu ograniczenia domen rozgłoszeniowych: Technika VLAN pozwala na podział dużych obszarów sieci lokalnej na kilka VLAN-ów, a cały ruch VLAN-a ogranicza się do danej sieci. Zmniejsza to wpływ ruchu rozgłoszeniowego sieci warstwy 2 na całą sieć.
- W celu zwiększenia bezpieczeństwa sieci: Urządzenia z różnych sieci VLAN nie mogą zbudować komunikacji w warstwie 2, dlatego użytkownicy mogą grupować i izolować urządzenia w celu zwiększenia bezpieczeństwa sieci.
- W celu uproszczenia zarządzania: Sieci VLAN grupują urządzenia w sposób logiczny, a nie fizyczny, dlatego urządzenia w tej samej sieci VLAN nie muszą być zlokalizowane w tym samym miejscu. Ułatwia to zatem zarządzanie urządzeniami będących w tej samej grupie roboczej, ale w innej lokalizacji.

# 2 Konfiguracja 802.1Q VLAN

Aby przeprowadzić konfigurację 802.1Q VLAN, wykonaj poniższe kroki:

- 1) Skonfiguruj parametry portu;
- 2) Skonfiguruj sieć VLAN - utwórz sieć VLAN i dodaj do sieci skonfigurowane porty.

## 2.1 Przez GUI

### 2.1.1 Konfiguracja PVID portów

Wybierz z menu **L2 FEATURES > VLAN > 802.1Q VLAN > Port Config**, aby wyświetlić poniższą stronę.

Rys. 2-1 Konfiguracja portu

| UNIT1                               |        | LAGS |                  |                        |     |                         |
|-------------------------------------|--------|------|------------------|------------------------|-----|-------------------------|
| <input type="checkbox"/>            | Port   | PVID | Ingress Checking | Acceptable Frame Types | LAG | Details                 |
| <input checked="" type="checkbox"/> | 1/0/1  | 1    | Enabled          | Admit All              | --- | <a href="#">Details</a> |
| <input type="checkbox"/>            | 1/0/2  | 1    | Enabled          | Admit All              | --- | <a href="#">Details</a> |
| <input type="checkbox"/>            | 1/0/3  | 1    | Enabled          | Admit All              | --- | <a href="#">Details</a> |
| <input type="checkbox"/>            | 1/0/4  | 1    | Enabled          | Admit All              | --- | <a href="#">Details</a> |
| <input type="checkbox"/>            | 1/0/5  | 1    | Enabled          | Admit All              | --- | <a href="#">Details</a> |
| <input type="checkbox"/>            | 1/0/6  | 1    | Enabled          | Admit All              | --- | <a href="#">Details</a> |
| <input type="checkbox"/>            | 1/0/7  | 1    | Enabled          | Admit All              | --- | <a href="#">Details</a> |
| <input type="checkbox"/>            | 1/0/8  | 1    | Enabled          | Admit All              | --- | <a href="#">Details</a> |
| <input type="checkbox"/>            | 1/0/9  | 1    | Enabled          | Admit All              | --- | <a href="#">Details</a> |
| <input type="checkbox"/>            | 1/0/10 | 1    | Enabled          | Admit All              | --- | <a href="#">Details</a> |

Total: 10      1 entry selected.      [Cancel](#)      [Apply](#)

Wybierz port i skonfiguruj jego parametry. Kliknij **Apply**.

#### PVID

Ustaw domyślny VLAN ID portu. Prawidłowe wartości wahają się od 1 do 4094.

Gdy port odbiera pakiet nietagowany, przełącznik oznacza pakiet tagiem VLAN w oparciu o PVID.


#### Ingress Checking

Kontrola na wejściu. Jeżeli włączysz tę funkcję, port będzie przyjmować tylko te pakiety, których VLAN ID znajdują się na liście VLAN portu, a inne będzie odrzucać. Jeżeli wyłączysz tę funkcję, port będzie przesyłać wszystkie pakiety.

|                        |                                                                                                                                                                                                                                                                                                           |
|------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Acceptable Frame Types | <p>Wybierz dopuszczalny typ ramki dla portu, a port będzie przeprowadzać to działanie przed uruchomieniem kontroli na wejściu.</p> <p><b>Admit All:</b> Port będzie przyjmować zarówno pakiety tagowane, jak i nietagowane.</p> <p><b>Tagged Only:</b> Port będzie przyjmować tylko pakiety tagowane.</p> |
| LAG                    | LAG (Link Aggregation Group), do której należy port.                                                                                                                                                                                                                                                      |
| Details                | Kliknij przycisk Details, aby zobaczyć sieci VLAN, do których należy port.                                                                                                                                                                                                                                |

---

## 2.1.2 Konfiguracja VLAN

Wybierz z menu **L2 FEATURES > VLAN > 802.1Q VLAN > VLAN Config** i kliknij  Add, aby wyświetlić poniższą stronę.

Rys. 2-2 Konfiguracja VLAN

VLAN Config

VLAN ID:  (2-4094, format: 2,4-5,8)

VLAN Name:  (1-16 characters)

**Untagged Ports**

---

Port:  (Format: 1/0/1, input or choose below)

UNIT1

1

2

3

4

5

6

7


8


LAGS


9

10

Select All

 Selected

 Unselected

 Not Available

**Tagged Ports**

---

Port:  (Format: 1/0/1, input or choose below)

UNIT1

1

2

3

4

5

6

7

8

LAGS

9

10

Select All

Cancel

Create

Wykonaj poniższe kroki, aby skonfigurować sieć VLAN:

- 1) Uzupełnij VLAN ID i opis identyfikacyjny, aby stworzyć sieć VLAN.

|           |                                                                       |
|-----------|-----------------------------------------------------------------------|
| VLAN ID   | Uzupełnij identyfikacyjny VLAN ID wartością z przedziału 2 - 4094.    |
| VLAN Name | Uzupełnij opis identyfikacyjny sieci VLAN, wprowadzając do 16 znaków. |

- 2) Wybierz odpowiednio port(y) tagowany(e) i port(y) nietagowany(e), aby dodać je do utworzonej sieci VLAN, w oparciu o topologię sieci.

|               |                                                                          |
|---------------|--------------------------------------------------------------------------|
| Untagged port | Wybrane porty będą przysyłać pakiety nietagowane w docelowej sieci VLAN. |
| Tagged port   | Wybrane porty będą przysyłać pakiety tagowane w docelowej sieci VLAN.    |

- 3) Kliknij **Apply**.

## 2.2 Przez CLI

### 2.2.1 Tworzenie sieci VLAN

Wykonaj poniższe kroki, aby utworzyć sieć VLAN:

|        |                                                                                                                                                                                                                                                                                                                                                                     |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Krok 1 | <b>configure</b><br>Uruchom tryb konfiguracji globalnej.                                                                                                                                                                                                                                                                                                            |
| Krok 2 | <b>vlan <i>vlan-list</i></b><br>Gdy wpisujesz nowy VLAN ID, przełącznik tworzy nową sieć VLAN i uruchamia tryb konfiguracji VLAN. Gdy wpisujesz istniejący VLAN ID, przełącznik bezpośrednio uruchamia tryb konfiguracji VLAN.<br><i>vlan-list</i> : Podaj ID lub ułóż listę ID sieci VLAN do konfiguracji. Prawidłowe wartości wahają się od 2 do 4094, np. 2-3,5. |
| Krok 3 | <b>name <i>descript</i></b><br>(Opcjonalnie) Uzupełnij identyfikacyjny opis VLAN.<br><i>descript</i> : Długość opisu musi mieścić się w zakresie 1 - 16 znaków.                                                                                                                                                                                                     |
| Krok 4 | <b>show vlan [ id <i>vlan-list</i> ]</b><br>Wyświetl globalne informacje określonych sieci VLAN. Jeżeli nie określisz żadnych sieci VLAN, polecenie wyświetli globalne informacje o wszystkich sieciach 802.1Q VLAN.<br><i>vlan-list</i> : Podaj ID lub ułóż listę ID sieci VLAN do konfiguracji. Prawidłowe wartości wahają się od 1 do 4094.                      |
| Krok 5 | <b>end</b><br>Powróć do trybu privileged EXEC.                                                                                                                                                                                                                                                                                                                      |
| Krok 6 | <b>copy running-config startup-config</b><br>Zapisz ustawienia w pliku konfiguracyjnym.                                                                                                                                                                                                                                                                             |

Poniższy schemat przedstawia przykładowy sposób utworzenia sieci VLAN 2 o nazwie RD:

```
Switch#configure
```

```
Switch(config)#vlan 2
```

```
Switch(config-vlan)#name RD
```

```
Switch(config-vlan)#show vlan id 2
```

```
VLAN Name Status Ports

2 RD active
```

```
Switch(config-vlan)#end
```

```
Switch#copy running-config startup-config
```

## 2.2.2 Konfiguracja portu

Wykonaj poniższe kroki, aby skonfigurować port:

|        |                                                                                                                                                                                                                                                                                                                                                                      |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Krok 1 | <b>configure</b><br>Uruchom tryb konfiguracji globalnej.                                                                                                                                                                                                                                                                                                             |
| Krok 2 | <b>interface {fastEthernet <i>port</i>   range fastEthernet <i>port-list</i>   gigabitEthernet <i>port</i>   range gigabitEthernet <i>port-list</i>   ten-gigabitEthernet <i>port</i>   range ten-gigabitEthernet <i>port-list</i>   port-channel <i>port-channel-id</i>   range port-channel <i>port-channel-list</i>}</b><br>Uruchom tryb konfiguracji interfejsu. |
| Krok 3 | <b>switchport pvid <i>vlan-id</i></b><br>Skonfiguruj PVID portu(ów). Domyślną wartością jest 1.<br><i>vlan-id</i> : Domyślny VLAN ID portu o wartości z zakresu 1 - 4094.                                                                                                                                                                                            |
| Krok 4 | <b>switchport check ingress</b><br>Kontrola na wejściu. Jeżeli włączysz tę funkcję, port będzie przyjmować tylko te pakiety, których VLAN ID znajdują się na liście VLAN portu, a inne będzie odrzucać. Jeżeli wyłączysz tę funkcję, port będzie przesyłać wszystkie pakiety.                                                                                        |
| Krok 5 | <b>switchport acceptable frame {all   tagged}</b><br>Wybierz dopuszczalny typ ramki dla portu, a port będzie przeprowadzać to działanie przed uruchomieniem kontroli na wejściu.<br><b>all</b> : Port będzie przyjmować zarówno pakiety tagowane, jak i nietagowane.<br><b>tagged</b> : Port będzie przyjmować tylko pakiety tagowane.                               |
| Krok 6 | <b>end</b><br>Powróć do trybu privileged EXEC mode.                                                                                                                                                                                                                                                                                                                  |
| Krok 7 | <b>copy running-config startup-config</b><br>Zapisz ustawienia w pliku konfiguracyjnym.                                                                                                                                                                                                                                                                              |

Poniższy schemat przedstawia przykładowy sposób konfiguracji PVID portu 1/0/5 jako 2, włączania kontroli na wejściu i ustawiania odpowiedniego typu ramki jako all:

```
Switch#configure
```

```
Switch(config)#interface gigabitEthernet 1/0/5
```

```
Switch(config-if)#switchport pvid 2
```

```
Switch(config-if)#switchport check ingress
```

```
Switch(config-if)#switchport acceptable frame all
```

```
Switch(config-if)#show interface switchport gigabitEthernet 1/0/5
```

```
Port Gi1/0/5:
```

```
PVID: 2
```

```
Acceptable frame type: All
```

```
Ingress Checking: Enable
```

```
Member in LAG: N/A
```

```
Link Type: General
```

```
Member in VLAN:
```

```
Vlan Name Egress-rule
```

```
----- -
```

```
1 System-VLAN Untagged
```

```
Switch(config-if)#end
```

```
Switch#copy running-config startup-config
```

## 2.2.3 Dodawanie portu do określonej sieci VLAN

Wykonaj poniższe kroki, aby dodać port do określonej sieci VLAN:

|        |                                                                                                                                                                                                                                                                                                                                                                      |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Krok 1 | <b>configure</b><br>Uruchom tryb konfiguracji globalnej.                                                                                                                                                                                                                                                                                                             |
| Krok 2 | <b>interface {fastEthernet <i>port</i>   range fastEthernet <i>port-list</i>   gigabitEthernet <i>port</i>   range gigabitEthernet <i>port-list</i>   ten-gigabitEthernet <i>port</i>   range ten-gigabitEthernet <i>port-list</i>   port-channel <i>port-channel-id</i>   range port-channel <i>port-channel-list</i>}</b><br>Uruchom tryb konfiguracji interfejsu. |
| Krok 3 | <b>switchport general allowed vlan <i>vlan-list</i> { tagged   untagged }</b><br>Dodaj porty do określonej sieci VLAN.<br><i>vlan-list</i> : Podaj ID lub ułóż listę ID sieci VLAN, do których porty będą dodawane. Wartość ID waha się od 1 do 4094.<br>tagged   untagged: Wybierz regułę wyjścia dla portu.                                                        |
| Krok 4 | <b>show interface switchport [fastEthernet <i>port</i>   gigabitEthernet <i>port</i>   ten-gigabitEthernet <i>port</i>   port-channel <i>lag-id</i>]</b><br>Zweryfikuj informacje o porcie.                                                                                                                                                                          |
| Krok 5 | <b>end</b><br>Powróć do trybu privileged EXEC.                                                                                                                                                                                                                                                                                                                       |

---

**Krok 6      copy running-config startup-config**Zapisz ustawienia w pliku konfiguracyjnym.

---

Poniższy schemat przedstawia przykładowy sposób dodawania portu 1/0/5 do sieci VLAN 2, i określania jego reguły wyjścia jako tagowanej:

**Switch#configure****Switch(config)#interface gigabitEthernet 1/0/5****Switch(config-if)#switchport general allowed vlan 2 tagged****Switch(config-if)#show interface switchport gigabitEthernet 1/0/5**

Port Gi1/0/5:

PVID: 2

Acceptable frame type: All

Ingress Checking: Enable

Member in LAG: N/A

Link Type: General

Member in VLAN:

| Vlan | Name        | Egress-rule |
|------|-------------|-------------|
| ---- | -----       | -----       |
| 1    | System-VLAN | Untagged    |
| 2    | RD          | Tagged      |

**Switch(config-if)#end****Switch#copy running-config startup-config**



# 3 Przykład konfiguracji

## 3.1 Wymagania sieciowe

- Biura działu A oraz działu B firmy mają różne lokalizacje, ale niektóre komputery w tych biurach łączą się z tym samym przełącznikiem.
- Wymagane jest, aby komputery komunikowały się ze sobą w ramach tego samego działu, ale niedozwolona jest komunikacja międzydziałowa.

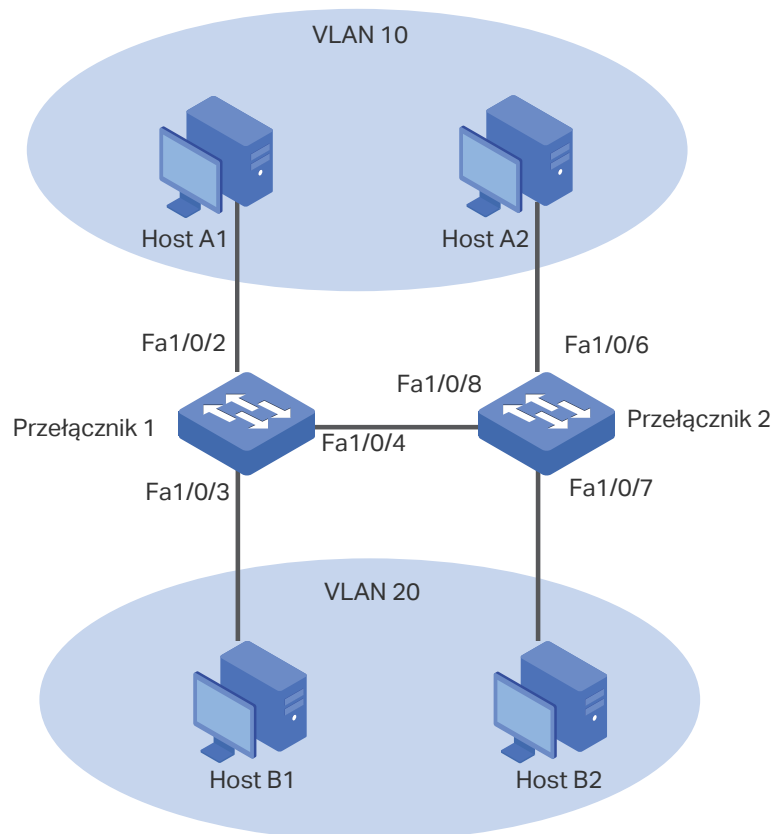
## 3.2 Schemat konfiguracji

- Podziel komputery z działu A i działu B odpowiednio na dwie sieci VLAN tak, aby komputery mogły się ze sobą komunikować wyłącznie w ramach tego samego działu.
- Urządzenia końcowe, takie jak komputery, nie obsługują zwykle tagowania VLAN. Dodaj nietagowane porty do odpowiednich sieci VLAN i określ ich PVID.
- Łącze pośrednie między dwoma przełącznikami przenosi ruch z dwóch sieci VLAN jednocześnie. Dodaj porty tagowane do obu sieci VLAN.

### 3.3 Topologia sieci

Poniższy schemat przedstawia topologię sieci. Host A1 oraz host A2 są w dziale A, natomiast host B1 oraz host B2 są w dziale B. Przełącznik 1 oraz przełącznik 2 mają różne lokalizacje. Host A1 oraz host B1 podłączeni są odpowiednio do portu 1/0/2 oraz 1/0/3 przełącznika 1, natomiast host A2 oraz host B2 podłączeni są odpowiednio do portu 1/0/6 oraz 1/0/7 przełącznika 2. Port 1/0/4 przełącznika 1 jest połączony z portem 1/0/8 przełącznika 2.


Rys. 3-1 Topologia sieci



W poniższych podrozdziałach opisano dwa sposoby przeprowadzenia procedury konfiguracji: przez GUI oraz przez CLI.

### 3.4 Przez GUI

Ustawienia przełącznika 1 i przełącznika 2 są podobne. W poniższym przykładzie omawiamy ustawienia przełącznika 1

- 1) Wybierz z menu **L2 FEATURES > VLAN > 802.1Q VLAN > VLAN Config** i kliknij  **Add** aby wyświetlić poniższą stronę. Utwórz VLAN 10 o nazwie Department\_A. Dodaj do VLAN 10 port 1/0/2 jako port nietagowany oraz port 1/0/4 jako port tagowany. Kliknij **Create**.

Rys. 3-2 Tworzenie VLAN 10 dla działu A

### VLAN Config

VLAN ID:  (2-4094, format: 2,4-5,8)

VLAN Name:  (1-16 characters)

#### Untagged Ports

Port:  (Format: 1/0/1, input or choose below)

Select All

UNIT1 LAGS

1  2  3  4  5  6  7  8  9  10

Selected  Unselected  Not Available

#### Tagged Ports

Port:  (Format: 1/0/1, input or choose below)

Select All

UNIT1 LAGS

1  2  3  4  5  6  7  8  9  10

- 2) Wybierz z menu **L2 FEATURES > VLAN > 802.1Q VLAN > VLAN Config** i kliknij **+** Add aby wyświetlić poniższą stronę. Utwórz VLAN 20 o nazwie Department\_B. Dodaj do sieci VLAN 20 port 1/0/3 jako port nietagowany oraz port 1/0/4 jako port tagowany. Kliknij **Create**.

Rys. 3-2 Tworzenie VLAN 20 dla działu B

### VLAN Config

VLAN ID:  (2-4094, format: 2,4-5,8)

VLAN Name:  (1-16 characters)

#### Untagged Ports

Port:  (Format: 1/0/1, input or choose below)

Select All

UNIT1 LAGS

1 2 3 4 5 6 7 8 9 10

Selected Unselected Not Available

#### Tagged Ports

Port:  (Format: 1/0/1, input or choose below)

Select All

UNIT1 LAGS

1 2 3 4 5 6 7 8 9 10

- Wybierz z menu **L2 FEATURES > VLAN > 802.1Q VLAN > Port Config**, aby wyświetlić poniższą stronę. Ustaw PVID portu 1/0/2 jako 10 i kliknij **Apply**. Ustaw PVID portu 1/0/3 jako 20 i kliknij **Apply**.

Rys. 3-4 Ustalanie PVID portów

Port Config

UNIT1 LAGS

| <input type="checkbox"/>            | Port   | PVID | Ingress Checking | Acceptable Frame Types | LAG | Details                 |
|-------------------------------------|--------|------|------------------|------------------------|-----|-------------------------|
|                                     |        | 20   |                  |                        |     |                         |
| <input type="checkbox"/>            | 1/0/1  | 1    | Enabled          | Admit All              | --- | <a href="#">Details</a> |
| <input type="checkbox"/>            | 1/0/2  | 10   | Enabled          | Admit All              | --- | <a href="#">Details</a> |
| <input checked="" type="checkbox"/> | 1/0/3  | 20   | Enabled          | Admit All              | --- | <a href="#">Details</a> |
| <input type="checkbox"/>            | 1/0/4  | 1    | Enabled          | Admit All              | --- | <a href="#">Details</a> |
| <input type="checkbox"/>            | 1/0/5  | 1    | Enabled          | Admit All              | --- | <a href="#">Details</a> |
| <input type="checkbox"/>            | 1/0/6  | 1    | Enabled          | Admit All              | --- | <a href="#">Details</a> |
| <input type="checkbox"/>            | 1/0/7  | 1    | Enabled          | Admit All              | --- | <a href="#">Details</a> |
| <input type="checkbox"/>            | 1/0/8  | 1    | Enabled          | Admit All              | --- | <a href="#">Details</a> |
| <input type="checkbox"/>            | 1/0/9  | 1    | Enabled          | Admit All              | --- | <a href="#">Details</a> |
| <input type="checkbox"/>            | 1/0/10 | 1    | Enabled          | Admit All              | --- | <a href="#">Details</a> |

Total: 10 1 entry selected. Cancel Apply

4) Kliknij  Save, aby zapisać ustawienia.

## 3.5 Przez CLI

Ustawienia przełącznika 1 i przełącznika 2 są podobne. W poniższym przykładzie omawiamy ustawienia przełącznika 1.

- 1) Utwórz VLAN 10 dla działu A i ustaw dla niej nazwę Department-A. W ten sam sposób utwórz VLAN 20 dla działu B i ustaw dla niej nazwę Department-B.

```
Switch_1#configure
```

```
Switch_1(config)#vlan 10
```

```
Switch_1(config-vlan)#name Department-A
```

```
Switch_1(config-vlan)#exit
```

```
Switch_1(config)#vlan 20
```

```
Switch_1(config-vlan)#name Department-B
```

```
Switch_1(config-vlan)#exit
```

- 2) Dodaj do VLAN 10 nietagowany port 1/0/2 i tagowany port 1/0/4. Dodaj do VLAN 20 nietagowany port 1/0/3 i tagowany port 1/0/4.

```
Switch_1(config)#interface gigabitEthernet 1/0/2
```

```
Switch_1(config-if)#switchport general allowed vlan 10 untagged
```

```
Switch_1(config-if)#exit
```

```
Switch_1(config)#interface gigabitEthernet 1/0/3
Switch_1(config-if)#switchport general allowed vlan 20 untagged
Switch_1(config-if)#exit
Switch_1(config)#interface gigabitEthernet 1/0/4
Switch_1(config-if)#switchport general allowed vlan 10 tagged
Switch_1(config-if)#switchport general allowed vlan 20 tagged
Switch_1(config-if)#exit
```

- 3) Ustaw PVID portu 1/0/2 jako 10, a PVID portu 1/0/3 jako 20.

```
Switch_1(config)#interface gigabitEthernet 1/0/2
Switch_1(config-if)#switchport pvid 10
Switch_1(config-if)#exit
Switch_1(config)#interface gigabitEthernet 1/0/3
Switch_1(config-if)#switchport pvid 20
Switch_1(config-if)#end
Switch_1#copy running-config startup-config
```

## Sprawdzanie konfiguracji

Sprawdzanie konfiguracji VLAN:

```
Switch_1#show vlan
```

| VLAN | Name         | Status | Ports                                                                                           |
|------|--------------|--------|-------------------------------------------------------------------------------------------------|
| 1    | System-VLAN  | active | Gi1/0/1, Gi1/0/2, Gi1/0/3, Gi1/0/4,<br>Gi1/0/5, Gi1/0/6, Gi1/0/7, Gi1/0/8,<br>Gi1/0/9, Gi1/0/10 |
| 10   | Department-A | active | Gi1/0/2, Gi1/0/4                                                                                |
| 20   | Department-B | active | Gi1/0/3, Gi1/0/4                                                                                |

Sprawdzanie konfiguracji VLAN:

```
Switch_1(config)#show interface switchport
```

| Port  | LAG | Type | PVID | Acceptable frame type | Ingress Checking |
|-------|-----|------|------|-----------------------|------------------|
| ----- | --- | ---- | ---- | -----                 | -----            |

---

|         |     |         |    |     |        |
|---------|-----|---------|----|-----|--------|
| Gi1/0/1 | N/A | General | 1  | All | Enable |
| Gi1/0/2 | N/A | General | 10 | All | Enable |
| Gi1/0/3 | N/A | General | 20 | All | Enable |
| Gi1/0/4 | N/A | General | 1  | All | Enable |
| Gi1/0/5 | N/A | General | 1  | All | Enable |
| .....   |     |         |    |     |        |

# Część 8

## Konfiguracja MAC VLAN

### ROZDZIAŁY

1. Informacje ogólne
2. Konfiguracja MAC VLAN
3. Przykład konfiguracji

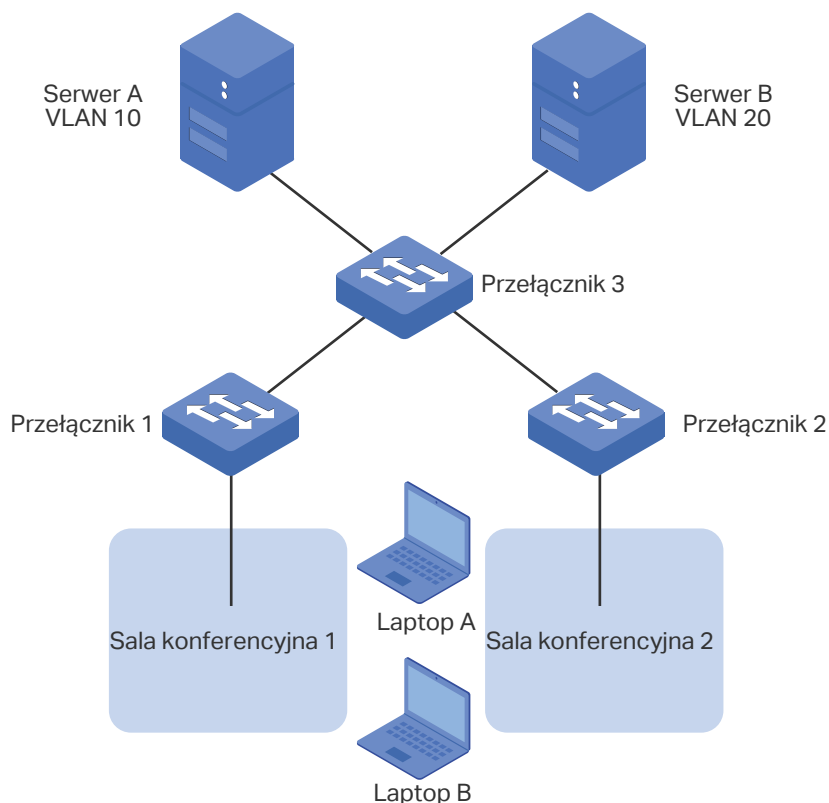


# 1 Informacje ogólne

Sieć VLAN jest z założenia dzielona na porty. Jest to najczęściej stosowany typ podziału, ale nie jest odpowiedni dla sieci, których topologia podlega częstym zmianom. Ze względu na coraz częstsze stosowanie urządzeń mobilnych w biurze urządzenia końcowe mogą łączyć się z siecią korzystając z różnych portów. Na przykład urządzenie końcowe, które ostatnim razem uzyskało dostęp do przełącznika poprzez port 1, tym razem może skorzystać z portu 2. Jeśli port 1 i port 2 należą do różnych sieci VLAN, użytkownik musi ponownie skonfigurować przełącznik, aby uzyskać dostęp do pierwotnej sieci VLAN. Korzystanie z MAC VLAN może rozwiązać ten problem. Funkcja ta dzieli sieci VLAN na podstawie adresów MAC urządzeń końcowych. W ten sposób urządzenia końcowe zawsze przynależą do sieci VLAN swojego adresu MAC, nawet gdy ich port dostępu ulegnie zmianie.

Poniższy schemat przedstawia często stosowane rozwiązanie z wykorzystaniem funkcji MAC VLAN.

Rys 1-1 Często stosowane rozwiązanie z wykorzystaniem funkcji MAC VLAN



Działy firmy korzystają ze wszystkich sal konferencyjnych, ale używają innych serwerów i laptopów. Dział A korzysta z serwera A i laptopa A, natomiast dział B korzysta z serwera B i laptopa B. Serwer A należy do VLAN 10, natomiast serwer B do VLAN 20. Wymagane jest, aby laptop A miał dostęp wyłącznie do serwera A, a laptop B wyłącznie do serwera B, niezależnie od tego, w której sali konferencyjnej są użytkowane. Aby spełnić ten warunek, wystarczy powiązać odpowiednio adresy MAC tych laptopów z odpowiadającymi im sieciami

VLAN. W ten sposób to adres MAC jest czynnikiem decydującym o dołączeniu do określonej sieci VLAN. Laptopy mogą uzyskać dostęp tylko do tej sieci VLAN, do której przynależą.

# 2 Konfiguracja MAC VLAN

Aby przeprowadzić konfigurację MAC VLAN, postępuj zgodnie z poniższymi krokami:

- 1) Skonfiguruj 802.1Q VLAN.
- 2) Powiąż adres MAC z VLAN.
- 3) Włącz MAC VLAN dla portu.

## Wskazówki dotyczące konfiguracji

Kiedy port w MAC VLAN odbiera nieotagowany pakiet danych przełącznik sprawdza najpierw, czy źródłowy adres MAC pakietu danych został powiązany z MAC VLAN. Jeżeli tak, przełącznik wprowadzi odpowiadający tag do pakietu danych i przekieruje go w obrębie VLAN. Jeżeli nie, przełącznik będzie kontynuował dopasowywanie pakietu danych do reguł innych sieci VLAN (jak np. protokół VLAN). Jeżeli odnajdzie dopasowanie, przełącznik przekieruje pakiet danych. W odwrotnym przypadku, przełącznik przetworzy pakiet danych zgodnie z regułą procesowania 802.1Q VLAN. Jeżeli port odbiera otagowany pakiet danych, przełącznik bezpośrednio procesuje pakiet danych zgodnie z regułą procesowania 802.1Q VLAN.

## 2.1 Przez GUI

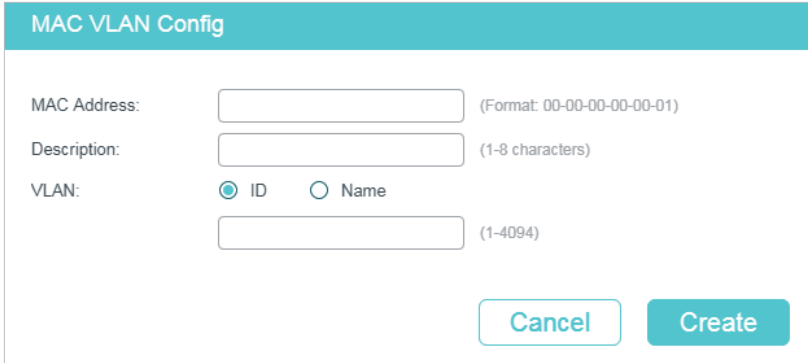
### 2.1.1 Konfiguracja 802.1Q VLAN

Przed konfiguracją MAC VLAN utwórz 802.1Q VLAN i ustaw typ portu zgodnie z wymaganiami sieciowymi. Więcej informacji znajdziesz w części *Konfiguracja 802.1Q VLAN*.

### 2.1.2 Wiązanie adresu MAC z VLAN

Wybierz menu **L2 FEATURES > VLAN > MAC VLAN** i kliknij  **Add**, aby wyświetlić następującą stronę.

Rys. 2-1 Tworzenie MAC VLAN



The screenshot shows a web-based configuration form titled "MAC VLAN Config". It contains the following fields and options:

- MAC Address:** A text input field with a placeholder "(Format: 00-00-00-00-00-01)".
- Description:** A text input field with a placeholder "(1-8 characters)".
- VLAN:** Radio buttons for "ID" (selected) and "Name", followed by a text input field with a placeholder "(1-4094)".
- At the bottom right, there are two buttons: "Cancel" and "Create".

Wykonaj poniższe kroki, aby powiązać adres MAC z 802.1Q VLAN:

- 1) Wprowadź adres MAC urządzenia, dodaj opis i wprowadź VLAN ID, aby powiązać go z siecią VLAN.

|              |                                                                               |
|--------------|-------------------------------------------------------------------------------|
| MAC Address  | Wprowadź adres MAC urządzenia w formacie 00-00-00-00-00-01.                   |
| Description  | Dodaj opis adresu MAC, maks. 8 znaków.                                        |
| VLAN ID/Name | Wprowadź numer ID lub nazwę 802.1Q VLAN, która zostanie powiązana z MAC VLAN. |

- 2) Kliknij **Create**.

#### Uwaga:

Jeden adres MAC może zostać powiązany tylko z jedną siecią VLAN.

## 2.1.3 Włączanie MAC VLAN dla portu

Domyślnie MAC VLAN jest wyłączony na wszystkich portach. Dla wybranych portów należy włączyć MAC VLAN ręcznie.

Wybierz menu **L2 FEATURES > VLAN > MAC VLAN**, aby załadować następującą stronę.

Rys. 2-2 Włączanie MAC VLAN dla portu

Port Enable

UNIT1

1

2

3

4

5

6

7


8


LAGS


9

10

Select All

 Selected

 Unselected

 Not Available

Apply

---

MAC VLAN Config

+ Add - Delete

| <input type="checkbox"/>  | Index | MAC Address | Description | VLAN ID | VLAN Name | Operation |
|---------------------------|-------|-------------|-------------|---------|-----------|-----------|
| No entries in this table. |       |             |             |         |           |           |

Total: 0

W sekcji **Port Enable** wybierz porty, dla których włączony będzie MAC VLAN i kliknij **Apply**.

#### Uwaga:

Port należący do grupy LAG (Link Aggregation Group) poddany jest konfiguracji LAG, nie jest konfigurowany osobno. Konfigurację samego portu przeprowadzić można dopiero, gdy port opuści grupę LAG.

## 2.2 Przez CLI

### 2.2.1 Konfiguracja 802.1Q VLAN

Przed konfiguracją MAC VLAN utwórz VLAN 802.1Q i ustaw typ portu zgodnie z wymaganiami sieciowymi. Więcej informacji znajdziesz w części *Konfiguracja 802.1Q VLAN*.

### 2.2.2 Wiązanie adresu MAC z VLAN

Wykonaj poniższe kroki, aby powiązać adres MAC z VLAN:

|        |                                                                                                                                                                                                                                                                                                                                                                         |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Krok 1 | <b>configure</b><br>Uruchom tryb konfiguracji globalnej.                                                                                                                                                                                                                                                                                                                |
| Krok 2 | <b>mac-vlan mac-address <i>mac-addr</i> vlan <i>vlan-id</i> [<i>description descrip</i>]</b><br>Powiąż adres MAC i VLAN.<br><br><i>mac-addr</i> : Określ adres MAC urządzenia w formacie xx:xx:xx:xx:xx:xx.<br><br><i>vlan-id</i> : Wprowadź numer ID VLAN 802.1Q, który zostanie powiązany z MAC VLAN.<br><br><i>descript</i> : Dodaj opis adresu MAC, maks. 8 znaków. |
| Krok 3 | <b>show mac-vlan { all   mac-address <i>mac-addr</i>   vlan <i>vlan-id</i> }</b><br>Sprawdź konfigurację MAC VLAN.<br><br><i>vid</i> : Określ, który MAC VLAN ma być wyświetlony.                                                                                                                                                                                       |
| Krok 4 | <b>end</b><br>Wróć do trybu privileged EXEC.                                                                                                                                                                                                                                                                                                                            |
| Krok 5 | <b>copy running-config startup-config</b><br>Zapisz ustawienia w pliku konfiguracyjnym.                                                                                                                                                                                                                                                                                 |

Poniższy przykład prezentuje wiązanie adresu MAC 00:19:56:8A:4C:71 i VLAN 10. Opis adresu to Dept.A.

**Switch#configure**

**Switch(config)#mac-vlan mac-address 00:19:56:8a:4c:71 vlan 10 description Dept.A**

**Switch(config)#show mac-vlan vlan 10**

| MAC-Addr          | Name   | VLAN-ID |
|-------------------|--------|---------|
| -----             | -----  | -----   |
| 00:19:56:8A:4C:71 | Dept.A | 10      |

**Switch(config)#end**

**Switch#copy running-config startup-config**

### 2.2.3 Włączanie MAC VLAN dla portu

Wykonaj poniższe kroki, aby włączyć MAC VLAN dla portu:

|        |                                                                                                                                                                                                                                                                                                                                                                      |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Krok 1 | <b>configure</b><br>Uruchom tryb konfiguracji globalnej.                                                                                                                                                                                                                                                                                                             |
| Krok 2 | <b>interface {fastEthernet <i>port</i>   range fastEthernet <i>port-list</i>   gigabitEthernet <i>port</i>   range gigabitEthernet <i>port-list</i>   ten-gigabitEthernet <i>port</i>   range ten-gigabitEthernet <i>port-list</i>   port-channel <i>port-channel-id</i>   range port-channel <i>port-channel-list</i>}</b><br>Uruchom tryb konfiguracji interfejsu. |
| Krok 3 | <b>mac-vlan</b><br>Włącz MAC VLAN dla portu.                                                                                                                                                                                                                                                                                                                         |
| Krok 4 | <b>show mac-vlan interface</b><br>Sprawdź konfigurację MAC VLAN na interfejsie.                                                                                                                                                                                                                                                                                      |
| Krok 5 | <b>end</b><br>Wróć do trybu privileged EXEC.                                                                                                                                                                                                                                                                                                                         |
| Krok 6 | <b>copy running-config startup-config</b><br>Zapisz ustawienia w pliku konfiguracyjnym.                                                                                                                                                                                                                                                                              |

Poniższy przykład prezentuje włączanie MAC VLAN dla portu 1/0/1.

**Switch#configure**

**Switch(config)#interface gigabitEthernet 1/0/1**

**Switch(config-if)#mac-vlan**

**Switch(config-if)#show mac-vlan interface**

```
Port STATUS
----- -
Gi1/0/1 Enable
Gi1/0/2 Disable
...
```

**Switch(config-if)#end**

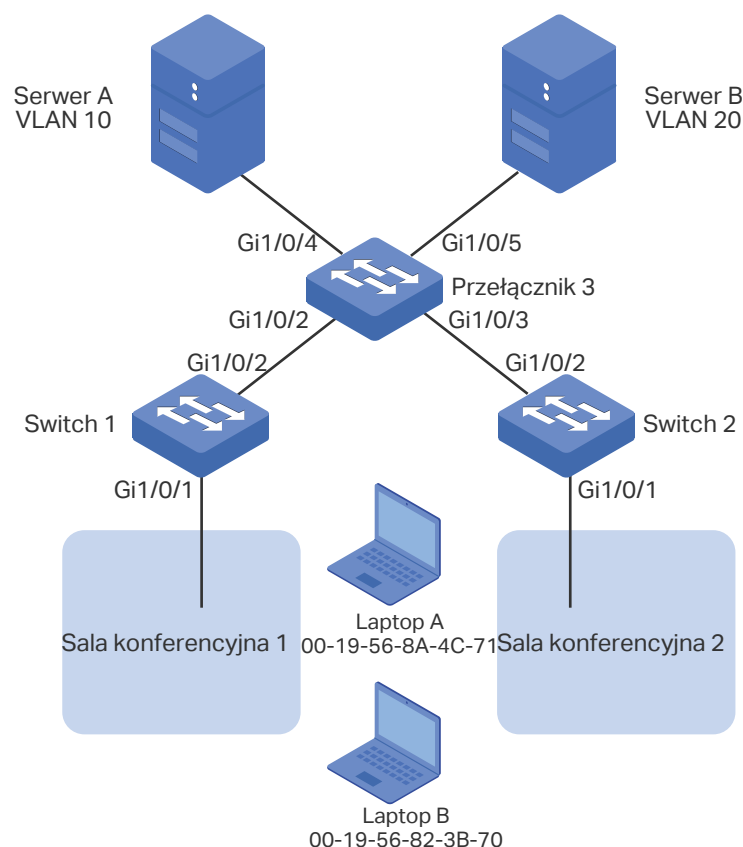
**Switch#copy running-config startup-config**

# 3 Przykład konfiguracji

## 3.1 Wymagania sieciowe

Jak pokazano poniżej, działy firmy korzystają ze wszystkich sal konferencyjnych, ale używają innych serwerów i laptopów. Dział A korzysta z serwera A i laptopa A, natomiast dział B korzysta z serwera B i laptopa B. Serwer A należy do VLAN 10, natomiast serwer B do VLAN 20. Wymagane jest, aby laptop A miał dostęp wyłącznie do serwera A, a laptop B wyłącznie do serwera B, niezależnie od tego, w której sali konferencyjnej są użytkowane.

Rys. 3-1 Topologia sieci



## 3.2 Schemat konfiguracji

Aby spełnić ten warunek, skonfiguruj MAC VLAN. Na przełączniku 1 i przełączniku 2 powiąż odpowiednio adresy MAC laptopów z odpowiadającymi im sieciami VLAN. W ten sposób laptopy mogą uzyskać dostęp tylko do tej sieci VLAN, do której przynależą, niezależnie od tego, w której sali konferencyjnej są użytkowane. Konfiguracja wygląda następująco:

- 1) Utwórz VLAN 10 oraz VLAN 20 na każdym z trzech przełączników i dodaj porty do sieci VLAN w oparciu o topologię sieci. Dla portów połączonych z laptopami ustaw egress rule jako Untagged; dla innych ustaw egress rule jako Tagged.

- 2) Na przełączniku 1 i przełączniku 2 powiąż odpowiednio adresy MAC laptopów z odpowiadającymi im sieciami VLAN i włącz MAC VLAN dla portów.

W poniższych podrozdziałach opisano dwa sposoby przeprowadzenia procedury konfiguracji: przez GUI oraz przez CLI.

### 3.3 Przez GUI

- Konfiguracja ustawień dla przełącznika 1 i przełącznika 2

Konfiguracja ustawień przełącznika 1 i przełącznika 2 wygląda tak samo. W poniższym przykładzie omawiamy konfigurację ustawień na przykładzie przełącznika 1.

- 1) Wybierz z menu **L2 FEATURES > VLAN > 802.1Q VLAN > VLAN Config** i kliknij  **Add** aby wyświetlić poniższą stronę. Utwórz VLAN 10 i dodaj do niej nietagowany port 1/0/1 i tagowany port 1/0/2. Kliknij **Create**.



Rys. 3-2 Tworzenie VLAN 10

### VLAN Config

VLAN ID:  (2-4094, format: 2,4-5,8)

VLAN Name:  (1-16 characters)

#### Untagged Ports

Port:  (Format: 1/0/1, input or choose below)

Select All

UNIT1 LAGS

1  2  3  4  5  6  7  8  9  10

Selected  Unselected  Not Available

#### Tagged Ports

Port:  (Format: 1/0/1, input or choose below)

Select All

UNIT1 LAGS

1  2  3  4  5  6  7  8  9  10

- Wybierz z menu **L2 FEATURES > VLAN > 802.1Q VLAN > VLAN Config** i kliknij **+** Add aby wyświetlić poniższą stronę. Utwórz VLAN 20 i dodaj do niej nietagowany port 1/0/1 i tagowany port 1/0/2 do VLAN 20. Kliknij **Create**.

Rys. 3-3 Tworzenie VLAN 20

### VLAN Config

VLAN ID:  (2-4094, format: 2,4-5,8)

VLAN Name:  (1-16 characters)

#### Untagged Ports

Port:  (Format: 1/0/1, input or choose below)

Select All

UNIT1 LAGS

1  2  3  4  5  6  7  8  9  10

Selected  Unselected  Not Available

#### Tagged Ports

Port:  (Format: 1/0/1, input or choose below)

Select All

UNIT1 LAGS

1  2  3  4  5  6  7  8  9  10

- Wybierz z menu **L2 FEATURES > VLAN > MAC VLAN** i kliknij **+ Add**, aby wyświetlić poniższą stronę. Ustaw odpowiednie parametry i kliknij **Create**, aby powiązać adres MAC laptopa A z siecią VLAN 10 oraz adres MAC laptopa B z VLAN 20.

Rys. 3-4 Tworzenie MAC VLAN

**MAC VLAN Config**

MAC Address:  (Format: 00-00-00-00-00-01)

Description:  (1-8 characters)

VLAN:  ID  Name

(1-4094)

- 4) Wybierz z menu **L2 FEATURES > VLAN > MAC VLAN**, aby wyświetlić poniższą stronę. W sekcji **Port Enable** zaznacz port 1/0/1 i kliknij **Apply**, aby włączyć MAC VLAN.

Rys. 3-5 Włączanie MAC VLAN dla portu

**Port Enable**

Select All

UNIT1:  1  2  3  4  5  6  7  8  9  10

LAGS:  1  2

Selected  Unselected  Not Available


**MAC VLAN Config**

| <input type="checkbox"/> | Index | MAC Address       | Description | VLAN ID | VLAN Name    | Operation                                                                 |
|--------------------------|-------|-------------------|-------------|---------|--------------|---------------------------------------------------------------------------|
| <input type="checkbox"/> | 1     | 00-19-56-8a-4c-71 | PCA         | 10      | Department_A | <input type="button" value="edit"/> <input type="button" value="delete"/> |
| <input type="checkbox"/> | 2     | 00-19-56-82-3b-70 | PCB         | 20      | Department_B | <input type="button" value="edit"/> <input type="button" value="delete"/> |

Total: 2

- 5) Kliknij  **Save**, aby zapisać ustawienia.

#### ■ Konfiguracja ustawień przełącznika 3

- 1) Wybierz z menu **L2 FEATURES > VLAN > 802.1Q VLAN > VLAN Config** i kliknij  **Add** aby wyświetlić poniższą stronę. Utwórz VLAN 10 i dodaj do niej nietagowany port 1/0/4 oraz tagowane porty 1/0/2-3. Kliknij **Create**.

Rys. 3-6 Tworzenie VLAN 10

### VLAN Config

VLAN ID:  (2-4094, format: 2,4-5,8)

VLAN Name:  (1-16 characters)

#### Untagged Ports

Port:  (Format: 1/0/1, input or choose below)

Select All

UNIT1 LAGS

1  2  3  4  5  6  7  8  9  10

Selected  Unselected  Not Available

#### Tagged Ports

Port:  (Format: 1/0/1, input or choose below)

Select All

UNIT1 LAGS

1  2  3  4  5  6  7  8  9  10

- 2) Kliknij **Create**, aby wyświetlić poniższą stronę. Utwórz VLAN 20 i dodaj do niej nietagowany port 1/0/5 oraz tagowane porty 1/0/2-3. Kliknij **Create**.

Rys. 3-7 Tworzenie VLAN 20

VLAN Config

VLAN ID:  (2-4094, format: 2,4-5,8)

VLAN Name:  (1-16 characters)

---

Untagged Ports

Port:  (Format: 1/0/1, input or choose below)

UNIT1

1

2

3

4

5

6

7

8

LAGS

9

10

Select All

Selected

Unselected

Not Available

---

Tagged Ports

Port:  (Format: 1/0/1, input or choose below)

UNIT1

1

2

3

4

5

LAGS

6

7

8

Select All

Cancel

Create

3) Kliknij Save, aby zapisać ustawienia.

## 3.4 Przez CLI

- Konfiguracja ustawień dla przełącznika 1 i przełącznika 2

Konfiguracja ustawień przełącznika 1 i przełącznika 2 wygląda podobnie. W poniższym przykładzie omawiamy konfigurację ustawień przełącznika 1.

- 1) Utwórz VLAN 10 dla działu A oraz VLAN 20 dla działu B.

```
Switch_1#configure
```

```
Switch_1(config)#vlan 10
```

```
Switch_1(config-vlan)#name deptA
```

```
Switch_1(config-vlan)#exit
```

```
Switch_1(config)#vlan 20
```

```
Switch_1(config-vlan)#name deptB
```

```
Switch_1(config-vlan)#exit
```

- 2) Dodaj tagowany port 1/0/2 i nietagowany port 1/0/1 zarówno do sieci VLAN 10, jak i VLAN 20. Następnie włącz MAC VLAN na porcie 1/0/1.

```
Switch_1(config)#interface gigabitEthernet 1/0/2
```

```
Switch_1(config-if)#switchport general allowed vlan 10,20 tagged
```

```
Switch_1(config-if)#exit
```

```
Switch_1(config)#interface gigabitEthernet 1/0/1
```

```
Switch_1(config-if)#switchport general allowed vlan 10,20 untagged
```

```
Switch_1(config-if)#mac-vlan
```

```
Switch_1(config-if)#exit
```

- 3) Powiąż adres MAC laptopa A z VLAN 10 oraz adres MAC laptopa B z VLAN 20.

```
Switch_1(config)#mac-vlan mac-address 00:19:56:8A:4C:71 vlan 10 description PCA
```

```
Switch_1(config)#mac-vlan mac-address 00:19:56:82:3B:70 vlan 20 description PCB
```

```
Switch_1(config)#end
```

```
Switch_1#copy running-config startup-config
```

#### ■ Konfiguracja ustawień dla przełącznika 3

- 1) Utwórz VLAN 10 dla działu A oraz VLAN 20 dla działu B.

```
Switch_3#configure
```

```
Switch_3(config)#vlan 10
```

```
Switch_3(config-vlan)#name deptA
```

```
Switch_3(config-vlan)#exit
```

```
Switch_3(config)#vlan 20
```

```
Switch_3(config-vlan)#name deptB
```

```
Switch_3(config-vlan)#exit
```

- 2) Dodaj tagowany port 1/0/2 i port 1/0/3 zarówno do sieci VLAN 10, jak i VLAN 20.

```
Switch_3(config)#interface gigabitEthernet 1/0/2
```

```
Switch_3(config-if)#switchport general allowed vlan 10,20 tagged
```

```
Switch_3(config-if)#exit
Switch_3(config)#interface gigabitEthernet 1/0/3
Switch_3(config-if)#switchport general allowed vlan 10,20 tagged
Switch_3(config-if)#exit
```

- 3) Dodaj nietagowany port 1/0/4 do VLAN 10 i nietagowany port 1/0/5 do VLAN 20.

```
Switch_3(config)#interface gigabitEthernet 1/0/4
Switch_3(config-if)#switchport general allowed vlan 10 untagged
Switch_3(config-if)#exit
Switch_3(config)#interface gigabitEthernet 1/0/5
Switch_3(config-if)#switchport general allowed vlan 20 untagged
Switch_3(config-if)#end
Switch_3#copy running-config startup-config
```

## Sprawdzanie konfiguracji

### ■ Przełącznik 1

```
Switch_1#show mac-vlan all
```

| MAC Add           | Name | VLAN-ID |
|-------------------|------|---------|
| 00:19:56:8A:4C:71 | PCA  | 10      |
| 00:19:56:82:3B:70 | PCB  | 20      |

### ■ Przełącznik 2

```
Switch_2#show mac-vlan all
```

| MAC Address       | Description | VLAN |
|-------------------|-------------|------|
| 00:19:56:8A:4C:71 | PCA         | 10   |
| 00:19:56:82:3B:70 | PCB         | 20   |

### ■ Przełącznik 3

```
Switch_3#show vlan
```

---

| VLAN  | Name        | Status | Ports                                                                                |
|-------|-------------|--------|--------------------------------------------------------------------------------------|
| ----- | -----       | -----  | -----                                                                                |
| 1     | System-VLAN | active | Gi1/0/1, Gi1/0/2, Gi1/0/3, Gi1/0/4,<br>Gi1/0/5, Gi1/0/6, Gi1/0/7, Gi1/0/8<br><br>... |
| 10    | DeptA       | active | Gi1/0/2, Gi1/0/3, Gi1/0/4                                                            |
| 20    | DeptB       | active | Gi1/0/2, Gi1/0/3, Gi1/0/5                                                            |



# Część 9

## Konfiguracja protokołu VLAN

### ROZDZIAŁY

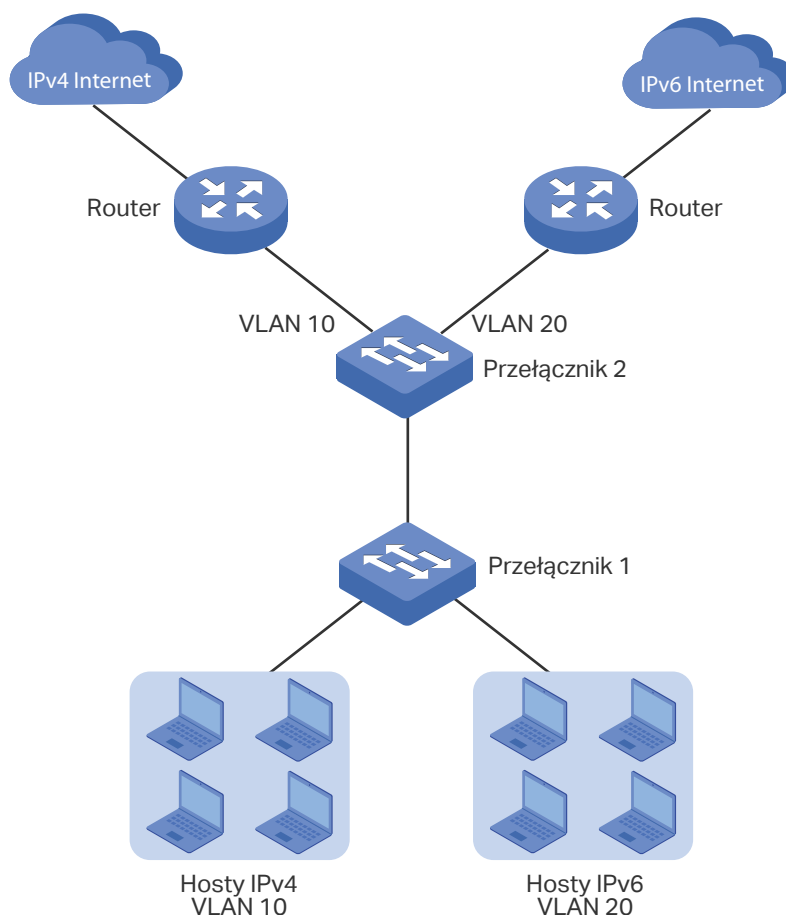
1. Informacje ogólne
2. Konfiguracja protokołu VLAN
3. Przykład konfiguracji

# 1 Informacje ogólne

Protokół VLAN to technologia, która dzieli sieci VLAN w oparciu o protokół warstwy sieci. Po skonfigurowaniu reguły protokołu VLAN na podstawie 802.1Q VLAN przełącznik może analizować określone części odebranych pakietów, kapsułkować pakiety w określonych formatach, a także przysyłać pakiety innych protokołów do odpowiednich VLAN-ów. Ze względu na to, że różne aplikacje i usługi korzystają z różnych protokołów, administratorzy sieci mogą korzystać z protokołu VLAN, aby zarządzać siecią w oparciu o określone aplikacje i usługi.

Poniższy schemat przedstawia często stosowane rozwiązanie z wykorzystaniem protokołu VLAN. Po skonfigurowaniu protokołu VLAN przełącznik 2 może przysyłać pakiety IPv4 i IPv6 z różnych VLAN-ów odpowiednio do sieci IPv4 i IPv6.

Rys. 1-1 Często stosowane rozwiązanie z wykorzystaniem protokołu VLAN



# 2 Konfiguracja protokołu VLAN

Aby przeprowadzić konfigurację protokołu VLAN, wykonaj poniższe kroki:

- 1) skonfiguruj 802.1Q VLAN;
- 2) utwórz szablon protokołu;
- 3) skonfiguruj protokół VLAN.

## Wskazówki dotyczące konfiguracji

- Możesz skorzystać z szablonów protokołu IP, ARP, RARP lub innych oferowanych przez przełączniki TP-Link lub utworzyć nowe szablony protokołu.
- W przypadku protokołu VLAN, gdy port otrzymuje nietagowany pakiet danych, przełącznik wyszukuje najpierw protokołu VLAN zgodnego z typem protokołu pakietu. Jeżeli pojawi się dopasowanie, przełącznik opatrzy pakiet danych odpowiednim tagiem VLAN i prześle go w ramach sieci VLAN. W innym wypadku, przełącznik prześle pakiet danych do domyślnej sieci VLAN, w oparciu o PVID (VLAN ID) portu odbierającego. (Jeżeli adres MAC sieci VLAN także został skonfigurowany, przełącznik najpierw przetworzy protokół VLAN, a następnie MAC VLAN.) Gdy port otrzymuje otagowany pakiet danych, przełącznik bezpośrednio przetwarza pakiet danych, zgodnie z regułą przetwarzania 802.1 Q VLAN.

## 2.1 Przez GUI

### 2.1.1 Konfiguracja 802.1Q VLAN

Przed konfiguracją protokołu VLAN, utwórz sieć 802.1Q VLAN ustaw typ portu zgodnie z wymaganiami środowiska sieciowego. Szczegółowe informacje znajdziesz w części *Konfiguracja 802.1Q VLAN*.

## 2.1.2 Tworzenie szablonów protokołu

Wybierz z menu **L2 FEATURES > VLAN > Protocol VLAN > Protocol Template**, aby wyświetlić poniższą stronę.

Rys. 2-1 Przeglądanie szablonów protokołu

| Protocol Template Config |    |               |                  |                |
|--------------------------|----|---------------|------------------|----------------|
|                          |    |               |                  | + Add - Delete |
| <input type="checkbox"/> | ID | Template Name | Protocol Type    |                |
| <input type="checkbox"/> | 1  | IP            | Ethernet II 0800 |                |
| <input type="checkbox"/> | 2  | ARP           | Ethernet II 0806 |                |
| <input type="checkbox"/> | 3  | RARP          | Ethernet II 8035 |                |
| <input type="checkbox"/> | 4  | IPX           | SNAP             |                |
| <input type="checkbox"/> | 5  | AT            | SNAP             |                |
| Total: 5                 |    |               |                  |                |

Wykonaj poniższe kroki, aby utworzyć szablon protokołu:

- 1) Sprawdź czy pożądany szablon nie istnieje już w sekcji **Protocol Template Config**. Jeżeli nie istnieje, kliknij **+ Add**, aby stworzyć nowy szablon.

Rys. 2-2 Tworzenie szablonu protokołu

**Protocol Template Config**

Template Name:  (1-8 characters)

Frame Type:  Ethernet II  SNAP  LLC

Ether Type:  (4 hexadecimal integers, 0600-FFFF)

**Template Name** Nadaj nazwę szablonowi, aby łatwo go zidentyfikować.

**Frame Type** Wybierz typ ramki nowego szablonu protokołu.

**Ethernet II:** Typowy format ramki sieci Ethernet. Po wybraniu opcji określ typ ramki poprzez wpisanie EtherType.

**SNAP:** Format ramki sieci Ethernet 802.3 oparty o standard IEEE 802.3 i IEEE 802.2 SNAP. Po wybraniu opcji określ typ ramki poprzez wpisanie EtherType.

**LLC:** Format ramki sieci Ethernet 802.3 oparty o standard IEEE 802.3 i IEEE 802.2 LLC. Po wybraniu opcji określ typ ramki poprzez wpisanie DSAP i SSAP.

**Ether Type** Uzupełnij typ protokołu Ethernet dla szablonu protokołu. Opcja jest dostępna przy wyborze **Ethernet II** i **SNAP**. Wpisanie EtherType służy identyfikacji typu danych ramki.

|      |                                                                                                                                                   |
|------|---------------------------------------------------------------------------------------------------------------------------------------------------|
| DSAP | Uzupełnij wartość DSAP dla szablonu protokołu. Opcja jest dostępna przy wyborze <b>LLC</b> . Wpisanie DSAP służy identyfikacji typu danych ramki. |
| SSAP | Uzupełnij wartość SSAP dla szablonu protokołu. Opcja jest dostępna przy wyborze <b>LLC</b> . Wpisanie SSAP służy identyfikacji typu danych ramki. |

2) Kliknij **Create**.



**Uwaga:**

Szablon protokołu powiązany z siecią VLAN nie może być usunięty.

## 2.1.3 Konfiguracja protokołu VLAN

Wybierz z menu **L2 FEATURES > VLAN > Protocol VLAN > Protocol VLAN Group** i kliknij **+ Add**, aby wyświetlić poniższą stronę.

Rys. 2-3 Konfiguracja grupy protokołu VLAN

Protocol VLAN Group Config

Template Name:

VLAN:  VLAN ID  VLAN Name

VLAN ID:  (1-4094)

802.1p Priority:

Port:  (Format: 1/0/1, input or choose below)

UNIT1

1

2

3

4

5

6

7

8

LAGS

9

10

Select All

Selected
  Unselected
  Not Available

Cancel

Create

Wykonaj poniższe kroki, aby skonfigurować grupę protokołu:

1) W sekcji **Protocol Group Config** określ następujące parametry.

|               |                                                                                       |
|---------------|---------------------------------------------------------------------------------------|
| Template Name | Wybierz wcześniej zdefiniowany szablon protokołu.                                     |
| VLAN ID/Name  | Podaj numer ID lub nazwę sieci 802.1Q VLAN, która będzie powiązana z protokołem VLAN. |

|                 |                                                                                                                                                                                                                                 |
|-----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 802.1p Priority | Określ priorytet 802.1p dla pakietów należących do protokołu VLAN. Przełącznik określi sekwencję przesyłania zgodnie z tą wartością. Pakiety o wyższej wartości priorytetu 802.1p są uznawane za pakiety o wyższym priorytecie. |
|-----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

2) Wybierz porty. Kliknij **Create**.

 **Uwaga:**

Port LAG (Link Aggregation Group) działa według konfiguracji LAG, a nie konfiguracji własnej. Konfiguracji portu obowiązuje jedynie po opuszczeniu LAG.

## 2.2 Przez CLI

### 2.2.1 Konfiguracja 802.1Q VLAN

Przed skonfigurowaniem protokołu VLAN, utwórz sieć 802.1Q VLAN i ustaw typ portu, zgodnie z wymaganiami środowiska sieciowego. Szczegółowe informacje znajdziesz w części *Konfiguracja 802.1Q VLAN*.

### 2.2.2 Tworzenie szablonu protokołu

Wykonaj poniższe kroki, aby utworzyć szablon protokołu:

|        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Krok 1 | <b>configure</b><br>Uruchom tryb konfiguracji globalnej.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Krok 2 | <b>protocol-vlan template name <i>protocol-name</i> frame { ether_2 ether-type <i>type</i>   snap ether-type <i>type</i>   llc dsap <i>dsap_type</i> ssap <i>ssap_type</i> }</b><br>Utwórz szablon protokołu.<br><br><i>protocol-name</i> : Uzupełnij nazwę protokołu, wprowadzając od 1 do 8 znaków.<br><br><i>type</i> : Wpisz 4 liczby systemu szesnastkowego jako typ protokołu Ethernet dla szablonu protokołu. Po wybraniu opcji określ typ ramki poprzez wpisanie EtherType.<br><br><i>dsap_type</i> : Wpisz 2 liczby systemu szesnastkowego jako wartość DSAP dla szablonu protokołu. Po wybraniu opcji określ typ ramki poprzez wpisanie DSAP.<br><br><i>ssap_type</i> : Wpisz 2 liczby systemu szesnastkowego jako wartość SSAP dla szablonu protokołu. Po wybraniu opcji określ typ ramki poprzez wpisanie SSAP. |
| Krok 3 | <b>show protocol-vlan template</b><br>Zweryfikuj szablony protokołu.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Krok 4 | <b>end</b><br>Powróć do trybu privileged EXEC.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |

---

Krok 5      **copy running-config startup-config**  
Zapisz ustawienia w pliku konfiguracyjnym.

---

Poniższy schemat przedstawia przykładowy sposób tworzenia szablonu protokołu IPv6:

**Switch#configure**

**Switch(config)#protocol-vlan template name IPv6 frame ether\_2 ether-type 86dd**

**Switch(config)#show protocol-vlan template**

| Index | Protocol Name | Protocol Type              |
|-------|---------------|----------------------------|
| 1     | IP            | EthernetII ether-type 0800 |
| 2     | ARP           | EthernetII ether-type 0806 |
| 3     | RARP          | EthernetII ether-type 8035 |
| 4     | IPX           | SNAP ether-type 8137       |
| 5     | AT            | SNAP ether-type 809B       |
| 6     | IPv6          | EthernetII ether-type 86DD |

**Switch(config)#end**

**Switch#copy running-config startup-config**

## 2.2.3 Konfiguracja protokołu VLAN

Wykonaj poniższe kroki, aby skonfigurować protokół VLAN:

---

Krok 1      **configure**  
Uruchom tryb konfiguracji globalnej.

---

Krok 2      **show protocol-vlan template**  
Sprawdź indeks każdego szablonu protokołu.

---

Krok 3      **protocol-vlan vlan vid priority priority template index**  
Powiąz szablon protokołu z siecią VLAN.

*vid* : Podaj numer ID sieci 802.1Q VLAN, który ma być powiązany z protokołem VLAN.

*priority* : Określ priorytet 802.1p dla pakietów należących do protokołu VLAN. Przełącznik określi sekwencję przesyłania zgodnie z tą wartością. Pakiety o wyższej wartości priorytetu 802.1p są uznawane za pakiety o wyższym priorytecie.

*index* : Uzupełnij indeks szablonu protokołu.

---

|        |                                                                                                                                                                                                                                                                                                              |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Krok 4 | <b>show protocol-vlan vlan</b><br>Sprawdź indeksy protokołu VLAN (entry-id) wszystkich grup protokołu.                                                                                                                                                                                                       |
| Krok 5 | <b>interface {fastEthernet port   range fastEthernet port-list   gigabitEthernet port   range gigabitEthernet port-list   ten-gigabitEthernet port   range ten-gigabitEthernet port-list   port-channel port-channel-id   range port-channel port-channel-list}</b><br>Uruchom tryb konfiguracji interfejsu. |
| Krok 6 | <b>protocol-vlan group entry-id</b><br>Dodaj określony port do grupy protokołu.<br><i>entry-id</i> : Indeks protokołu VLAN.                                                                                                                                                                                  |
| Krok 7 | <b>end</b><br>Powróć do trybu uprzywilejowanego (Privileged EXEC Mode).                                                                                                                                                                                                                                      |
| Krok 8 | <b>copy running-config startup-config</b><br>Zapisz ustawienia w pliku konfiguracyjnym.                                                                                                                                                                                                                      |

Poniższy schemat przedstawia przykładowy sposób wiązania szablonu protokołu IPv6 jako VLAN 10 i dodawania portu 1/0/2 do protokołu VLAN:

### Switch#configure

#### Switch(config)#show protocol-vlan template

| Index | Protocol Name | Protocol Type              |
|-------|---------------|----------------------------|
| 1     | IP            | EthernetII ether-type 0800 |
| 2     | ARP           | EthernetII ether-type 0806 |
| 3     | RARP          | EthernetII ether-type 8035 |
| 4     | IPX           | SNAP ether-type 8137       |
| 5     | AT            | SNAP ether-type 809B       |
| 6     | IPv6          | EthernetII ether-type 86DD |

#### Switch(config)#protocol-vlan vlan 10 priority 5 template 6

#### Switch(config)#show protocol-vlan vlan

| Index | Protocol-Name | VID | Priority | Member |
|-------|---------------|-----|----------|--------|
| 1     | IPv6          | 10  | 0        |        |

#### Switch(config)#interface gigabitEthernet 1/0/2



```
Switch(config-if)#protocol-vlan group 1
```

```
Switch(config-if)#show protocol-vlan vlan
```

| Index | Protocol-Name | VID | Priority | Member  |
|-------|---------------|-----|----------|---------|
| 1     | IPv6          | 10  | 5        | Gi1/0/2 |

```
Switch(config-if)#end
```

```
Switch#copy running-config startup-config
```

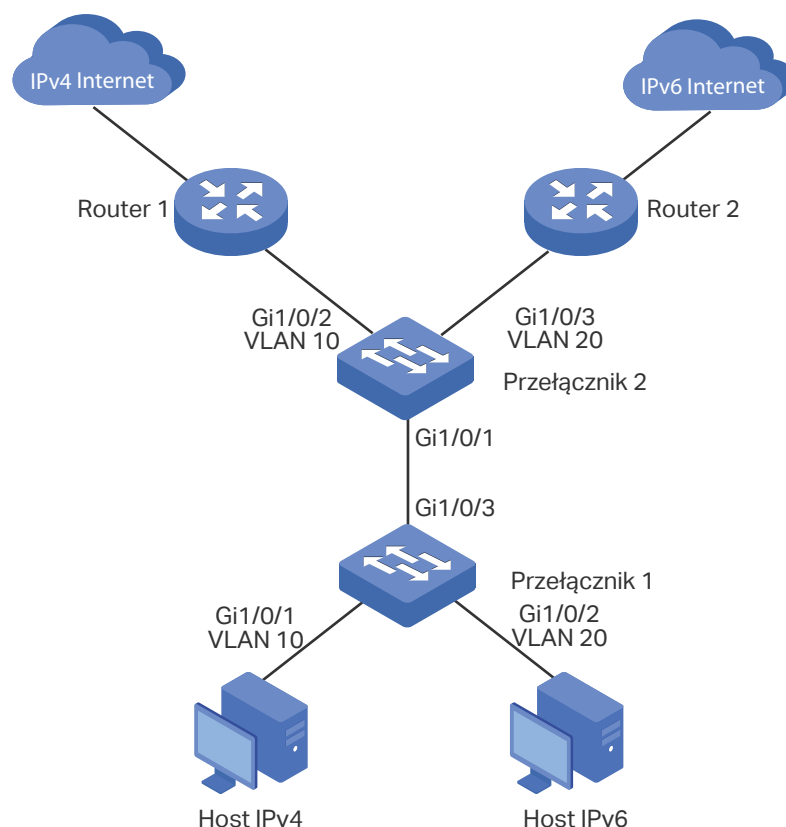
# 3 Przykład konfiguracji

## 3.1 Wymagania sieciowe

W firmie pracownicy korzystają zarówno z hostów IPv4, jak i hostów IPv6, a dostęp odpowiednio do sieci IPv4 i IPv6 udzielany jest im z wykorzystaniem różnych routerów. Wymaga się, aby pakiety IPv4 przesyłane były do sieci IPv4, a pakiety IPv6 do sieci IPv6, a inne pakiety odrzucane.

Poniższy schemat przedstawia topologię sieci. Host IPv4 należy do VLAN 10, a host IPv6 należy do VLAN 20, natomiast dostęp do sieci uzyskują poprzez przełącznik 1. Przełącznik 2 podłączony jest do dwóch routerów, aby umożliwić dostęp odpowiednio do sieci IPv4 i sieci IPv6. Routery należą odpowiednio do VLAN 10 oraz VLAN 20.

Rys. 3-1 Topologia sieci



## 3.2 Schemat konfiguracji

Aby spełnić omówiony powyżej warunek, możesz skonfigurować protokół VLAN na porcie 1/0/1 przełącznika 2. Gdy port ten otrzyma pakiety, przełącznik 2 prześle je do odpowiednich VLAN-ów, zgodnie z ich typem protokołu. Konfiguracja na przełączniku 2 wygląda w następujący sposób:


- 1) Utwórz VLAN 10 i VLAN 20 oraz dodaj porty do odpowiednich VLAN-ów.
- 2) Skorzystaj z szablonu protokołu IPv4, który zapewnia przełącznik i utwórz szablon protokołu IPv6.
- 3) Powiąż szablony protokołu z odpowiednimi sieciami VLAN, aby utworzyć grupy protokołu, a następnie dodaj port 1/0/1 do grup.

Skonfiguruj 802.1Q VLAN na przełączniku 1 zgodnie z topologią sieci.

W poniższych podrozdziałach opisano dwa sposoby przeprowadzenia procedury konfiguracji: przez GUI oraz przez CLI:

### 3.3 Przez GUI

- Konfiguracja ustawień dla przełącznika 1

- 1) Wybierz z menu **L2 FEATURES > VLAN > 802.1Q VLAN > VLAN Config** i kliknij  **Add** aby wyświetlić poniższą stronę. Utwórz VLAN 10 i dodaj do niej nietagowany port 1/0/1 oraz nietagowany port 1/0/3. Kliknij **Create**.

Rys. 3-2 Tworzenie VLAN 10

VLAN Config

VLAN ID:  (2-4094, format: 2,4-5,8)

VLAN Name:  (1-16 characters)

Untagged Ports

Port:  (Format: 1/0/1, input or choose below)

UNIT1
LAGS

Select All
 

1

2

3

4

5

6

7

8

9

10

 Selected

 Unselected

 Not Available

Tagged Ports

Port:  (Format: 1/0/1, input or choose below)

UNIT1
LAGS

Select All
 

1

2

3

4

5

6

7

8

9

10

 Selected


 Unselected

 Not Available

Cancel

Create

Configuration Guide ■ 189

- 4) Kliknij  **Add**, aby wyświetlić poniższą stronę. Utwórz VLAN 20 i dodaj do niej nietagowane porty 1/0/2-3. Kliknij **Create**.

Rys. 3-3 Tworzenie VLAN 20

### VLAN Config

VLAN ID:  (2-4094, format: 2,4-5,8)

VLAN Name:  (1-16 characters)




#### Untagged Ports

Port:  (Format: 1/0/1, input or choose below)

Select All

**UNIT1**      **LAGS**

1  2  3  4  5  6  7  8  9  10

 Selected     Unselected     Not Available




#### Tagged Ports


Port:  (Format: 1/0/1, input or choose below)

Select All


**UNIT1**      **LAGS**

1  2  3  4  5  6  7  8  9  10

 Selected     Unselected     Not Available

- 5) Kliknij  **Save**, aby zapisać ustawienia.

- Konfiguracja ustawień dla przełącznika 2

- 1) Wybierz z menu **L2 FEATURES > VLAN > 802.1Q VLAN > VLAN Config** i kliknij  **Add** aby wyświetlić poniższą stronę. Utwórz VLAN 10 i dodaj do niej tagowany port 1/0/1 i nietagowany port 1/0/2. Kliknij **Create**.

Rys. 3-4 Tworzenie VLAN 10

### VLAN Config

VLAN ID:  (2-4094, format: 2,4-5,8)

VLAN Name:  (1-16 characters)

#### Untagged Ports

Port:  (Format: 1/0/1, input or choose below)

Select All

**UNIT1**      **LAGS**

1  2  3  4  5  6  7  8  9  10

 Selected     Unselected     Not Available

#### Tagged Ports

Port:  (Format: 1/0/1, input or choose below)

Select All

**UNIT1**      **LAGS**

1  2  3  4  5  6  7  8  9  10

 Selected     Unselected     Not Available

- 2) Kliknij **+** **Add**, aby wyświetlić poniższą stronę. Utwórz VLAN 20 i dodaj do niej tagowany port 1/0/1 oraz nietagowany port 1/0/3. Kliknij **Create**.

Rys. 3-5 Tworzenie VLAN 20

### VLAN Config

VLAN ID:  (2-4094, format: 2,4-5,8)

VLAN Name:  (1-16 characters)

#### Untagged Ports

Port:  (Format: 1/0/1, input or choose below)

Select All

UNIT1 LAGS

1  2  3  4  5  6  7  8  9  10

Selected  Unselected  Not Available

#### Tagged Ports

Port:  (Format: 1/0/1, input or choose below)

Select All

UNIT1 LAGS

1  2  3  4  5  6  7  8  9  10

Selected  Unselected  Not Available

- 3) Wybierz z menu **L2 FEATURES > VLAN > 802.1Q VLAN > Port Config**, aby wyświetlić poniższą stronę. Ustaw PVID portu 1/0/2 i portu 1/0/3 odpowiednio jako 10 i 20. Kliknij **Apply**.

Rys. 3-6 Konfiguracja portu

| UNIT1                               | LAGS | Port   | PVID | Ingress Checking | Acceptable Frame Types | LAG | Details                 |
|-------------------------------------|------|--------|------|------------------|------------------------|-----|-------------------------|
| <input type="checkbox"/>            |      |        | 20   |                  |                        |     |                         |
| <input type="checkbox"/>            |      | 1/0/1  | 1    | Enabled          | Admit All              | --- | <a href="#">Details</a> |
| <input type="checkbox"/>            |      | 1/0/2  | 10   | Enabled          | Admit All              | --- | <a href="#">Details</a> |
| <input checked="" type="checkbox"/> |      | 1/0/3  | 20   | Enabled          | Admit All              | --- | <a href="#">Details</a> |
| <input type="checkbox"/>            |      | 1/0/4  | 1    | Enabled          | Admit All              | --- | <a href="#">Details</a> |
| <input type="checkbox"/>            |      | 1/0/5  | 1    | Enabled          | Admit All              | --- | <a href="#">Details</a> |
| <input type="checkbox"/>            |      | 1/0/6  | 1    | Enabled          | Admit All              | --- | <a href="#">Details</a> |
| <input type="checkbox"/>            |      | 1/0/7  | 1    | Enabled          | Admit All              | --- | <a href="#">Details</a> |
| <input type="checkbox"/>            |      | 1/0/8  | 1    | Enabled          | Admit All              | --- | <a href="#">Details</a> |
| <input type="checkbox"/>            |      | 1/0/9  | 1    | Enabled          | Admit All              | --- | <a href="#">Details</a> |
| <input type="checkbox"/>            |      | 1/0/10 | 1    | Enabled          | Admit All              | --- | <a href="#">Details</a> |

Total: 10      1 entry selected.     

- 4) Wybierz z menu **L2 FEATURES > VLAN > Protocol VLAN > Protocol Template** i kliknij **+ Add**, aby wyświetlić poniższą stronę. Wpisz **IPv6** w polu protocol name, wybierz **Ethernet II** w rubryce frame type, wpisz **86DD** w polu Ether Type i kliknij **Create**, aby utworzyć szablon protokołu IPv6.

*Wskazówka:* Przełącznik zapewnia gotowy szablon protokołu IPv4. Musisz utworzyć tylko szablon protokołu IPv6.

Rys. 3-7 Tworzenie szablonu protokołu IPv6

**Protocol Template Config**

Template Name:  (1-8 characters)

Frame Type:  Ethernet II  SNAP  LLC

Ether Type:  (4 hexadecimal integers, 0600-FFFF)

- 5) Wybierz z menu **L2 FEATURES > VLAN > Protocol VLAN > Protocol VLAN Group** i kliknij **+ Add**, aby wyświetlić poniższą stronę. Wybierz nazwę protokołu IP (tj. szablon protokołu IPv4), wpisz VLAN ID 10, zaznacz port 1 i kliknij **Create**. Wybierz nazwę protokołu IPv6, wpisz VLAN ID 20, zaznacz port 1 i kliknij **Create**.



Rys. 3-7 Konfiguracja grupy protokołu IPv4

### Protocol VLAN Group Config

Template Name:

VLAN:  VLAN ID  VLAN Name

VLAN ID:  (1-4094)

802.1p Priority:

Port:  (Format: 1/0/1, input or choose below)

Select All

UNIT1 LAGS

1  2  3  4  5  6  7  8  9  10

Selected  Unselected  Not Available

Rys. 3-8 Konfiguracja grupy protokołu IPv6

### Protocol VLAN Group Config

Template Name:

VLAN:  VLAN ID  VLAN Name

VLAN ID:  (1-4094)

802.1p Priority:


Port:  (Format: 1/0/1, input or choose below)

Select All

UNIT1 LAGS

1  2  3  4  5  6  7  8  9  10

Selected  Unselected  Not Available

- 6) Kliknij , aby zapisać ustawienia.

## 3.4 Przez CLI

### ■ Konfiguracja ustawień dla przełącznika 1

- 1) Utwórz VLAN 10 i VLAN 20.

```
Switch_1#configure
```

```
Switch_1(config)#vlan 10
```

```
Switch_1(config-vlan)#name IPv4
```

```
Switch_1(config-vlan)#exit
```

```
Switch_1(config)#vlan 20
```

```
Switch_1(config-vlan)#name IPv6
```

```
Switch_1(config-vlan)#exit
```

- 2) Dodaj nietagowany port 1/0/1 do VLAN 10. Dodaj nietagowany port 1/0/2 do VLAN 20. Dodaj nietagowany port 1/0/3 zarówno do VLAN10, jak i do VLAN 20.

```
Switch_1(config)#interface gigabitEthernet 1/0/1
```

```
Switch_1(config-if)#switchport general allowed vlan 10 untagged
```

```
Switch_1(config-if)#exit
```

```
Switch_1(config)#interface gigabitEthernet 1/0/2
```

```
Switch_1(config-if)#switchport general allowed vlan 20 untagged
```

```
Switch_1(config-if)#exit
```

```
Switch_1(config)#interface gigabitEthernet 1/0/3
```

```
Switch_1(config-if)#switchport general allowed vlan 10,20 untagged
```

```
Switch_1(config-if)#end
```

```
Switch_1#copy running-config startup-config
```

### ■ Konfiguracja ustawień dla przełącznika 2

- 1) Utwórz VLAN 10 i VLAN 20.

```
Switch_2#configure
```

```
Switch_2(config)#vlan 10
```

```
Switch_2(config-vlan)#name IPv4
```

```
Switch_2(config-vlan)#exit
```

```
Switch_2(config)#vlan 20
```

```
Switch_2(config-vlan)#name IPv6
```

```
Switch_2(config-vlan)#exit
```

- 2) Dodaj tagowany port 1/0/1 zarówno do VLAN 10, jak i do VLAN 20. Ustaw PVID nietagowanego portu 1/0/2 jako 10 i dodaj go do VLAN 10. Ustaw PVID nietagowanego portu 1/0/3 jako 20 i dodaj go do VLAN 20.

```
Switch_2(config)#interface gigabitEthernet 1/0/1
```

```
Switch_2(config-if)#switchport general allowed vlan 10,20 tagged
```

```
Switch_2(config-if)#exit
```

```
Switch_2(config)#interface gigabitEthernet 1/0/2
```

```
Switch_2(config-if)#switchport pvid 10
```

```
Switch_2(config-if)#switchport general allowed vlan 10 untagged
```

```
Switch_2(config-if)#exit
```

```
Switch_2(config)#interface gigabitEthernet 1/0/3
```

```
Switch_2(config-if)#switchport mode general
```

```
Switch_2(config-if)#switchport pvid 20
```

```
Switch_2(config-if)#switchport general allowed vlan 20 untagged
```

```
Switch_2(config-if)#exit
```

- 3) Utwórz szablon protokołu IPv6.

```
Switch_2(config)#protocol-vlan template name IPv6 frame ether_2 ether-type 86dd
```

```
Switch_2(config)#show protocol-vlan template
```

| Index | Protocol Name | Protocol Type               |
|-------|---------------|-----------------------------|
| 1     | IP            | EthernetII ether-type 0800  |
| 2     | ARP           | EthernetII ether-type 0806  |
| 3     | RARP          | EthernetII ether-type 8035  |
| 4     | IPX           | SNAP ether-type 8137        |
| 5     | AT            | SNAP ether-type 809b        |
| 6     | IPv6          | Ethernet II ether-type 86dd |

- 4) Skonfiguruj grupy protokołu.

```
Switch_2(config)#protocol-vlan vlan 10 priority 0 template 1
```

```
Switch_2(config)#protocol-vlan vlan 20 priority 0 template 6
```

- 5) Dodaj port 1/0/1 do grup protokołu.

```
Switch_2(config)#show protocol-vlan vlan
```

| Index | Protocol-Name | VID | Member |
|-------|---------------|-----|--------|
| 1     | IP            | 10  |        |
| 2     | IPv6          | 20  |        |

```
Switch_2(config)#interface gigabitEthernet 1/0/1
```

```
Switch_2(config-if)#protocol-vlan group 1
```

```
Switch_2(config-if)#protocol-vlan group 2
```

```
Switch_2(config-if)#exit
```

```
Switch_2(config)#end
```

```
Switch_2#copy running-config startup-config
```

## Sprawdzanie konfiguracji

### ■ Przełącznik 1

Sprawdzanie konfiguracji 802.1Q VLAN:

```
Switch_1#show vlan
```

| VLAN | Name        | Status | Ports                                                                     |
|------|-------------|--------|---------------------------------------------------------------------------|
| 1    | System-VLAN | active | Gi1/0/1, Gi1/0/2, Gi1/0/3, Gi1/0/4<br>.....<br>Gi1/0/8, Gi1/0/9, Gi1/0/10 |
| 10   | IPv4        | active | Gi1/0/1, Gi1/0/3                                                          |
| 20   | IPv6        | active | Gi1/0/2, Gi1/0/3                                                          |

### ■ Przełącznik 2

Sprawdzanie konfiguracji 802.1Q VLAN:

```
Switch_2#show vlan
```

| VLAN | Name        | Status | Ports                                                                     |
|------|-------------|--------|---------------------------------------------------------------------------|
| 1    | System-VLAN | active | Gi1/0/1, Gi1/0/2, Gi1/0/3, Gi1/0/4<br>.....<br>Gi1/0/8, Gi1/0/9, Gi1/0/10 |
| 10   | IPv4        | active | Gi1/0/1, Gi1/0/2                                                          |
| 20   | IPv6        | active | Gi1/0/1, Gi1/0/3                                                          |

Sprawdzanie konfiguracji grupy protokołu:

Switch\_2#show protocol-vlan vlan

| Index | Protocol-Name | VID | Priority | Member  |
|-------|---------------|-----|----------|---------|
| 1     | IP            | 10  | 0        | Gi1/0/1 |
| 2     | IPv6          | 20  | 0        | Gi1/0/1 |

# Część 10

## Konfiguracja VLAN-VPN

### ROZDZIAŁY

1. VLAN-VPN
2. Podstawowa konfiguracja VLAN-VPN
3. Elastyczna konfiguracja VLAN-VPN
4. Przykłady konfiguracji

# 1 VLAN-VPN

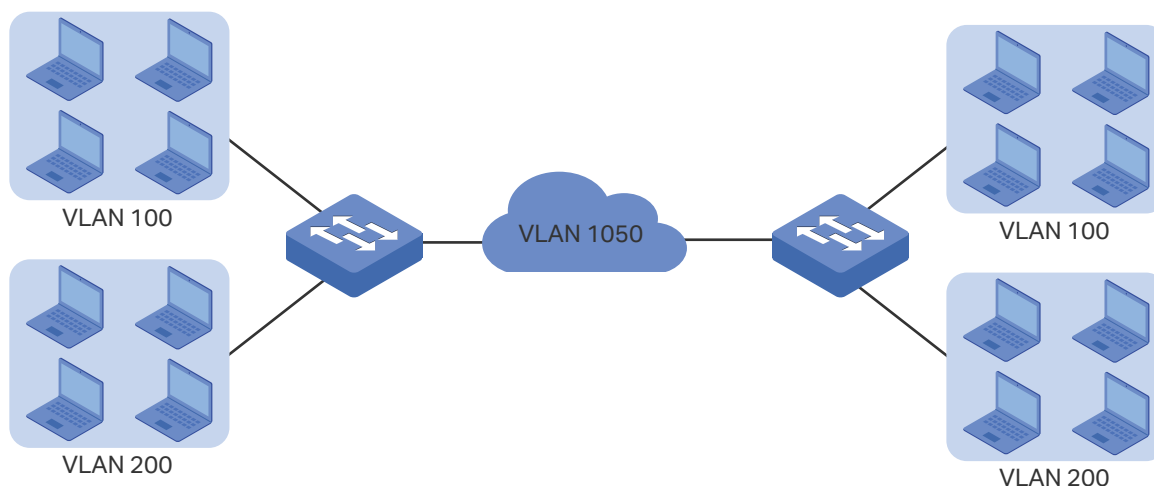
## 1.1 Informacje ogólne

VLAN-VPN (Virtual Private Network) jest to łatwa we wdrożeniu technologia VLAN warstwy 2. Zwykle stosuje się ją na obrzeżach sieci ISP (Internet Service Provider).

Korzystając z VLAN-VPN, gdy pakiety przesyłane są z sieci klienta do sieci ISP, przełącznik dodaje do pakietu tag zewnętrzny z zewnętrznym VLAN ID. Zatem pakiety mogą być przesyłane przez sieć ISP w podwójnymi tagami VLAN. W sieci ISP pakiety przesyłane są zgodnie z ich zewnętrznym tagiem VLAN (tag VLAN sieci ISP), natomiast tag wewnętrzny uważany jest za część danych właściwych. Przekazując pakiety z sieci ISP do sieci klienta przełącznik usuwa zewnętrzny tag VLAN pakietów. Zatem pakiety przesyłane są zgodnie z wewnętrznym tagiem VLAN (tag VLAN sieci klienta) w sieci klienta).

Poniższy schemat przedstawia zwykle stosowane rozwiązanie z wykorzystaniem VLAN-VPN. Aby umożliwić komunikację pomiędzy dwoma sieciami VLAN klientów poprzez sieć ISP, można skonfigurować VLAN-VPN na przełącznikach brzegowych ISP, aby zezwolić na transmisję pakietów z sieci VLAN 100 i VLAN 200 klienta przez sieć ISP z zewnętrznym tagiem sieci VLAN 1050.

Rys. 1-1 Zwykle stosowane rozwiązanie z wykorzystaniem VLAN-VPN



## 1.2 Obsługiwane funkcje

Funkcja VLAN-VPN obejmuje: podstawowy VLAN-VPN oraz elastyczny VLAN-VPN (mapowanie VLAN).

### Basic (podstawowy) VLAN-VPN

Wszystkie pakiety z sieci VLAN klienta kapsułkowane są z tym samym tagiem VLAN sieci ISP, a następnie przesyłane do sieci ISP. Ponadto można także ustawić TPID (Tag Protocol Identifier), aby zapewnić zgodność z urządzeniami w sieci ISP.

### Flexible (elastyczny) VLAN-VPN

Można skonfigurować różne VLAN-y w sieci klienta, aby mapować do różnych sieci VLAN-ów sieci ISP.

Gdy przełącznik odbierze pakiet z tagiem sieci klienta, sprawdzi listę VLAN Mapping. Jeśli znajdzie dopasowanie, kapsułkuje pakiet z odpowiadającym mu tagiem VLAN sieci ISP i prześle go do odpowiadającego mu portu. Jeśli nie znajdzie dopasowania, przetworzy pakiet zgodnie z regułami MAC VLAN, protokołu VLAN oraz 802.1Q VLAN. Porty nietagowane przełącznik bezpośrednio przetwarza zgodnie z regułami MAC VLAN, protokołu VLAN oraz 802.1Q VLAN.



# 2 Podstawowa konfiguracja VLAN-VPN

Aby przeprowadzić podstawową konfigurację VLAN-VPN, wykonaj poniższe kroki:

- 1) skonfiguruj 802.1Q VLAN;
- 2) skonfiguruj porty NNI oraz porty UNI;
- 3) włącz globalnie VLAN-VPN.

## Wskazówki dotyczące konfiguracji

- Wartość TPID w ustawieniach przełącznika wynosi 0x8100. Jeśli urządzenia w sieci ISP nie obsługują tej wartości, należy ją zmienić, aby mieć pewność, że pakiety VLAN-VPN wysyłane do sieci ISP będą rozpoznawane i przesyłane przez urządzenia innych producentów.
- Możesz przejść do sekcji 802.1Q VLAN, aby dostosować funkcję Ingress Checking do swoich potrzeb. Przy włączonej funkcji Ingress Checking port wykona to działanie jako pierwsze, a następnie rozpocznie przetwarzanie pakietów w oparciu o konfigurację VLAN-VPN. Jeśli funkcja Ingress Checking jest wyłączona, port od razu rozpocznie przetwarzanie pakietów w oparciu o konfigurację VLAN-VPN.

## 2.1 Przez GUI

### 2.1.1 Konfiguracja 802.1Q VLAN

Przed skonfigurowaniem VLAN-VPN utwórz 802.1Q VLAN, dodaj porty do odpowiadających im VLAN-ów i skonfiguruj funkcję Ingress Checking na portach stosownie do swoich potrzeb. Szczegółowe informacje znajdziesz w części *Konfiguracja 802.1Q VLAN*.

## 2.1.2 Podstawowa konfiguracja VLAN-VPN

Wybierz z menu **L2 FEATURES > VLAN > VLAN VPN > VPN Config**, aby wyświetlić poniższą stronę.

Rys. 2-1 Podstawowa konfiguracja VPN

Global Config

---

VLAN VPN:  Enable Apply

---

Port Config

UNIT1
LAGS

| <input type="checkbox"/>            | Port   | Port Role | TPID | Missdrop |
|-------------------------------------|--------|-----------|------|----------|
| <input checked="" type="checkbox"/> | 1/0/1  | --        | 8100 | Disabled |
| <input type="checkbox"/>            | 1/0/2  | --        | 8100 | Disabled |
| <input type="checkbox"/>            | 1/0/3  | --        | 8100 | Disabled |
| <input type="checkbox"/>            | 1/0/4  | --        | 8100 | Disabled |
| <input type="checkbox"/>            | 1/0/5  | --        | 8100 | Disabled |
| <input type="checkbox"/>            | 1/0/6  | --        | 8100 | Disabled |
| <input type="checkbox"/>            | 1/0/7  | --        | 8100 | Disabled |
| <input type="checkbox"/>            | 1/0/8  | --        | 8100 | Disabled |
| <input type="checkbox"/>            | 1/0/9  | --        | 8100 | Disabled |
| <input type="checkbox"/>            | 1/0/10 | --        | 8100 | Disabled |

Total: 10
1 entry selected.
Cancel
Apply

Wykonaj poniższe kroki, aby skonfigurować podstawowe parametry VLAN-VPN:

- 1) W sekcji **Global Config** włącz globalnie VLAN-VPN i kliknij **Apply**.

---

VLAN-VPN Włącz globalnie funkcję VLAN-VPN.

---

- 2) W sekcji **VPN Port Config** wybierz co najmniej jeden port i skonfiguruj odpowiednie parametry. Kliknij **Apply**.

---

Port Role Wybierz rolę portu, która będzie mieć zastosowanie dla funkcji VLAN-VPN.

**NNI:** Porty NNI są zwykle połączone z siecią ISP, a pakiety przesyłane przez te porty mają zewnętrzne tagi VLAN.

**UNI:** Porty UNI są zwykle połączone z siecią klienta. Zewnętrzne tagi VLAN są dodawane lub usuwane, gdy pakiety są przesyłane przez port VPN.

*Uwaga:*

Bezpośrednie przetaczanie pomiędzy trybami UNI i NNI nie jest obsugiwane. Aby zmienić tryb, należy najpierw zmienić rolę portu na "--".

---

|          |                                                                                                                                                                                                                                                                        |
|----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| TPID     | Określ wartość TPID. TPID to pole tagu VLAN i jego modyfikacje są wymagane, gdy podwójnie tagowane pakiety mają być rozpoznawane przez urządzenia innych producentów.                                                                                                  |
| Missdrop | Włącz funkcję Missdrop. Opcja ta ma zastosowanie tylko w przypadku pakietów tagowanych. Po włączeniu tej funkcji pakiety tagowane, które nie pasują do wpisów Mapowania VLAN będą odrzucane.<br><br><i>Uwaga:</i> Funkcję Missdrop można włączyć tylko na portach NNI. |

### Uwaga:

- PVID portu UNI powinno być określane jako VLAN ID sieci VLAN ISP.
- Port należący do LAG (Link Aggregation Group) dostosowuje się do konfiguracji LAG zamiast korzystać z własnej. Konfiguracja własna portu ma zastosowanie dopiero w momencie, gdy port opuszcza LAG.

## 2.2 Przez CLI

### 2.2.1 Konfiguracja 802.1Q VLAN

Przed skonfigurowaniem VLAN-VPN utwórz 802.1Q VLAN, dodaj porty do odpowiadających im VLAN-ów i skonfiguruj funkcję Ingress Checking na portach stosownie do swoich potrzeb. Szczegółowe informacje znajdziesz w części *Konfiguracja 802.1Q VLAN*.

### 2.2.1 Podstawowa konfiguracja VLAN-VPN

Wykonaj poniższe kroki, aby skonfigurować podstawowe parametry VLAN-VPN:

|        |                                                                                                                                                                                                                                                                                                              |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Krok 1 | <b>configure</b><br>Uruchom tryb konfiguracji globalnej.                                                                                                                                                                                                                                                     |
| Krok 2 | <b>dot1q-tunnel</b><br>Włącz globalnie funkcję VLAN-VPN.                                                                                                                                                                                                                                                     |
| Krok 3 | <b>interface {fastEthernet port   range fastEthernet port-list   gigabitEthernet port   range gigabitEthernet port-list   ten-gigabitEthernet port   range ten-gigabitEthernet port-list   port-channel port-channel-id   range port-channel port-channel-list}</b><br>Uruchom tryb konfiguracji interfejsu. |

---

|         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|---------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Krok 4  | <b>switchport dot1q-tunnel mode { nni   uni }</b><br>Wybierz rolę portu, która będzie mieć zastosowanie dla funkcji VLAN-VPN.<br><br><i>nni</i> : Porty NNI są zwykle połączone z siecią ISP, a pakiety przesyłane przez te porty mają zewnętrzne tagi VLAN.<br><br><i>uni</i> : Porty UNI są zwykle połączone z siecią klienta. Zewnętrzne tagi VLAN są dodawane lub usuwane, gdy pakiety są przesyłane przez port VPN.<br><br><i>Uwaga:</i><br>Bezpośrednie przełączanie pomiędzy trybami UNI i NNI nie jest obsługiwane. Aby zmienić tryb, należy skorzystać z polecenia <b>no switchport dot1q-tunnel mode</b> , aby wyłączyć aktualny tryb. |
| Krok 5  | <b>switchport dot1q-tunnel tpid <i>tpid</i></b><br>Określ wartość TPID. TPID to pole tagu VLAN i jego modyfikacje są wymagane, gdy podwójnie tagowane pakiety mają być rozpoznawane przez urządzenia innych producentów.<br><br><i>tpid</i> : Wprowadź IPID dla portu. Muszą to być 4 liczby szesnastkowe. Wartością domyślną jest 8100.                                                                                                                                                                                                                                                                                                         |
| Krok 6  | <b>switchport dot1q-tunnel missdrop</b><br>Włącz funkcję Missdrop. Opcja ta ma zastosowanie tylko w przypadku pakietów tagowanych. Po włączeniu tej funkcji pakiety tagowane, które nie pasują do wpisów Mapowania VLAN będą odrzucane. Domyślnie funkcja jest wyłączona.<br><br><i>Uwaga:</i> Funkcję Missdrop można włączyć tylko na portach NNI.                                                                                                                                                                                                                                                                                              |
| Krok 7  | <b>show dot1q-tunnel</b><br>Przejrzyj globalną konfigurację VLAN-VPN.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Krok 8  | <b>show dot1q-tunnel interface</b><br>Przejrzyj konfigurację interfejsu podstawowych parametrów VLAN-VPN.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Krok 9  | <b>end</b><br>Powróć do trybu privileged EXEC.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Krok 10 | <b>copy running-config startup-config</b><br>Zapisz ustawienia w pliku konfiguracyjnym.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |

---

Poniższy schemat przedstawia przykładowy sposób globalnego włączania funkcji VLAN-VPN, ustawiania portu 1/0/1 przełącznika jako portu UNI oraz portu 1/0/2 jako portu NNI:

```
Switch#configure
```

```
Switch(config)#dot1q-tunnel
```

```
Switch(config)#interface gigabitEthernet 1/0/1
```

```
Switch(config-if)#switchport dot1q-tunnel mode uni
```

```
Switch(config-if)#exit
```

```
Switch(config)#interface gigabitEthernet 1/0/2
```

```
Switch(config-if)#switchport dot1q-tunnel mode nni
```

```
Switch(config-if)#show dot1q-tunnel
```

```
VLAN-VPN Mode: Enabled
```

```
Mapping Mode: Disabled
```

```
Switch(config-if)#show dot1q-tunnel interface
```

| Port    | Type  | Tpid   | Miss Drop | LAG |
|---------|-------|--------|-----------|-----|
| -----   | ----- | -----  | -----     | --- |
| Gi1/0/1 | UNI   | 0x8100 | Disable   | N/A |
| Gi1/0/2 | NNI   | 0x8100 | Enable    | N/A |

```
...
```

```
Switch(config-if)#end
```

```
Switch#copy running-config startup-config
```

# 3 Elastyczna konfiguracja VLAN-VPN

Aby przeprowadzić elastyczną konfigurację VLAN-VPN, wykonaj poniższe kroki:

- 1) skonfiguruj 802.1Q VLAN oraz podstawowy VLAN-VPN;
- 2) skonfiguruj mapowanie VLAN.

## Wskazówki dotyczące konfiguracji

- Zanim zaczniesz skonfiguruj najpierw 802.1Q VLAN i podstawowy VLAN-VPN.
- PVID portu UNI możesz dostosować do swoich potrzeb. Pakietom nietagowanym i tagowanym, które nie mają dopasowania wśród wpisów mapowania VLAN, można przydzielić zewnętrzny tag VLAN z PVID zgodnie z konfiguracją.

## 3.1 Przez GUI

Wybierz z menu **L2 FEATURES > VLAN > VLAN VPN > VLAN Mapping**, aby wyświetlić poniższą stronę.

Rys. 3-1 Włączanie elastycznego VLAN-VPN

Global Config

---

VLAN Mapping:  Enable Apply

VLAN Mapping Config

+ Add - Delete

| <input type="checkbox"/>  | Index | Port | C VLAN ID | C VLAN Name | SP VLAN ID | SP VLAN Name | Description | Operation |
|---------------------------|-------|------|-----------|-------------|------------|--------------|-------------|-----------|
| No entries in this table. |       |      |           |             |            |              |             |           |
| Total: 0                  |       |      |           |             |            |              |             |           |

Wykonaj poniższe kroki, aby przeprowadzić elastyczną konfigurację VLAN-VPN:

- 1) W sekcji **Global Config** włącz globalnie mapowanie VLAN i kliknij **Apply**.
- 2) W sekcji **VLAN Mapping Config** kliknij + **Add**, aby wyświetlić poniższą stronę. Skonfiguruj następujące parametry.

Rys. 3-2 Tworzenie wpisu mapowania VLAN

|             |                                                                           |
|-------------|---------------------------------------------------------------------------|
| Port        | Wybierz port NNI, aby włączyć mapowanie VLAN.                             |
| C VLAN      | Określ sieć VLAN klienta portu UNI wpisując VLAN ID lub nazwę sieci VLAN. |
| SP VLAN     | Określ sieć VLAN ISP portu UNI wpisując VLAN ID lub nazwę sieci VLAN.     |
| Description | Dodaj opis, aby ułatwić identyfikację mapowania VLAN.                     |

3) Kliknij **Create**.

## 3.2 Przez CLI

Wykonaj poniższe kroki, aby przeprowadzić elastyczną konfigurację VLAN-VPN:

|        |                                                                                                                                                                                                                                                                                                                                                                              |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Krok 1 | <b>configure</b><br>Uruchom tryb konfiguracji globalnej.                                                                                                                                                                                                                                                                                                                     |
| Krok 2 | <b>dot1q-tunnel mapping</b><br>Włącz globalnie mapowanie VLAN.                                                                                                                                                                                                                                                                                                               |
| Krok 3 | <b>interface {fastEthernet <i>port</i>   range fastEthernet <i>port-list</i>   gigabitEthernet <i>port</i>   range gigabitEthernet <i>port-list</i>   ten-gigabitEthernet <i>port</i>   range ten-gigabitEthernet <i>port-list</i>   port-channel <i>port-channel-id</i>   range port-channel <i>port-channel-list</i>}</b><br>Wybierz port NNI, aby włączyć mapowanie VLAN. |
| Krok 4 | <b>switchport dot1q-tunnel mapping <i>c-vlan</i> <i>sp-vlan</i> [ <i>descript</i> ]</b><br>Ustaw wpisy mapowania VLAN dla określonych portów.<br><br><i>c vlan</i> : Wpisz VLAN ID sieci klienta.<br><br><i>sp vlan</i> : Wpisz VLAN ID sieci ISP.<br><br><i>descript</i> : Dodaj opis, aby ułatwić identyfikację mapowania VLAN.                                            |

---

Krok 5      **end**  
Powróć do trybu privileged EXEC.

---

Krok 6      **copy running-config startup-config**  
Zapisz ustawienia w pliku konfiguracyjnym.

---

Poniższy schemat przedstawia przykładowy sposób włączania mapowania VLAN i ustawiania wpisu mapowania VLAN o nazwie mapping1 na porcie 1/0/3 w celu mapowania sieci VLAN 15 klienta do sieci VLAN 1040 ISP:

**Switch#configure**

**Switch(config)#dot1q-tunnel mapping**

**Switch(config)#show dot1q-tunnel**

VLAN-VPN Mode:    Enabled

Mapping Mode:     Enabled

**Switch(config)#interface gigabitEthernet 1/0/3**

**Switch(config-if)#switchport dot1q-tunnel mapping 15 1040 mapping1**

**Switch(config-if)#show dot1q-tunnel mapping**

| Port    | C-VLAN | SP-VLAN | Name     |
|---------|--------|---------|----------|
| -----   | -----  | -----   | -----    |
| Gi1/0/3 | 15     | 1040    | mapping1 |

**Switch(config-if)#end**

**Switch#copy running-config startup-config**



# 4 Przykłady konfiguracji

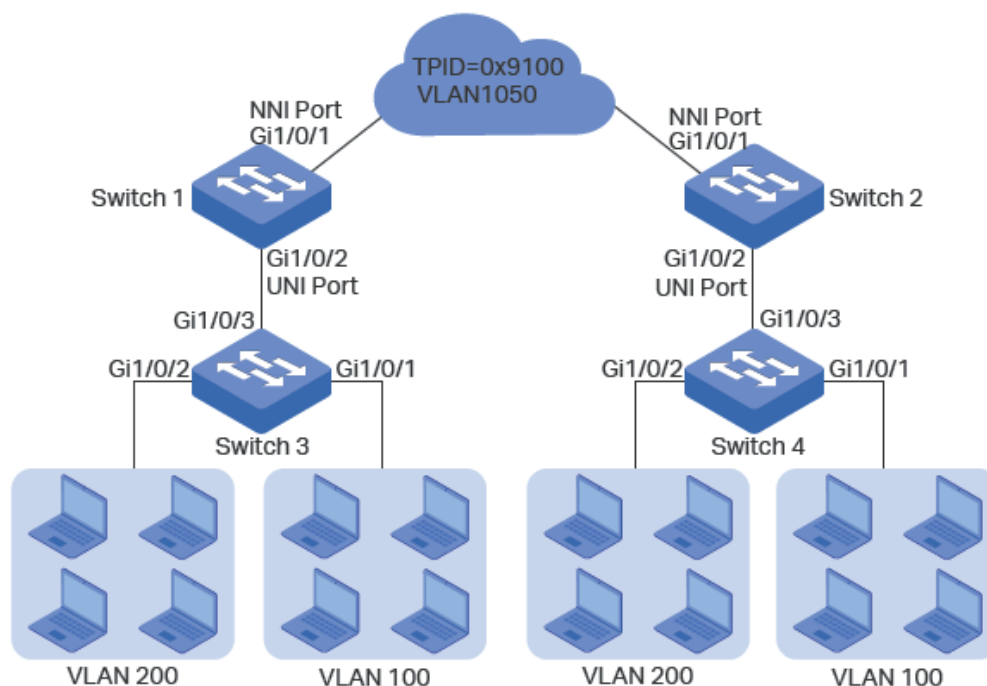
## 4.1 Przykład podstawowego VLAN VPN

### 4.1.1 Wymagania sieci

Firma ma dwa oddziały, a komputery należą odpowiednio do sieci VLAN 100 i sieci VLAN 200. Sieć VLAN ISP to VLAN 1050, a TPID przyjęte przez sieć ISP to 0x9100.

Oddziały firmy muszą komunikować się ze sobą poprzez sieć ISP. Wymaga się także, żeby transmisja ruchu z sieci VLAN 100 i VLAN 200 odbywała się w sieci VLAN 1050.

Rys. 4-1 Topologia sieci



### 4.1.2 Schemat konfiguracji

Aby spełnić warunek, który umożliwi transmisję ruchu z VLAN 100 i VLAN 200 przez sieć VLAN 1050, użytkownicy mogą skonfigurować podstawowy VLAN-VPN na przełączniku 1 i przełączniku 2, aby umożliwić przesyłanie pakietów z podwójnym tagiem VLAN i tym samym zapewnić ich wzajemną komunikację. Ogólna procedura konfiguracji wygląda w następujący sposób:

Schemat konfiguracji dotyczy tylko przełącznika 1 i przełącznika 3, ponieważ konfiguracja przełącznika 2 jest taka sama jak przełącznika 1, a konfiguracja przełącznika 4 pokrywa się z konfiguracją przełącznika 3.

- 1) Skonfiguruj 802.1Q VLAN na przełączniku 1. Parametry znajdują się poniżej:

|            | VLAN 100 | VLAN 200 | VLAN 1050 | PVID |
|------------|----------|----------|-----------|------|
| Port 1/0/1 | -        | -        | Tagged    | 1    |
| Port 1/0/2 | Tagged   | Tagged   | Untagged  | 1050 |

- 2) Skonfiguruj 802.1Q VLAN na przełączniku 3. Parametry znajdują się poniżej:

|            | VLAN 100 | VLAN 200 | PVID |
|------------|----------|----------|------|
| Port 1/0/1 | -        | Untagged | 100  |
| Port 1/0/2 | Untagged | -        | 200  |
| Port 1/0/3 | Tagged   | Tagged   | 1    |

- 3) Skonfiguruj VLAN VPN na przełączniku 1. Ustaw port 1/0/1 jako port NNI oraz port 1/0/2 jako port UNI; ustaw TPID jako 0x9100.

W poniższych podrozdziałach opisano dwa sposoby przeprowadzenia procedury konfiguracji: przez GUI oraz przez CLI.

### 4.1.3 Przez GUI

#### ■ Konfiguracja przełącznika 1

- 1) Przejdź do **L2 FEATURES > VLAN > 802.1Q VLAN**, aby utworzyć VLAN 100, VLAN 200 i VLAN 1050. Ustaw egress rule portu 1/0/2 w sieci VLAN 100 i VLAN 200 jako Tagged, a w sieci VLAN 1050 jako Untagged; ustaw egress rule portu 1/0/1 w sieci VLAN 1050 jako Tagged.

Rys. 4-2 Tworzenie VLAN 100

### VLAN Config

VLAN ID:  (2-4094, format: 2,4-5,8)

VLAN Name:  (1-16 characters)

#### Untagged Ports

Port:  (Format: 1/0/1, input or choose below)

UNIT1                      LAGS

Select All

1 2 3 4 5 6 7 8 9 10

 Selected     Unselected     Not Available

#### Tagged Ports

Port:  (Format: 1/0/1, input or choose below)

UNIT1                      LAGS

Select All

1 2 3 4 5 6 7 8 9 10

Rys. 4-3 Tworzenie VLAN 200

### VLAN Config

VLAN ID:  (2-4094, format: 2,4-5,8)

VLAN Name:  (1-16 characters)

#### Untagged Ports

Port:  (Format: 1/0/1, input or choose below)

Select All

UNIT1 LAGS

1  2  3  4  5  6  7  8  9  10

Selected  Unselected  Not Available

#### Tagged Ports

Port:  (Format: 1/0/1, input or choose below)

Select All

UNIT1 LAGS

1  2  3  4  5  6  7  8  9  10

Rys. 4-4 Tworzenie VLAN 1050

### VLAN Config

VLAN ID:  (2-4094, format: 2,4-5,8)

VLAN Name:  (1-16 characters)

#### Untagged Ports

Port:  (Format: 1/0/1, input or choose below)

UNIT1

1

2

3

4

5

LAGS

6

7

8

9

10

Select All

Selected

Unselected

Not Available

#### Tagged Ports

Port:  (Format: 1/0/1, input or choose below)

UNIT1

1

2

3

4

5

LAGS

6

7

8

9

10

Select All

Cancel

Create

- 2) Przejdź do **L2 FEATURES > VLAN > Port Config**, aby ustawić PVID jako 1050 dla portu 1/0/2 i pozostaw wartość domyślną 1 dla portu 1/0/1.

Rys. 4-5 Konfiguracja PVID

| Port Config                         |       |      |                  |                        |     |                         |
|-------------------------------------|-------|------|------------------|------------------------|-----|-------------------------|
| UNIT1                               |       | LAGS |                  |                        |     |                         |
| <input type="checkbox"/>            | Port  | PVID | Ingress Checking | Acceptable Frame Types | LAG | Details                 |
| <input type="checkbox"/>            | 1/0/1 | 1    | Enabled          | Admit All              | --- | <a href="#">Details</a> |
| <input checked="" type="checkbox"/> | 1/0/2 | 1050 | Enabled          | Admit All              | --- | <a href="#">Details</a> |

- 3) Przejdź do **L2 FEATURES > VLAN > VLAN VPN > VPN Config**, włącz globalnie VLAN VPN; ustaw port 1/0/1 jako port NNI, a port 1/0/2 jako port UNI. Ustaw także TPID portu 1/0/1 jako 9100.


Rys. 4-6 Włączanie globalne VLAN VPN i konfiguracja portów

Global Config

VLAN VPN:  Enable Apply

Port Config

| UNIT1                    |       | LAGS      |      |          |                    |  |
|--------------------------|-------|-----------|------|----------|--------------------|--|
| <input type="checkbox"/> | Port  | Port Role | TPID | Missdrop | Use Inner Priority |  |
| <input type="checkbox"/> | 1/0/1 | NNI       | 9100 | Disabled | Disabled           |  |
| <input type="checkbox"/> | 1/0/2 | UNI       | 8100 | Disabled | Disabled           |  |
| <input type="checkbox"/> | 1/0/3 | --        | 8100 | Disabled | Disabled           |  |

- 4) Kliknij  Save, aby zapisać ustawienia.

#### ■ Konfiguracja przełącznika 3

- 1) Przejdź do **L2 FEATURES > VLAN > 802.1Q VLAN**, aby utworzyć VLAN 100 i VLAN 200. Ustaw egress rules portu 1/0/1 w sieci VLAN 100 jako Untagged; egress rules portu 1/0/2 w sieci VLAN 200 jako Untagged; egress rule portu 1/0/3 w sieci VLAN 100 i VLAN 200 jako Tagged.

Rys. 4-7 Tworzenie VLAN 100

### VLAN Config

VLAN ID:  (2-4094, format: 2,4-5,8)

VLAN Name:  (1-16 characters)

#### Untagged Ports

Port:  (Format: 1/0/1, input or choose below)

Select All

UNIT1 LAGS

1  2  3  4  5  6  7  8  9  10

Selected  Unselected  Not Available

#### Tagged Ports

Port:  (Format: 1/0/1, input or choose below)

Select All

UNIT1 LAGS

1  2  3  4  5  6  7  8  9  10

Rys. 4-8 Tworzenie VLAN 200

### VLAN Config

VLAN ID:  (2-4094, format: 2,4-5,8)

VLAN Name:  (1-16 characters)

---

Untagged Ports

Port:  (Format: 1/0/1, input or choose below)

UNIT1

1

2

3

4

5

LAGS

6

7

8

9

10

Select All

Selected

Unselected

Not Available

---

Tagged Ports

Port:  (Format: 1/0/1, input or choose below)

UNIT1

1

2

3

4

5

LAGS

6

7

8

9

10

Select All

Cancel

Create

- 2) Przejdź do **L2 FEATURES > VLAN > Port Config**, aby ustawić PVID jako 100 dla portu 1/0/1 oraz 200 dla portu 1/0/2.

Rys. 4-9 Konfiguracja PVID

| Port Config              |       |      |                  |                        |     |                         |
|--------------------------|-------|------|------------------|------------------------|-----|-------------------------|
| UNIT1                    |       | LAGS |                  |                        |     |                         |
| <input type="checkbox"/> | Port  | PVID | Ingress Checking | Acceptable Frame Types | LAG | Details                 |
| <input type="checkbox"/> | 1/0/1 | 100  | Enabled          | Admit All              | --  | <a href="#">Details</a> |
| <input type="checkbox"/> | 1/0/2 | 200  | Enabled          | Admit All              | --  | <a href="#">Details</a> |
| <input type="checkbox"/> | 1/0/3 | 1    | Enabled          | Admit All              | --  | <a href="#">Details</a> |

- 3) Kliknij **Save**, aby zapisać ustawienia.



#### 4.1.4 Przez CLI

Konfiguracja ustawień przełącznika 1 i przełącznika 2 wygląda tak samo. W poniższym przykładzie omawiamy konfigurację ustawień na przykładzie przełącznika 1.

- Konfiguracja ustawień przełącznika 1

- 1) Utwórz VLAN 1050, VLAN 100 i VLAN 200.

```
Switch_1#configure
```

```
Switch_1(config)#vlan 1050
```

```
Switch_1(config-vlan)#name SP_VLAN
```

```
Switch_1(config-vlan)#exit
```

```
Switch_1(config)#vlan 100
```

```
Switch_1(config-vlan)#name C_VLAN100
```

```
Switch_1(config-vlan)#exit
```

```
Switch_1(config)#vlan 200
```

```
Switch_1(config-vlan)#name C_VLAN200
```

```
Switch_1(config-vlan)#exit
```

- 2) Dodaj port 1/0/1 do VLAN 1050 jako port tagowany, ustaw PVID jako 1050, ustaw port jako port NNI i ustaw TPID jako 9100.

```
Switch_1(config)#interface gigabitEthernet 1/0/1
```

```
Switch_1(config-if)#switchport general allowed vlan 1050 tagged
```

```
Switch_1(config-if)#switchport pvid1050
```

```
Switch_1(config-if)#switchport dot1q-tunnel mode nni
```

```
Switch_1(config-if)#switchport dot1q-tunnel tpid 9100
```

```
Switch_1(config-if)#exit
```

- 3) Dodaj port 1/0/2 do VLAN 1050 jako port nietagowany i dodaj go do VLAN 100 i VLAN 200 jako port tagowany. Ustaw PVID portu jako 1050. Ustaw port jako port UNI.

```
Switch_1(config)#interface gigabitEthernet 1/0/2
```

```
Switch_1(config-if)#switchport general allowed vlan 1050 untagged
```

```
Switch_1(config-if)#switchport general allowed vlan 100,200 tagged
```

```
Switch_1(config-if)#switchport pvid 1050
```

```
Switch_1(config-if)#switchport dot1q-tunnel mode uni
```

```
Switch_1(config-if)#exit
```

- 4) Włącz globalnie VLAN VPN

```
Switch_1(config)#dot1q-tunnel
Switch_1(config)#end
Switch_1#copy running-config startup-config
```

#### ■ Konfiguracja przełącznika 3

- 1) Utwórz VLAN 100 i VLAN 200.

```
Switch_3#configure
Switch_3(config)#vlan 100
Switch_3(config-vlan)#name C_VLAN100
Switch_3(config-vlan)#exit
Switch_3(config)#vlan 200
Switch_3(config-vlan)#name C_VLAN200
Switch_3(config-vlan)#exit
```

- 2) Dodaj port 1/0/1 do VLAN 100 i port 1/0/2 do VLAN 200 jako porty nietagowane; dodaj port 1/0/3 do VLAN 100 i VLAN 200 jako port tagowany. Ustaw PVID jako 100 dla portu 1/0/1 i 200 dla portu 1/0/2.

```
Switch_3(config)#interface gigabitEthernet 1/0/1
Switch_3(config-if)#switchport general allowed vlan 100 untagged
Switch_3(config-if)#switchport pvid 100
Switch_3(config-if)#exit
Switch_3(config)#interface gigabitEthernet 1/0/2
Switch_3(config-if)#switchport general allowed vlan 200 untagged
Switch_3(config-if)#switchport pvid 200
Switch_3(config-if)#exit
Switch_3(config)#interface gigabitEthernet 1/0/3
Switch_3(config-if)#switchport general allowed vlan 100,200 tagged
Switch_3(config-if)#end
Switch_3#copy running-config startup-config
```

### **Sprawdzanie konfiguracji VLAN VPN na przełączniku 1**

Sprawdzanie konfiguracji globalnej VLAN VPN:

```
Switch_3#show dot1q-tunnel
VLAN VPN Mode: Enabled
```

Mapping Mode: Disabled

Sprawdzanie konfiguracji portu up-link VPN i portu VPN:

Switch\_3#show dot1q-tunnel interface

| Port    | Type  | Tpid   | Miss Drop | LAG |
|---------|-------|--------|-----------|-----|
| -----   | ----- | -----  | -----     | --- |
| Gi1/0/1 | NNI   | 0x9100 | Disable   | N/A |
| Gi1/0/2 | UNI   | 0x8100 | Enable    | N/A |
| Gi1/0/3 | NONE  | 0x8100 | Disable   | N/A |
| Gi1/0/4 | NONE  | 0x8100 | Disable   | N/A |

...

Sprawdzanie konfiguracji portów:

Switch\_3#show interface switchport gigabitEthernet 1/0/1

Port Gi1/0/1:

PVID: 1050

Acceptable frame type: All

Ingress Checking: Enable

Member in LAG: N/A

Link Type: General

Member in VLAN:

| Vlan | Name        | Egress-rule |
|------|-------------|-------------|
| ---- | -----       | -----       |
| 1    | System-VLAN | Untagged    |
| 1050 | SP_VLAN     | Tagged      |

Switch\_3#show interface switchport gigabitEthernet 1/0/2

Port Gi1/0/2:

PVID: 1050

Acceptable frame type: All

Ingress Checking: Enable

Member in LAG: N/A

Link Type: General

Member in VLAN:

| Vlan | Name        | Egress-rule |
|------|-------------|-------------|
| ---- | -----       | -----       |
| 1    | System-VLAN | Untagged    |
| 100  | C_VLAN100   | Tagged      |
| 200  | C_VLAN200   | Tagged      |
| 1050 | SP_VLAN     | Untagged    |

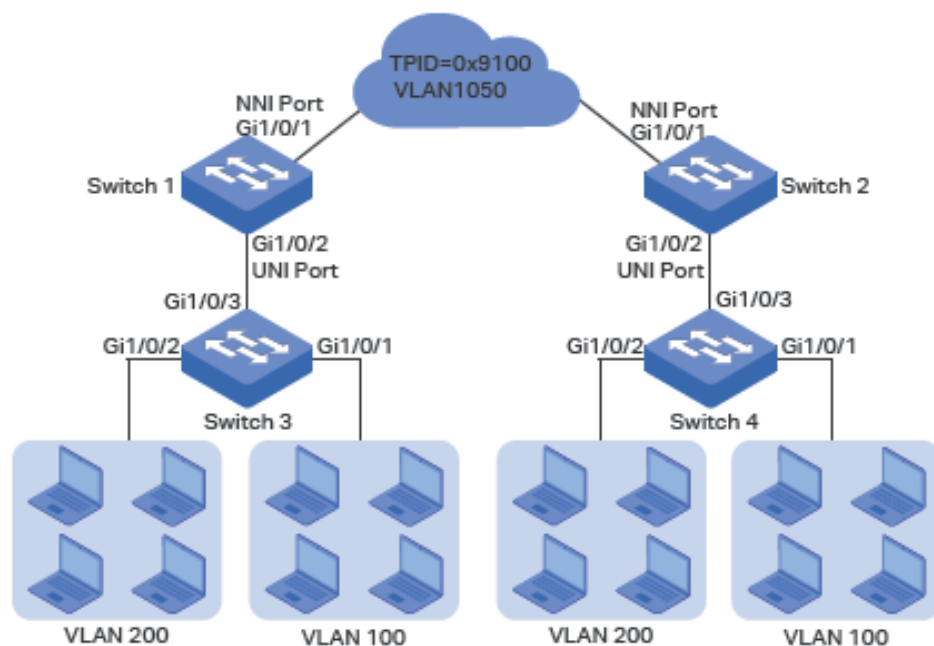
## 4.2 Przykład elastycznego VLAN VPN

### 4.2.1 Wymagania sieciowe

Firma ma dwa oddziały, a komputery należą odpowiednio do sieci VLAN 100 i sieci VLAN 200. Sieć VLAN ISP to VLAN 1050 i VLAN 1060, a TPID przyjęte przez sieć ISP to 0x9100.

Oddziały firmy muszą komunikować się ze sobą poprzez sieć ISP. Wymaga się także, żeby transmisja ruchu z sieci VLAN 100 odbywała się w sieci VLAN 1050, natomiast transmisji ruchu z sieci VLAN 200 w sieci VLAN 1060.

Rys. 4-10 Topologia sieci



## 4.2.2 Schemat konfiguracji

Aby spełnić warunek, który umożliwi całą transmisję ruchu z VLAN 100 i VLAN 200 przez różną sieć VLAN ISP, użytkownicy mogą skonfigurować elastyczny VLAN-VPN na przełączniku 1 i przełączniku 2, aby umożliwić mapowanie VLAN 100 do VLAN 1050 oraz VLAN 200 do VLAN 1060 i tym samym transmisję pakietów z sieci VLAN 100 i VLAN 200 odpowiednio przez sieć VLAN 1050 i VLAN 1060.

Schemat konfiguracji dotyczy tylko przełącznika 1 i przełącznika 3, ponieważ konfiguracja przełącznika 2 jest taka sama jak przełącznika 1, a konfiguracja przełącznika 4 pokrywa się z konfiguracją przełącznika 3.

1) Skonfiguruj 802.1Q VLAN na przełączniku 1. Parametry znajdują się poniżej:

|            | VLAN 100 | VLAN 200 | VLAN 1050 | VLAN 1060 | PVID |
|------------|----------|----------|-----------|-----------|------|
| Port 1/0/1 | -        | -        | Tagged    | Tagged    | 1    |
| Port 1/0/2 | Tagged   | Tagged   | Untagged  | Untagged  | 1050 |

2) Skonfiguruj 802.1Q VLAN na przełączniku 3. Parametry znajdują się poniżej:

|            | VLAN 100 | VLAN 200 | PVID |
|------------|----------|----------|------|
| Port 1/0/1 | -        | Untagged | 100  |
| Port 1/0/2 | Untagged | -        | 200  |
| Port 1/0/3 | Tagged   | Tagged   | 1    |

3) Skonfiguruj VLAN VPN na przełączniku 1. Ustaw port 1/0/1 jako port NNI i port 1/0/2 jako port UNI; ustaw TPID jako 0x9100; ustaw mapowanie VLAN 100 do VLAN 1050 oraz VLAN 200 do VLAN 1060.

W poniższych podrozdziałach opisano dwa sposoby przeprowadzenia procedury konfiguracji: przez GUI oraz przez CLI.

## 4.2.3 Przez GUI

### ■ Konfiguracja ustawień przełącznika 1

1) Przejdź do **L2 FEATURES > VLAN > 802.1Q VLAN**, aby utworzyć VLAN 100, VLAN 200, VLAN 1050 i VLAN 1060. Ustaw egress rule portu 1/0/2 w VLAN 100 i VLAN 200 jako Tagged oraz Untagged w sieci VLAN 1050 i VLAN 1060; ustaw egress rule portu 1/0/1 w sieci VLAN 1050 i VLAN 1060 jako Tagged.

Rys. 4-11 Tworzenie VLAN 100

### VLAN Config

VLAN ID:  (2-4094, format: 2,4-5,8)

VLAN Name:  (1-16 characters)

#### Untagged Ports

Port:  (Format: 1/0/1, input or choose below)

UNIT1                      LAGS

Select All

1    2    3    4    5    6    7    8    9    10

Selected    Unselected    Not Available

#### Tagged Ports

Port:  (Format: 1/0/1, input or choose below)

UNIT1                      LAGS

Select All

1    2    3    4    5    6    7    8    9    10

Rys. 4-12 Tworzenie VLAN 200

### VLAN Config

VLAN ID:  (2-4094, format: 2,4-5,8)

VLAN Name:  (1-16 characters)

#### Untagged Ports

Port:  (Format: 1/0/1, input or choose below)

Select All

UNIT1 LAGS

1  2  3  4  5  6  7  8  9  10

Selected  Unselected  Not Available

#### Tagged Ports

Port:  (Format: 1/0/1, input or choose below)

Select All

UNIT1 LAGS

1  2  3  4  5  6  7  8  9  10

Rys. 4-13 Tworzenie VLAN 1050

### VLAN Config

VLAN ID:  (2-4094, format: 2,4-5,8)

VLAN Name:  (1-16 characters)

#### Untagged Ports

Port:  (Format: 1/0/1, input or choose below)

Select All

UNIT1 LAGS

1  2  3  4  5  6  7  8  9  10

Selected  Unselected  Not Available

#### Tagged Ports

Port:  (Format: 1/0/1, input or choose below)

Select All

UNIT1 LAGS

1  2  3  4  5  6  7  8  9  10



Rys. 4-14 Tworzenie VLAN 1060

### VLAN Config

VLAN ID:  (2-4094, format: 2,4-5,8)

VLAN Name:  (1-16 characters)

#### Untagged Ports

Port:  (Format: 1/0/1, input or choose below)

Select All

UNIT1      LAGS

1  2  3  4  5  6  7  8  9  10

Selected     Unselected     Not Available

#### Tagged Ports

Port:  (Format: 1/0/1, input or choose below)

Select All

UNIT1      LAGS

1  2  3  4  5  6  7  8  9  10

- 2) Przejdź do **L2 FEATURES > VLAN > Port Config**, aby ustawić PVID jako 1050 dla portu 1/0/2 i pozostaw wartość domyślną 1 dla portu 1/0/1.

Rys. 4-15 Konfiguracja PVID

| Port Config                         |       |      |                  |                        |     |                         |
|-------------------------------------|-------|------|------------------|------------------------|-----|-------------------------|
| UNIT1                               |       | LAGS |                  |                        |     |                         |
| <input type="checkbox"/>            | Port  | PVID | Ingress Checking | Acceptable Frame Types | LAG | Details                 |
| <input type="checkbox"/>            | 1/0/1 | 1    | Enabled          | Admit All              | --- | <a href="#">Details</a> |
| <input checked="" type="checkbox"/> | 1/0/2 | 1050 | Enabled          | Admit All              | --- | <a href="#">Details</a> |

- 3) Przejdź do **L2 FEATURES > VLAN > VLAN VPN > VPN Config**, włącz globalnie VLAN VPN; ustaw port 1/0/1 jako port NNI i port 1/0/2 jako port UNI. Ustaw TPID portu 1/0/1 jako 9100.

Rys. 4-16 Włączanie globalnie VLAN VPN i konfiguracja portów

Global Config

VLAN VPN:  Enable

Port Config

| UNIT1                    | LAGS | Port  | Port Role | TPID | Missdrop | Use Inner Priority |
|--------------------------|------|-------|-----------|------|----------|--------------------|
| <input type="checkbox"/> |      | 1/0/1 | NNI       | 9100 | Disabled | Disabled           |
| <input type="checkbox"/> |      | 1/0/2 | UNI       | 8100 | Disabled | Disabled           |
| <input type="checkbox"/> |      | 1/0/3 | --        | 8100 | Disabled | Disabled           |

- 4) Przejdź do **L2 FEATURES > VLAN > VLAN VPN > VLAN Mapping**, włącz globalnie mapowanie VLAN. Następnie skonfiguruj mapowanie VLAN dla portu UNI 1/0/2.

Rys. 4-17 Mapowanie VLAN 100 do VLAN 1050

VLAN Mapping Config

Port:   (Format: 1/0/1)

Select All

UNIT1:  1  2  3  4  5  6  7  8  9  10

LAGS:  1  2

C VLAN:  ID  Name  (1-4094)

SP VLAN:  ID  Name  (1-4094)

Description:  (Optional. 1-16 characters)

Rys. 4-18 Mapowanie VLAN 200 do VLAN 1060

**VLAN Mapping Config**

Port:   (Format: 1/0/1)


UNIT1                      LAGS

Select All

C VLAN:  ID    Name  
 (1-4094)

SP VLAN:  ID    Name  
 (1-4094)

Description:  (Optional. 1-16 characters)

5) Kliknij  **Save**, aby zapisać ustawienia.

■ Konfiguracja ustawień przełącznika 3

- 1) Przejdź do **L2 FEATURES > VLAN > 802.1Q VLAN**, aby utworzyć VLAN 100 i VLAN 200. Ustaw egress rules portu 1/0/1 w sieci VLAN 100 jako Untagged; egress rules portu 1/0/2 w sieci VLAN 200 jako Untagged; egress rule portu 1/0/3 w sieci VLAN 100 i VLAN 200 jako Tagged.

Rys. 4-19 Tworzenie VLAN 100

### VLAN Config

VLAN ID:  (2-4094, format: 2,4-5,8)

VLAN Name:  (1-16 characters)

#### Untagged Ports

Port:  (Format: 1/0/1, input or choose below)

Select All

UNIT1 LAGS

1  2  3  4  5  6  7  8  9  10

Selected  Unselected  Not Available

#### Tagged Ports

Port:  (Format: 1/0/1, input or choose below)

Select All

UNIT1 LAGS

1  2  3  4  5  6  7  8  9  10

Rys. 4-20 Tworzenie VLAN 200

### VLAN Config

VLAN ID:  (2-4094, format: 2,4-5,8)

VLAN Name:  (1-16 characters)

---

Untagged Ports

Port:  (Format: 1/0/1, input or choose below)

Select All

UNIT1

2

3

4

5

6

7

8

LAGS

9

10

Selected

Unselected

Not Available

---

Tagged Ports

Port:  (Format: 1/0/1, input or choose below)

Select All

UNIT1

1

2

3

4

5

6

7

8

LAGS

9

10

Cancel

Create

- 2) Przejdź do **L2 FEATURES > VLAN > Port Config**, aby ustawić PVID jako 100 dla portu 1/0/1 i 200 dla portu 1/0/2.

Rys. 4-21 Konfiguracja PVID

| Port Config              |       |      |                  |                        |     |                         |
|--------------------------|-------|------|------------------|------------------------|-----|-------------------------|
| UNIT1                    |       | LAGS |                  |                        |     |                         |
| <input type="checkbox"/> | Port  | PVID | Ingress Checking | Acceptable Frame Types | LAG | Details                 |
| <input type="checkbox"/> | 1/0/1 | 100  | Enabled          | Admit All              | --- | <a href="#">Details</a> |
| <input type="checkbox"/> | 1/0/2 | 200  | Enabled          | Admit All              | --- | <a href="#">Details</a> |
| <input type="checkbox"/> | 1/0/3 | 1    | Enabled          | Admit All              | --- | <a href="#">Details</a> |

- 3) Kliknij  **Save**, aby zapisać ustawienia.

## 4.2.4 Przez CLI

- Konfiguracja ustawień przełącznika 1

- 1) Utwórz VLAN 100, VLAN 200, VLAN 1050 i VLAN 1060.

```
Switch_1#configure
```

```
Switch_1(config)#vlan 1050
```

```
Switch_1(config-vlan)#name SP_VLAN1050
```

```
Switch_1(config-vlan)#exit
```

```
Switch_1(config)#vlan 1060
```

```
Switch_1(config-vlan)#name SP_VLAN1060
```

```
Switch_1(config-vlan)#exit
```

```
Switch_1(config)#vlan 100
```

```
Switch_1(config-vlan)#name C_VLAN100
```

```
Switch_1(config-vlan)#exit
```

```
Switch_1(config)#vlan 200
```

```
Switch_1(config-vlan)#name C_VLAN200
```

```
Switch_1(config-vlan)#exit
```

- 2) Dodaj port 1/0/1 do VLAN 1050 i VLAN 1060 jako port tagowany, ustaw PVID jako 1050, port jako port NNI oraz ustaw TPID jako 9100.

```
Switch_1(config)#interface gigabitEthernet 1/0/1
```

```
Switch_1(config-if)#switchport general allowed vlan 1050,1060 tagged
```

```
Switch_1(config-if)#switchport pvid1050
```

```
Switch_1(config-if)#switchport dot1q-tunnel mode nni
```

```
Switch_1(config-if)#switchport dot1q-tunnel tpid 9100
```

```
Switch_1(config-if)#exit
```

- 3) Dodaj port 1/0/2 do VLAN 1050 i VLAN 1060 jako port nietagowany i dodaj go do VLAN 100 i VLAN 200 jako port tagowany. Ustaw PVID jako 1050. Ustaw port jako port UNI.

```
Switch_1(config)#interface gigabitEthernet 1/0/2
```

```
Switch_1(config-if)#switchport general allowed vlan 1050,1060 untagged
```

```
Switch_1(config-if)#switchport general allowed vlan 100,200 tagged
```

```
Switch_1(config-if)#switchport pvid 1050
```

```
Switch_1(config-if)#switchport dot1q-tunnel mode uni
```

```
Switch_1(config-if)#exit
```

- 4) Włącz mapowanie VLAN. Ustaw mapowanie VLAN 100 do VLAN 1050 i VLAN 200 do VLAN 1060 dla portu 1/0/2.

```
Switch_1(config)#dot1q-tunnel mapping
```

```
Switch_1(config)#interface gigabitEthernet 1/0/2
```

```
Switch_1(config-if)#switchport dot1q-tunnel mapping 100 1050 mapping
```

```
Switch_1(config-if)#switchport dot1q-tunnel mapping 200 1060 mapping
```

```
Switch_1(config-if)#exit
```

- 5) Włącz globalnie VLAN VPN

```
Switch_1(config)#dot1q-tunnel
```

```
Switch_1(config)#end
```

```
Switch_1#copy running-config startup-config
```

#### ■ Konfiguracja ustawień przełącznika 3

- 1) Utwórz VLAN 100 i VLAN 200.

```
Switch_3#configure
```

```
Switch_3(config)#vlan 100
```

```
Switch_3(config-vlan)#name C_VLAN100
```

```
Switch_3(config-vlan)#exit
```

```
Switch_3(config)#vlan 200
```

```
Switch_3(config-vlan)#name C_VLAN200
```

```
Switch_3(config-vlan)#exit
```

- 2) Dodaj port 1/0/1 do VLAN 100 i port 1/0/2 do VLAN 200 jako porty nietagowane; dodaj port 1/0/3 do VLAN 100 i VLAN 200 jako port tagowany. Ustaw PVID jako 100 dla portu 1/0/1 i 200 dla portu 1/0/2.

```
Switch_3(config)#interface gigabitEthernet 1/0/1
```

```
Switch_3(config-if)#switchport general allowed vlan 100 untagged
```

```
Switch_3(config-if)#switchport pvid 100
```

```
Switch_3(config-if)#exit
```

```
Switch_3(config)#interface gigabitEthernet 1/0/2
```

```
Switch_3(config-if)#switchport general allowed vlan 200 untagged
```

```
Switch_3(config-if)#switchport pvid 200
```

```
Switch_3(config-if)#exit
```

```
Switch_3(config)#interface gigabitEthernet 1/0/3
```

```
Switch_3(config-if)#switchport general allowed vlan 100,200 tagged
```

```
Switch_3(config-if)#end
```

```
Switch_3#copy running-config startup-config
```



# Część 11

## Konfiguracja GVRP

### ROZDZIAŁY

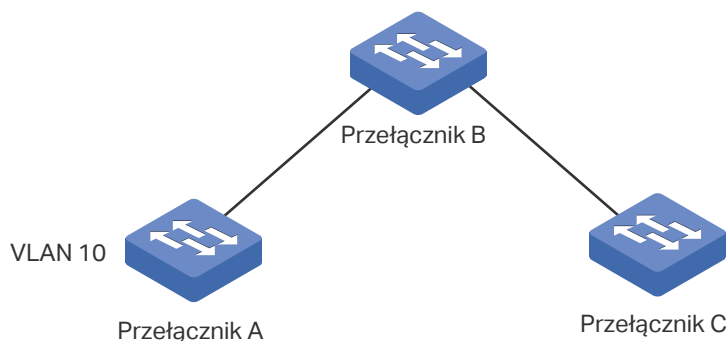
1. Informacje ogólne
2. Konfiguracja GVRP
3. Przykład konfiguracji

# 1 Informacje ogólne

GVRP (GARP VLAN Registration Protocol) to zastosowanie GARP (Generic Attribute Registration Protocol), które umożliwia zarejestrowanie i wyrejestrowanie wartości atrybutu VLAN i dynamiczne tworzenie sieci VLAN.

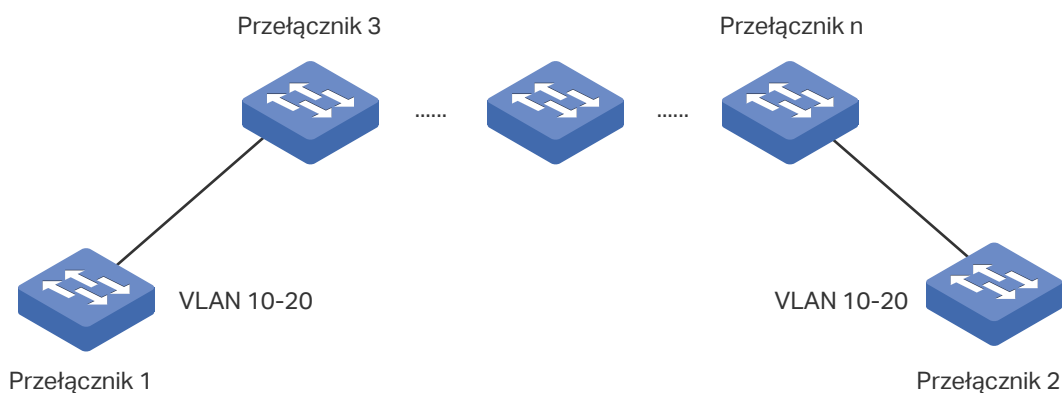
Bez GVRP konfiguracja w sieci tego samego VLAN-u wymagałaby jego ręcznej konfiguracji na każdym z urządzeń. Jak pokazano na Rys. 1-1, przełącznik A, B i C połączone są poprzez porty trunk. VLAN 10 skonfigurowano na przełączniku A, a VLAN 1 na przełączniku B i C. Przełącznik C może odbierać wiadomości wysyłane z przełącznika A w sieci VLAN 10 tylko wtedy, gdy administrator ręcznie utworzy VLAN 10 na przełączniku B i C.

Rys. 1-1 Topologia VLAD



W tej sytuacji konfiguracja nie sprawia większych trudności. Natomiast w przypadku większych i bardziej złożonych sieci ręczna konfiguracja byłaby znacznie bardziej czasochłonna i wymagająca. Funkcja GVRP może być stosowana do dynamicznego wdrażania konfiguracji VLAN. Dzięki GVRP przełącznik jest w stanie wymieniać informacje o konfiguracji VLAN z sąsiadującymi przełącznikami GVRP oraz dynamicznie tworzyć VLAN-y i zarządzać nimi. Zmniejsza to nakład pracy związany z konfiguracją VLAN-u i zapewnia poprawność jego konfiguracji.

Rys. 1-2 Topologia GVRP



## 2 Konfiguracja GVRP

Aby przeprowadzić konfigurację GVRP, postępuj zgodnie z poniższymi krokami.

- 1) Utwórz VLAN.
- 2) Włącz GVRP globalnie.
- 1) 3) Włącz GVRP na każdym porcie i skonfiguruj odpowiednie parametry.

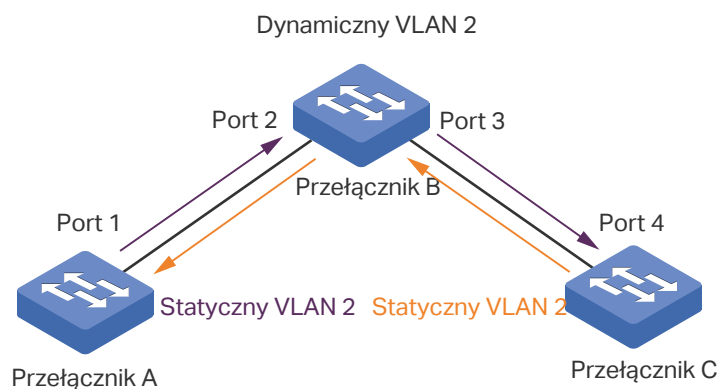
### Wskazówki dotyczące konfiguracji

Aby dynamicznie utworzyć VLAN na wszystkich portach na łączy sieci, należy ustawić ten sam statyczny VLAN po obu stronach łącza.

Ręcznie skonfigurowany 802.1Q VLAN nazywany jest statycznym, a VLAN utworzony przez GVRP to dynamiczny VLAN. Porty w statycznej sieci VLAN mogą inicjować wysyłanie komunikatu rejestracyjnego GVRP do innych portów. Port rejestruje sieci VLAN tylko po otrzymaniu komunikatu GVRP. Jako że komunikaty mogą być wysyłane tylko między dwoma podmiotami GVRP, do konfiguracji sieci VLAN na wszystkich portach łącza wymagana jest rejestracja dwustronna. Aby przeprowadzić rejestrację dwustronną należy ręcznie skonfigurować ten sam statyczny VLAN po obu stronach łącza.

Jak pokazano na poniższym rysunku, rejestracja VLAN z przełącznika A do przełącznika C skutkuje dodaniem portu 2 do VLAN 2. Rejestracja VLAN z przełącznika C do przełącznika A skutkuje dodaniem portu 3 do VLAN 2.

Rys. 2-1 Topologia sieci



Analogicznie, aby usunąć z łącza VLAN, wymagane jest dwustronne wyrejestrowanie. Należy ręcznie usunąć statyczny VLAN po obu stronach łącza.

## 2.1 Przez GUI

Wybierz z menu **L2 FEATURES > VLAN > GVRP > GVRP Config**, aby wyświetlić poniższą stronę.

Rys. 2-2 Konfiguracja GVRP

**GVRP**

---

GVRP:  Enable Apply

---

**Port Config**

UNIT1
LAGS

| <input type="checkbox"/>            | ID | Port   | Status   | Registration Mode | LeaveAll Timer (1000-30000 centiseconds) | Join Timer (20-1000 centiseconds) | Leave Timer (60-3000 centiseconds) | LAG |
|-------------------------------------|----|--------|----------|-------------------|------------------------------------------|-----------------------------------|------------------------------------|-----|
| <input checked="" type="checkbox"/> | 1  | 1/0/1  | Disabled | Normal            | 1000                                     | 20                                | 60                                 | --- |
| <input type="checkbox"/>            | 2  | 1/0/2  | Disabled | Normal            | 1000                                     | 20                                | 60                                 | --- |
| <input type="checkbox"/>            | 3  | 1/0/3  | Disabled | Normal            | 1000                                     | 20                                | 60                                 | --- |
| <input type="checkbox"/>            | 4  | 1/0/4  | Disabled | Normal            | 1000                                     | 20                                | 60                                 | --- |
| <input type="checkbox"/>            | 5  | 1/0/5  | Disabled | Normal            | 1000                                     | 20                                | 60                                 | --- |
| <input type="checkbox"/>            | 6  | 1/0/6  | Disabled | Normal            | 1000                                     | 20                                | 60                                 | --- |
| <input type="checkbox"/>            | 7  | 1/0/7  | Disabled | Normal            | 1000                                     | 20                                | 60                                 | --- |
| <input type="checkbox"/>            | 8  | 1/0/8  | Disabled | Normal            | 1000                                     | 20                                | 60                                 | --- |
| <input type="checkbox"/>            | 9  | 1/0/9  | Disabled | Normal            | 1000                                     | 20                                | 60                                 | --- |
| <input type="checkbox"/>            | 10 | 1/0/10 | Disabled | Normal            | 1000                                     | 20                                | 60                                 | --- |

Total: 10
1 entry selected.
Cancel
Apply

Aby skonfigurować GVRP, postępuj zgodnie z poniższymi krokami:

- 1) W sekcji **GVRP**, włącz GVRP globalnie i kliknij **Apply**.
- 2) W sekcji **Port Config** wybierz co najmniej jeden port, ustaw stan jako Enable i odpowiednio skonfiguruj powiązane parametry.

|        |                                                                            |
|--------|----------------------------------------------------------------------------|
| Port   | Wybierz port do konfiguracji GVRP. Możesz zaznaczyć więcej niż jeden port. |
| Status | Włącz lub wyłącz GVRP na porcie. Opcja jest domyślnie wyłączona.           |

|                              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Registration Mode            | <p>Wybierz tryb rejestracji GVRP dla portu.</p> <p><b>Normal:</b> W tym trybie port może dynamicznie rejestrować i wyrejestrowywać sieci VLAN oraz przekazywać dane rejestracyjne dynamicznych i statycznych sieci VLAN.</p> <p><b>Fixed:</b> W tym trybie port nie może dynamicznie rejestrować i wyrejestrowywać sieci VLAN. Port może przekazywać dane rejestracyjne tylko statycznych sieci VLAN.</p> <p><b>Forbidden:</b> W tym trybie nie może dynamicznie rejestrować i wyrejestrowywać sieci VLAN. Port może przekazywać dane tylko VLAN 1.</p>               |
| LeaveAll Timer (centisecond) | <p>Po włączeniu podmiotu GARP, włączony zostanie licznik LeaveAll. Po wygaśnięciu czasu LeaveAll podmiot GARP wyśle komunikaty LeaveAll do pozostałych podmiotów GARP, żeby te ponownie zarejestrowały wszystkie informacje o jego atrybutach. Po wszystkich podmiot restartuje licznik LeaveAll.</p> <p>Parametr czasowy licznika wynosi od 1000 do 30000 setnych sekundy i powinien być całkowitą wielokrotnością liczby 5. Wartość domyślna to 1000 setnych sekundy.</p>                                                                                           |
| Join Timer (centisecond)     | <p>Licznik Join kontroluje wysyłanie komunikatów Join. Podmiot GVRP włącza licznik Join po wysłaniu pierwszego komunikatu Join. Jeżeli podmiot nie otrzyma żadnej odpowiedzi, po wygaśnięciu czasu Join wyśle drugi komunikat, aby upewnić się, że komunikat Join może być wysłany do pozostałych podmiotów.</p> <p>Parametr czasowy licznika wynosi od 20 do 1000 setnych sekundy i powinien być całkowitą wielokrotnością liczby 5. Wartość domyślna to 20 setnych sekundy.</p>                                                                                     |
| Leave Timer (centisecond)    | <p>Licznik Leave kontroluje wyrejestrowywanie atrybutów. Podmiot wyśle komunikat Leave, jeżeli będzie wymagał od innych podmiotów wyrejestrowania części jego atrybutów. Po otrzymaniu komunikatu przez podmiot włączony zostaje licznik Leave. Jeżeli podmiot nie dostanie żadnego komunikatu Join dla odpowiadającego atrybutu przed wygaśnięciem czasu Leave, podmiot wyrejestrowuje atrybut.</p> <p>Parametr czasowy licznika wynosi od 60 do 3000 setnych sekundy i powinien być całkowitą wielokrotnością liczby 5. Wartość domyślna to 60 setnych sekundy.</p> |
| LAG                          | Wyświetl grupę LAG do której należy port.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |

### 3) Kliknij **Apply**.

#### Uwaga:

- Port należący do grupy LAG konfigurowany jest z grupą, nie oddzielnie. Konfiguracja portu może być przeprowadzona dopiero, gdy port opuści grupę LAG.
- Reguła wyjścia portów dodanych dynamicznie do sieci VLAN jest tagowana.
- Reguła wyjścia portów stałych powinna być tagowana.
- Ustawiając parametry czasowe licznika upewnij się, że wartości mieszczą się w wymaganym zakresie. Wartość LeaveAll powinna być większa niż dziesięciokrotność wartości Leave lub równa z nią. Wartość Leave powinna być większa niż dwukrotność wartości Join lub równa z nią.

## 2.2 Przez CLI

|        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Krok 1 | <b>configure</b><br>Wejdź w tryb konfiguracji globalnej.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Krok 2 | <b>gvrp</b><br>Włącz GVRP globalnie.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Krok 3 | <b>interface {fastEthernet <i>port</i>   range fastEthernet <i>port-list</i>   gigabitEthernet <i>port</i>   range gigabitEthernet <i>port-list</i>   ten-gigabitEthernet <i>port</i>   range ten-gigabitEthernet <i>port-list</i>   port-channel <i>port-channel-id</i>   range port-channel <i>port-channel-list</i>}</b><br>Wejdź w tryb konfiguracji interfejsu.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Krok 4 | <b>gvrp</b><br>Włącz GVRP na porcie.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Krok 5 | <b>gvrp registration { normal   fixed   forbidden }</b><br>Skonfiguruj tryb rejestracji GVRP dla portu. Domyślnie ustawiony jest tryb Normal.<br><br>normal: W tym trybie port może dynamicznie rejestrować i wyrejestrowywać sieci VLAN oraz przekazywać dane rejestracyjne dynamicznych i statycznych sieci VLAN.<br><br>fixed (stały): W tym trybie port nie może dynamicznie rejestrować i wyrejestrowywać sieci VLAN. Port może przekazywać dane rejestracyjne tylko statycznych sieci VLAN.<br><br>forbidden (zabroniony): W tym trybie nie może dynamicznie rejestrować i wyrejestrowywać sieci VLAN. Port może przekazywać dane tylko VLAN 1.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Krok 6 | <b>gvrp timer { leaveall   join   leave } <i>value</i></b><br>Ustaw odpowiednio liczniki GARP.<br><br>leaveall: Po włączeniu podmiotu GARP, włączony zostanie licznik LeaveAll. Po wygaśnięciu czasu LeaveAll podmiot GARP wyśle komunikaty LeaveAll do pozostałych podmiotów GARP, żeby te ponownie zarejestrowały wszystkie informacje o jego atrybutach. Po wszystkim podmiot restartuje licznik LeaveAll.<br><br>join: Licznik Join kontroluje wysyłanie komunikatów Join. Podmiot GVRP włącza licznik Join po wysłaniu pierwszego komunikatu Join. Jeżeli podmiot nie otrzyma żadnej odpowiedzi, wyśle drugi komunikat po wygaśnięciu czasu Join, aby upewnić się, że komunikat Join może być wysłany do pozostałych podmiotów.<br><br>leave: Licznik Leave kontroluje wyrejestrowywanie atrybutów. Podmiot wyśle komunikat Leave, jeżeli będzie wymagał od innych podmiotów wyrejestrowania części jego atrybutów. Po otrzymaniu komunikatu przez podmiot włączony zostaje licznik Leave. Jeżeli podmiot nie dostanie żadnego komunikatu Join dla odpowiadającego atrybutu przed wygaśnięciem czasu Leave, podmiot wyrejestrowuje atrybut.<br><br><i>value</i> : Ustaw parametr czasowy licznika. Powinien być całkowitą wielokrotnością liczby 5. Dla licznika LeaveAll wartość powinna wynosić od 1000 do 30000 setnych sekundy, wartość domyślna to 1000. Dla licznika Join wartość powinna wynosić od 20 do 1000 setnych sekundy, wartość domyślna to 20. Dla licznika Leave wartość powinna wynosić od 60 do 3000 setnych sekundy, wartość domyślna to 60. |

|         |                                                                                                                                                                                                                     |
|---------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Krok 7  | <b>show gvrp global</b><br>Sprawdź globalne ustawienia GVRP.                                                                                                                                                        |
| Krok 8  | <b>show gvrp interface [ fastEthernet <i>port</i>   gigabitEthernet <i>port</i>   ten-gigabitEthernet <i>port</i>   port-channel <i>port-channel-id</i> ]</b><br>Sprawdź konfigurację GVRP wybranego portu lub LAG. |
| Krok 9  | <b>end</b><br>Wróć do trybu privileged EXEC.                                                                                                                                                                        |
| Krok 10 | <b>copy running-config startup-config</b><br>Zapisz ustawienia w pliku konfiguracyjnym.                                                                                                                             |

 **Uwaga:**

- Port należący do grupy LAG konfigurowany jest z grupą, nie oddzielnie. Konfiguracja portu może być przeprowadzona dopiero, gdy port opuści grupę LAG.
- Reguła wyjścia portów dodanych dynamicznie do sieci VLAN jest tagowana.
- Reguła wyjścia portów stałych powinna być tagowana.
- Ustawiając parametry czasowe licznika upewnij się, że wartości mieszczą się w wymaganym zakresie. Wartość LeaveAll powinna być większa niż dziesięciokrotność wartości Leave lub równa z nią. Wartość Leave powinna być większa niż dwukrotność wartości Join lub równa z nią.

Poniższy przykład prezentuje włączanie GVRP globalnie i na porcie 1/0/1, konfigurację trybu rejestracji GVRP na stały i zachowanie wartości domyślnych liczników:

**Switch#configure**

**Switch(config)#gvrp**

**Switch(config)#interface gigabitEthernet 1/0/1**

**Switch(config-if)#gvrp**

**Switch(config-if)#gvrp registration fixed**

**Switch(config-if)#show gvrp global**

GVRP Global Status

-----

Enabled

**Switch(config-if)# show gvrp interface gigabitEthernet 1/0/1**

| Port    | Status  | Reg-Mode | LeaveAll | JoinIn | Leave | LAG |
|---------|---------|----------|----------|--------|-------|-----|
| ----    | -----   | -----    | -----    | -----  | ----- | --- |
| Gi1/0/1 | Enabled | Fixed    | 1000     | 20     | 60    | N/A |

```
Switch(config-if)#end
```

```
Switch#copy running-config startup-config
```

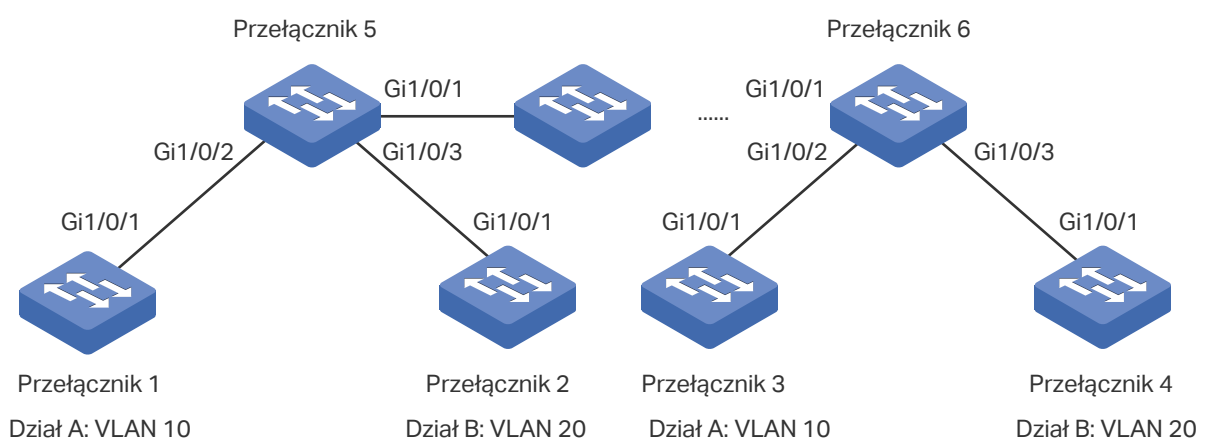


# 3 Przykład konfiguracji

## 3.1 Wymagania sieciowe

Dział A i dział B firmy połączone są za pomocą przełączników. Biura jednego działu rozmieszczone są na różnych piętrach. Jak pokazano na Rys. 3-1, topologia sieci jest skomplikowana. Aby komputery z tego samego działu mogły się ze sobą komunikować, wymagana jest konfiguracja tego samego VLAN-u na różnych przełącznikach.

Rys. 3-1 Topologia sieci



## 3.2 Schemat konfiguracji

W celu zmniejszenia obciążenia związanego z ręczną konfiguracją i obsługą należy włączyć funkcję GVRP, która pozwala na wdrożenie dynamicznej rejestracji VLAN i aktualizacji przełączników.

Konfigurując GVRP należy wziąć pod uwagę następujące kwestie:

- Działy firmy należą do różnych VLAN-ów. Aby mieć pewność, że przełączniki tworzą VLAN swojego działu wyłącznie dynamicznie, tryb rejestracji dla portów na przełączniku 1 i przełączniku 4 powinien być ustawiony jako Fixed, gdyż zapobiega to dynamicznemu rejestrowaniu i wyrejestrowywaniu VLAN-ów i sprawia, że na portach przesyłana jest tylko informacja o statycznej rejestracji VLAN.
- Aby skonfigurować dynamiczne tworzenie VLAN na innych przełącznikach, ustaw tryb rejestracji dla odpowiednich portów jako Normal, co pozwoli na dynamiczne rejestrowanie i wyrejestrowywanie VLAN-ów.

W poniższych podrozdziałach opisano dwa sposoby przeprowadzenia procedury konfiguracji: przez GUI oraz przez CLI.

### 3.3 Przez GUI

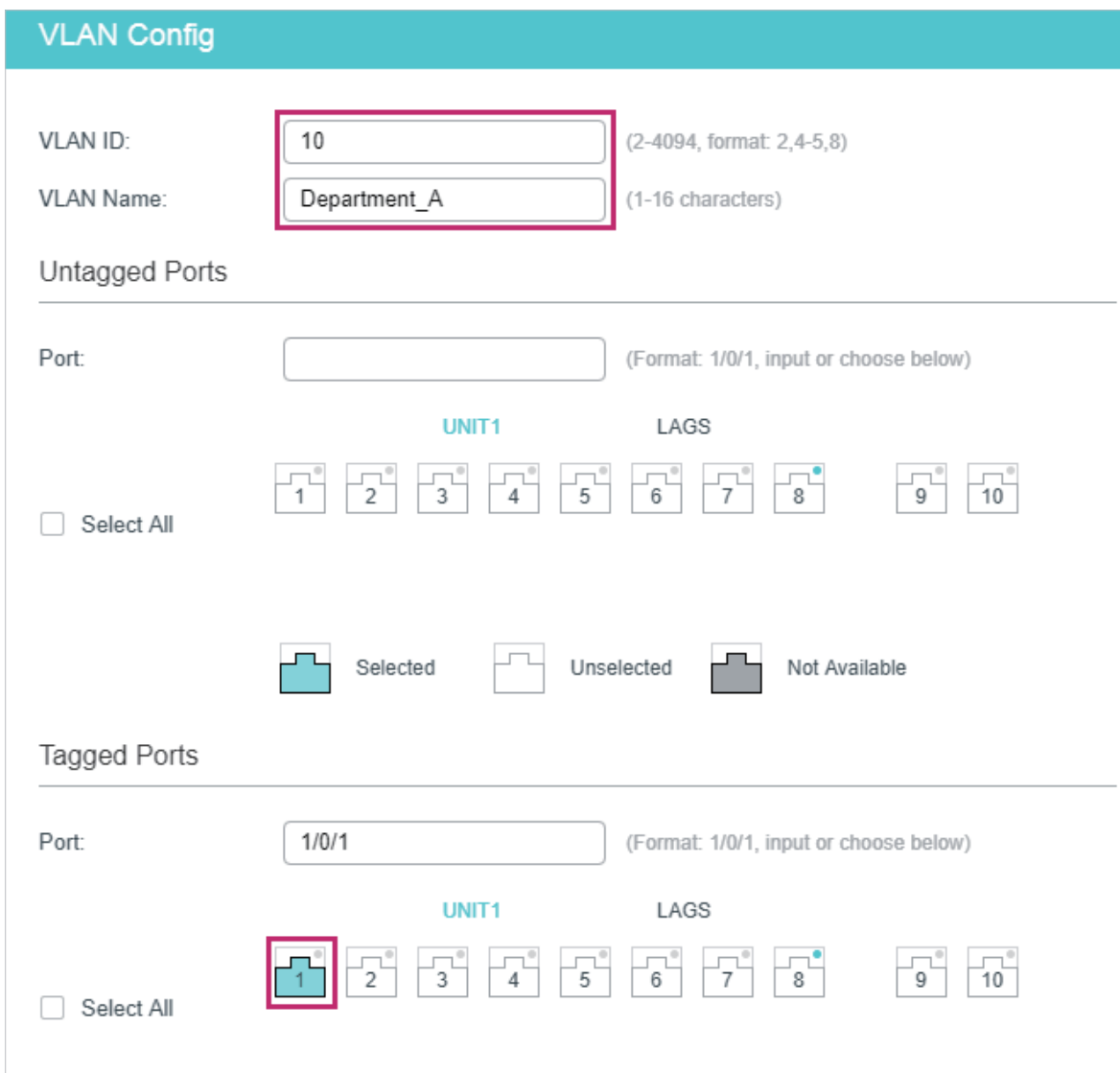
Konfiguracja GVRP przełącznika 3 jest taka sama jak przełącznika 1, a przełącznika 4 taka sama jak przełącznika 2. Inne przełączniki mają podobne ustawienia.

Poniższe procedury konfiguracji omówiono na przykładzie przełącznika 1, przełącznika 2 oraz przełącznika 5.

- Konfiguracja przełącznika 1

- 1) Wybierz z menu **L2 FEATURES > VLAN > 802.1Q VLAN > VLAN Config** i kliknij  **Add** aby wyświetlić poniższą stronę. Utwórz VLAN 10 i dodaj do niego tagowany port 1/0/1. Kliknij **Create**.

Rys. 3-2 Tworzenie VLAN 10



The screenshot shows the 'VLAN Config' interface. At the top, the title 'VLAN Config' is displayed in a teal header. Below this, there are two input fields: 'VLAN ID' with the value '10' and 'VLAN Name' with the value 'Department\_A'. A red box highlights these two fields. To the right of the 'VLAN ID' field, the text '(2-4094, format: 2,4-5,8)' is visible. To the right of the 'VLAN Name' field, the text '(1-16 characters)' is visible. Below these fields is the 'Untagged Ports' section. It starts with a 'Port:' label and an empty input field, with the text '(Format: 1/0/1, input or choose below)' to its right. Underneath, there are two columns of port icons: 'UNIT1' and 'LAGS'. The 'UNIT1' column contains icons for ports 1 through 8, and the 'LAGS' column contains icons for ports 9 and 10. A legend below the icons shows a teal icon for 'Selected', a white icon for 'Unselected', and a grey icon for 'Not Available'. In the 'Untagged Ports' section, port 1 in the UNIT1 column is selected and highlighted with a red box. Below the 'Untagged Ports' section is the 'Tagged Ports' section. It starts with a 'Port:' label and an input field containing '1/0/1', with the text '(Format: 1/0/1, input or choose below)' to its right. Underneath, there are two columns of port icons: 'UNIT1' and 'LAGS'. The 'UNIT1' column contains icons for ports 1 through 8, and the 'LAGS' column contains icons for ports 9 and 10. A legend below the icons shows a teal icon for 'Selected', a white icon for 'Unselected', and a grey icon for 'Not Available'. In the 'Tagged Ports' section, port 1 in the UNIT1 column is selected and highlighted with a red box.

- 2) Wybierz z menu **L2 FEATURES > VLAN > GVRP**, aby wyświetlić poniższą stronę. Włącz globalnie GVRP, a następnie kliknij **Apply**. Zaznacz port 1/0/1, ustaw Status jako Enable, a Registration Mode jako Fixed. Wartości regulacji czasowych pozostaw domyślnie. Kliknij **Apply**.

Rys. 3-3 Konfiguracja GVRP

GVRP


GVRP:  Enable

Port Config

UNIT1 LAGS

| <input type="checkbox"/>            | ID | Port   | Status   | Registration Mode | LeaveAll Timer (1000-30000 centiseconds) | Join Timer (20-1000 centiseconds) | Leave Timer (60-3000 centiseconds) | LAG |
|-------------------------------------|----|--------|----------|-------------------|------------------------------------------|-----------------------------------|------------------------------------|-----|
| <input checked="" type="checkbox"/> | 1  | 1/0/1  | Enabled  | Fixed             | 1000                                     | 20                                | 60                                 | --- |
| <input type="checkbox"/>            | 2  | 1/0/2  | Disabled | Normal            | 1000                                     | 20                                | 60                                 | --- |
| <input type="checkbox"/>            | 3  | 1/0/3  | Disabled | Normal            | 1000                                     | 20                                | 60                                 | --- |
| <input type="checkbox"/>            | 4  | 1/0/4  | Disabled | Normal            | 1000                                     | 20                                | 60                                 | --- |
| <input type="checkbox"/>            | 5  | 1/0/5  | Disabled | Normal            | 1000                                     | 20                                | 60                                 | --- |
| <input type="checkbox"/>            | 6  | 1/0/6  | Disabled | Normal            | 1000                                     | 20                                | 60                                 | --- |
| <input type="checkbox"/>            | 7  | 1/0/7  | Disabled | Normal            | 1000                                     | 20                                | 60                                 | --- |
| <input type="checkbox"/>            | 8  | 1/0/8  | Disabled | Normal            | 1000                                     | 20                                | 60                                 | --- |
| <input type="checkbox"/>            | 9  | 1/0/9  | Disabled | Normal            | 1000                                     | 20                                | 60                                 | --- |
| <input type="checkbox"/>            | 10 | 1/0/10 | Disabled | Normal            | 1000                                     | 20                                | 60                                 | --- |

Total: 10 1 entry selected.

3) Kliknij  Save, aby zapisać ustawienia.

#### ■ Konfiguracja przełącznika 2

1) Wybierz z menu **L2 FEATURES > VLAN > 802.1Q VLAN > VLAN Config** i kliknij  Add aby wyświetlić poniższą stronę. Utwórz VLAN 20 i dodaj do niego tagowany port 1/0/1. Kliknij **Create**.

Rys. 3-4 Tworzenie VLAN 20

### VLAN Config

VLAN ID:  (2-4094, format: 2,4-5,8)

VLAN Name:  (1-16 characters)

#### Untagged Ports

Port:

(Format: 1/0/1, input or choose below)

**UNIT1**                      **LAGS**

Select All

1    2    3    4    5    6    7    8    9    10

Selected    Unselected    Not Available

#### Tagged Ports

Port:  (Format: 1/0/1, input or choose below)

**UNIT1**                      **LAGS**

Select All

1    2    3    4    5    6    7    8    9    10

Selected    Unselected    Not Available

- Wybierz z menu **L2 FEATURES > VLAN > GVRP**, aby wyświetlić poniższą stronę. Włącz globalnie GVRP, a następnie kliknij **Apply**. Zaznacz port 1/0/1, ustaw Status jako Enable, a Registration Mode jako Fixed. Wartości regulacji czasowych pozostaw domyślnie. Kliknij **Apply**.

Rys. 3-5 Konfiguracja GVRP

GVRP


GVRP:  Enable

Port Config

UNIT1 LAGS

| <input type="checkbox"/>            | ID | Port   | Status   | Registration Mode | LeaveAll Timer (1000-30000 centiseconds) | Join Timer (20-1000 centiseconds) | Leave Timer (60-3000 centiseconds) | LAG |
|-------------------------------------|----|--------|----------|-------------------|------------------------------------------|-----------------------------------|------------------------------------|-----|
| <input checked="" type="checkbox"/> | 1  | 1/0/1  | Enabled  | Fixed             | 1000                                     | 20                                | 60                                 | --- |
| <input type="checkbox"/>            | 2  | 1/0/2  | Disabled | Normal            | 1000                                     | 20                                | 60                                 | --- |
| <input type="checkbox"/>            | 3  | 1/0/3  | Disabled | Normal            | 1000                                     | 20                                | 60                                 | --- |
| <input type="checkbox"/>            | 4  | 1/0/4  | Disabled | Normal            | 1000                                     | 20                                | 60                                 | --- |
| <input type="checkbox"/>            | 5  | 1/0/5  | Disabled | Normal            | 1000                                     | 20                                | 60                                 | --- |
| <input type="checkbox"/>            | 6  | 1/0/6  | Disabled | Normal            | 1000                                     | 20                                | 60                                 | --- |
| <input type="checkbox"/>            | 7  | 1/0/7  | Disabled | Normal            | 1000                                     | 20                                | 60                                 | --- |
| <input type="checkbox"/>            | 8  | 1/0/8  | Disabled | Normal            | 1000                                     | 20                                | 60                                 | --- |
| <input type="checkbox"/>            | 9  | 1/0/9  | Disabled | Normal            | 1000                                     | 20                                | 60                                 | --- |
| <input type="checkbox"/>            | 10 | 1/0/10 | Disabled | Normal            | 1000                                     | 20                                | 60                                 | --- |

Total: 10 1 entry selected.

3) Kliknij  Save, aby zapisać ustawienia.

#### ■ Konfiguracja przełącznika 5

1) Wybierz z menu **L2 FEATURES > VLAN > GVRP**, aby wyświetlić poniższą stronę. łącz globalnie GVRP, a następnie kliknij **Apply**. Zaznacz porty 1/0/1-3, ustaw Status jako Enable, a wartości Registration Mode oraz regulacji czasowych pozostaw domyślne. Kliknij **Apply**.


Rys. 3-6 Konfiguracja GVRP

GVRP

GVRP:  Enable

Port Config

| UNIT1                               |    | LAGS   |          |                   |                                          |                                   |                                    |                                       |                                      |
|-------------------------------------|----|--------|----------|-------------------|------------------------------------------|-----------------------------------|------------------------------------|---------------------------------------|--------------------------------------|
| <input type="checkbox"/>            | ID | Port   | Status   | Registration Mode | LeaveAll Timer (1000-30000 centiseconds) | Join Timer (20-1000 centiseconds) | Leave Timer (60-3000 centiseconds) | LAG                                   |                                      |
|                                     |    |        | Enable   |                   |                                          |                                   |                                    |                                       |                                      |
| <input checked="" type="checkbox"/> | 1  | 1/0/1  | Enabled  | Normal            | 1000                                     | 20                                | 60                                 | ---                                   |                                      |
| <input checked="" type="checkbox"/> | 2  | 1/0/2  | Enabled  | Normal            | 1000                                     | 20                                | 60                                 | ---                                   |                                      |
| <input checked="" type="checkbox"/> | 3  | 1/0/3  | Enabled  | Normal            | 1000                                     | 20                                | 60                                 | ---                                   |                                      |
| <input type="checkbox"/>            | 4  | 1/0/4  | Disabled | Normal            | 1000                                     | 20                                | 60                                 | ---                                   |                                      |
| <input type="checkbox"/>            | 5  | 1/0/5  | Disabled | Normal            | 1000                                     | 20                                | 60                                 | ---                                   |                                      |
| <input type="checkbox"/>            | 6  | 1/0/6  | Disabled | Normal            | 1000                                     | 20                                | 60                                 | ---                                   |                                      |
| <input type="checkbox"/>            | 7  | 1/0/7  | Disabled | Normal            | 1000                                     | 20                                | 60                                 | ---                                   |                                      |
| <input type="checkbox"/>            | 8  | 1/0/8  | Disabled | Normal            | 1000                                     | 20                                | 60                                 | ---                                   |                                      |
| <input type="checkbox"/>            | 9  | 1/0/9  | Disabled | Normal            | 1000                                     | 20                                | 60                                 | ---                                   |                                      |
| <input type="checkbox"/>            | 10 | 1/0/10 | Disabled | Normal            | 1000                                     | 20                                | 60                                 | ---                                   |                                      |
| Total: 10                           |    |        |          |                   | 3 entries selected.                      |                                   |                                    | <input type="button" value="Cancel"/> | <input type="button" value="Apply"/> |

2) Kliknij  Save, aby zapisać ustawienia.

### 3.4 Przez CLI

Konfiguracja GVRP przełącznika 3 jest taka sama jak przełącznika 1, a przełącznika 4 taka sama jak przełącznika 2. Inne przełączniki mają podobne ustawienia.

Poniższe procedury konfiguracji omówiono na przykładzie przełącznika 1, przełącznika 2 oraz przełącznika 5.

#### ■ Konfiguracja przełącznika 1

1) Włącz globalnie GVRP.

```
Switch_1#configure
```

```
Switch_1(config)#gvrp
```

2) Utwórz VLAN 10.

```
Switch_1(config)#vlan 10
```

```
Switch_1(config-vlan)#name Department A
```

```
Switch_1(config-vlan)#exit
```

- 3) Dodaj tagowany port 1/0/1 do VLAN 10. Włącz GVRP na porcie i ustaw registration mode jako Fixed.

```
Switch_1(config)#interface gigabitEthernet 1/0/1
Switch_1(config-if)#switchport general allowed vlan 10 tagged
Switch_1(config-if)#gvrp
Switch_1(config-if)#gvrp registration fixed
Switch_1(config-if)#end
Switch_1#copy running-config startup-config
```

#### ■ Konfiguracja przełącznika 2

- 1) Włącz globalnie GVRP.

```
Switch_2#configure
Switch_2(config)#gvrp
```

- 2) Utwórz VLAN 20.

```
Switch_2(config)#vlan 20
Switch_2(config-vlan)#name Department B
Switch_2(config-vlan)#exit
```

- 3) Dodaj tagowany port 1/0/1 do VLAN 20. Włącz GVRP na porcie i ustaw registration mode jako Fixed.

```
Switch_2(config)#interface gigabitEthernet 1/0/1
Switch_2(config-if)#switchport general allowed vlan 20 tagged
Switch_2(config-if)#gvrp
Switch_2(config-if)#gvrp registration fixed
Switch_2(config-if)#end
Switch_2#copy running-config startup-config
```

#### ■ Konfiguracja przełącznika 5

- 1) Włącz globalnie GVRP.

```
Switch_5#configure
Switch_5(config)#gvrp
```

- 2) Włącz GVRP na portach 1/0/1-3.

```
Switch_5(config)#interface range gigabitEthernet 1/0/1-3
Switch_5(config-if-range)#gvrp
```

```
Switch_5(config-if-range)#end
```

```
Switch_5#copy running-config startup-config
```

## Sprawdzanie konfiguracji

### ■ Przełącznik 1

Sprawdzanie globalnej konfiguracji GVRP:

```
Switch_1#show gvrp global
```

```
GVRP Global Status
```

```

```

```
Enabled
```

Sprawdzanie konfiguracji GVRP dla portu 1/0/1:

```
Switch_1#show gvrp interface
```

| Port    | Status   | Reg-Mode | LeaveAll | JoinIn | Leave | LAG |
|---------|----------|----------|----------|--------|-------|-----|
| ----    | -----    | -----    | -----    | -----  | ----- | --- |
| Gi1/0/1 | Enabled  | Fixed    | 1000     | 20     | 60    | N/A |
| Gi1/0/2 | Disabled | Normal   | 1000     | 20     | 60    | N/A |

```
.....
```

### ■ Przełącznik 2

Sprawdzanie globalnej konfiguracji GVRP:

```
Switch_2#show gvrp global
```

```
GVRP Global Status
```

```

```

```
Enabled
```

Sprawdzanie konfiguracji GVRP dla portu 1/0/1:

```
Switch_2#show gvrp interface
```

| Port    | Status  | Reg-Mode | LeaveAll | JoinIn | Leave | LAG |
|---------|---------|----------|----------|--------|-------|-----|
| ----    | -----   | -----    | -----    | -----  | ----- | --- |
| Gi1/0/1 | Enabled | Fixed    | 1000     | 20     | 60    | N/A |



```
Gi1/0/2 Disabled Normal 1000 20 60 N/A
```

```
.....
```

#### ■ Przetąicznik 5

Sprawdzanie globalnej konfiguracji GVRP:

GVRP Global Status

```

```

Enabled

Sprawdzanie konfiguracji GVRP dla portów 1/0/1-3:

Switch\_5#show gvrp interface

| Port    | Status   | Reg-Mode | LeaveAll | JoinIn | Leave | LAG |
|---------|----------|----------|----------|--------|-------|-----|
| ----    | -----    | -----    | -----    | -----  | ----- | --- |
| Gi1/0/1 | Enabled  | Normal   | 1000     | 20     | 60    | N/A |
| Gi1/0/2 | Enabled  | Normal   | 1000     | 20     | 60    | N/A |
| Gi1/0/3 | Enabled  | Normal   | 1000     | 20     | 60    | N/A |
| Gi1/0/4 | Disabled | Normal   | 1000     | 20     | 60    | N/A |

```
.....
```

# Część 12

## Konfiguracja multicastu L2

### ROZDZIAŁY

1. Multicast warstwy 2
2. Konfiguracja IGMP Snooping
3. Konfiguracja MLD Snooping
4. Konfiguracja MVR
5. Konfiguracja filtrowania pakietów multicastu
6. Przeglądanie informacji Multicast Snooping
7. Przykłady konfiguracji

# 1 Multicast warstwy 2

## 1.1 Informacje ogólne

W sieci point-to-multipoint pakiety mogą być przesyłane na trzy sposoby: poprzez transmisję typu unicast, broadcast lub multicast. W przypadku transmisji unicast wiele kopii tej samej informacji przesyłanych jest do wszystkich odbiorców, co wymaga dużej przepustowości.

W przypadku transmisji broadcast informacja przesyłana jest do wszystkich użytkowników sieci, niezależnie od tego, czy jej potrzebują, co powoduje marnowanie zasobów sieciowych i wpływa negatywnie na bezpieczeństwo informacji.

Natomiast transmisja multicast rozwiązuje wszystkie problemy powodowane przez transmisję unicast i broadcast. W przypadku tej transmisji urządzenie źródłowe wysyła tylko jedną informację i tylko ci użytkownicy, którzy jej potrzebują, otrzymają jej kopię. W sieci point-to-multipoint technologia multicast nie tylko pozwala na wydajną transmisję danych, ale także wymaga znacznie mniejszej przepustowości i redukuje obciążenie sieci.

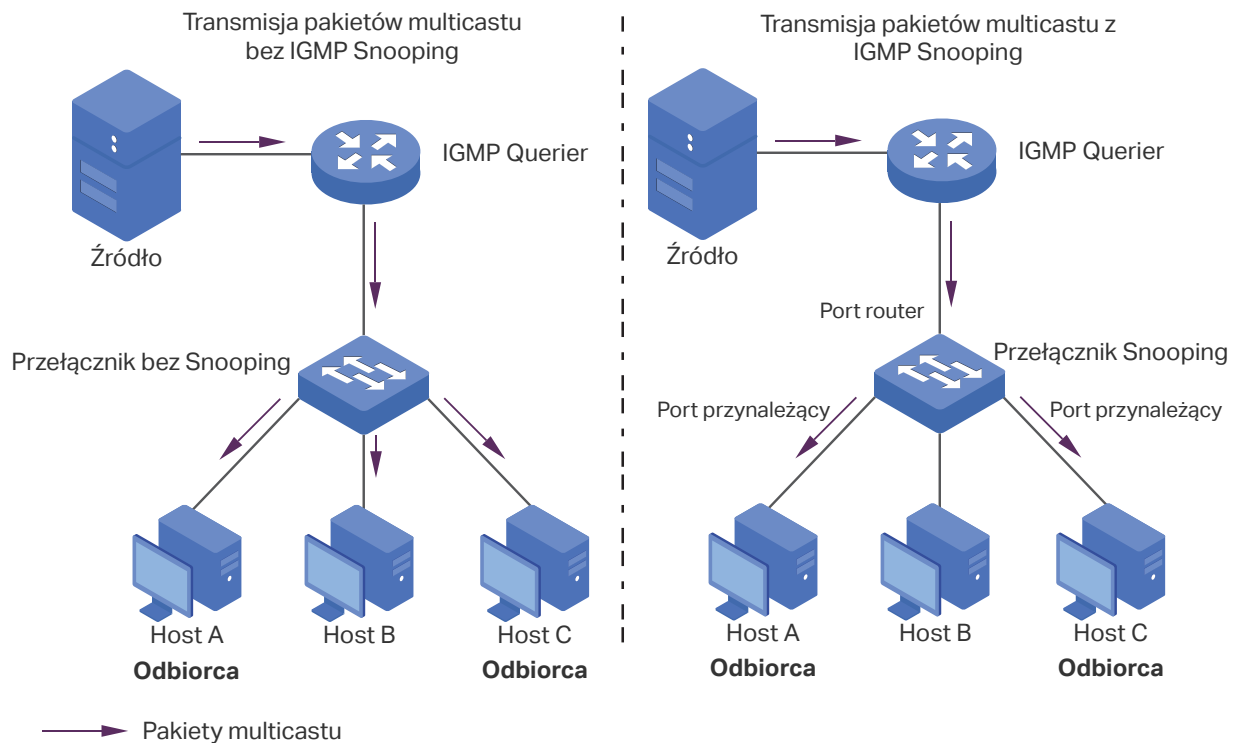
Jeśli chodzi o stronę praktyczną tego rozwiązania, dostawca Internetu ma możliwość oferowania dodatkowych usług, takich jak telewizja na żywo, IPTV, kształcenie na odległość, telemedycyna, radio internetowe i wideokonferencje w czasie rzeczywistym.

Multicast warstwy 2 umożliwia przełącznikom warstwy 2 nasłuchiwanie pakietów IGMP (Internet Group Management Protocol) przesyłanych pomiędzy IGMP Querier a hostami w celu stworzenia tablicy przekierowań ruchu multicastowego oraz zarządzania i kontrolowania transmisji pakietów.

Posługując się przykładem IGMP, gdy funkcja IGMP Snooping jest wyłączona na urządzeniu warstwy 2, pakiety multICASTu rozsyłane są w ramach sieci warstwy 2; gdy funkcja IGMP Snooping jest włączona na urządzeniu warstwy 2, dane multICASTu ze znajomej grupy multICASTowej są przesyłane do wyznaczonych odbiorców, a nie rozsyłane w ramach sieci warstwy 2.

Przedstawiono to poniżej:

Rys. 1-1 IGMP Snooping



Poniżej omówiono podstawowe pojęcia związane z IGMP Snooping: IGMP querier, przełącznik snooping, port router i port przynależący.

### IGMP Querier

IGMP querier to router multicast (router lub przełącznik warstwy 3), który wysyła zapytania w celu kontroli listy przynależności do grup multicastowych dla każdej powiązanej sieci oraz czasu trwania każdej przynależności.

Zwykle tylko jedno urządzenie w danej sieci fizycznej pełni rolę urządzenia odpytującego. Jeśli w sieci jest więcej niż jeden router multicast, uruchomiona zostanie procedura wyboru urządzenia odpytującego.

### Przełącznik Snooping

Przełącznik Snooping jest to przełącznik z uruchomioną funkcją IGMP Snooping. Przełącznik obsługuje tablicę przekierowań ruchu multicastowego poprzez podsłuch transmisji IGMP pomiędzy hostem a urządzeniem odpytującym. Korzystając z tablicy przekierowań ruchu multicastowego przełącznik może przesyłać dane multicastu tylko na porty, które są w odpowiedniej grupie multicastowej, aby ograniczyć zalewanie sieci warstwy 2 danymi multicastu.

### Port router

Port router to port przełącznika Snooping, który łączy się z IGMP querier.

### Port przynależący

Port przynależący to port przełącznika Snooping, który łączy się z hostem.

## 1.2 Obsługiwane funkcje

### Protokół multicastu warstwy 2 dla IPv4: IGMP Snooping

Na urządzeniach warstwy 2 IGMP Snooping sprawdza pakiety IGMP przesyłane przez sieć, przechwytyjąc informacje. Potrafi pasywnie nasłuchiwać komunikatów IGMP i w ten sposób uczyć się grup multicastowych. Potem następuje automatyczna konfiguracja portów przełącznika lub VLAN-ów i w efekcie ruch multicastowy jest wysyłany wyłącznie na odpowiednie porty przełącznika.

### Protokół multicastu warstwy 2 dla IPv6: MLD Snooping

Na urządzeniach warstwy 2 MLD Snooping sprawdza pakiety MLD przesyłane przez sieć, przechwytyjąc informacje. Potrafi pasywnie nasłuchiwać komunikatów MLD i w ten sposób uczyć się grup multicastowych. Potem następuje automatyczna konfiguracja portów przełącznika lub VLAN-ów i w efekcie ruch multicastowy jest wysyłany wyłącznie na odpowiednie porty przełącznika.

### MVR (Multicast VLAN Registration)

Funkcja MVR umożliwia kierowanie ruchu multicastowego VLAN-u do portów multicastu należących do innych VLAN-ów protokołu IPv4. W przypadku IGMP Snooping, jeżeli porty należą do innych VLAN-ów, kopia strumienia multicastowego przesyłana jest do każdego VLAN-u, który ma przypisane porty. Natomiast MVR zapewnia VLAN dedykowany transmisji multicastowej w sieci warstwy 2, aby zapobiec powielaniu strumieni multicastowych skierowanych do klientów przynależących do różnych VLAN-ów. Klienci mogą dynamicznie dołączać do VLAN-u multicastowego, a także go opuszczać, bez ingerencji w swoje powiązania z innymi VLAN-ami. Dostępne są dwa tryby MVR:

- Tryb kompatybilności

W trybie kompatybilności przełącznik MVR nie przesyła IGMP querier otrzymanych od przełącznika raportów oraz komunikatów leave, zatem IGMP querier nie ma możliwości nauczenia się przynależności grup multicastowych od przełącznika MVR. Aby możliwe było przesłanie wszystkich wymaganych strumieni multicastowych do przełącznika MVR poprzez VLAN multicastowy, IGMP querier musi być skonfigurowany statycznie.

- Tryb dynamiczny

W trybie dynamicznym, po otrzymaniu od hostów raportu lub komunikatu leave, przełącznik MVR prześle te informacje do IGMP querier poprzez VLAN multicastowy (z odpowiednią translacją VLAN ID). Zatem IGMP querier może nauczyć się przynależności grup multicastowych poprzez raporty i komunikaty leave, a także może przysyłać strumienie multicastowe do przełącznika MVR poprzez VLAN multicastowy, zgodnie z tablicą przekierowań ruchu multicastowego.

### Filtrowanie pakietów multicastu

Funkcja filtrowania pakietów multicastu umożliwia kontrolę grup multicastowych, do których host może przynależeć. Filtrowanie przyłączeń do grup multicastowych może odbywać się dla poszczególnych portów, poprzez konfigurację profili IP multicast (profili IGMP lub MLD), a następnie wiązanie ich z poszczególnymi portami przełącznika.

# 2 Konfiguracja IGMP Snooping

Aby przeprowadzić proces konfiguracji IGMP Snooping wykonaj poniższe kroki:

- 1) Uruchom IGMP Snooping globalnie i skonfiguruj parametry globalne.
- 2) Skonfiguruj IGMP Snooping dla VLAN-ów.
- 3) Skonfiguruj IGMP Snooping dla portów.
- 4) Skonfiguruj statyczne dołączanie hostów do grup (opcjonalnie).

## Uwaga:

Funkcja IGMP Snooping działa wyłącznie przy uruchomieniu globalnym - dla VLAN-u oraz odpowiednich portów.

## 2.1 Przez GUI

### 2.1.1 Konfiguracja globalna IGMP Snooping

Wybierz z menu L2 FEATURES > Multicast > IGMP Snooping > Global Config, aby wyświetlić poniższą stronę.

Rys. 2-1 Konfiguracja globalna IGMP Snooping

Global Config

---

IGMP Snooping:  Enable

IGMP Version:  v1  v2  v3

Unknown Multicast Groups:  Forward  Discard

Header Validation:  Enable

Wykonaj poniższe kroki, aby skonfigurować globalnie IGMP Snooping:

- 1) W sekcji Global Config uruchom globalnie IGMP Snooping i skonfiguruj parametry globalne

IGMP Snooping

Uruchom lub wyłącz globalnie IGMP Snooping.

|                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|--------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| IGMP Version             | <p>Podaj wersję IGMP.</p> <p><b>v1:</b> Przełącznik działa w trybie IGMPv1 Snooping. Może przetwarzać wyłącznie otrzymane od hosta komunikaty IGMPv1. Komunikaty innych wersji są ignorowane.</p> <p><b>v2:</b> Przełącznik działa w trybie IGMPv2 Snooping. Może przetwarzać zarówno komunikaty IGMPv1, jak i IGMPv2, otrzymane od hosta. Komunikaty IGMPv3 są ignorowane.</p> <p><b>v3:</b> Przełącznik działa w trybie IGMPv3 Snooping. Może przetwarzać otrzymane od hosta komunikaty wszystkich wersji: IGMPv1, IGMPv2 oraz IGMPv3.</p>                                                                                                                                                                                       |
| Unknown Multicast Groups | <p>Zdecyduj w jaki sposób przełącznik ma przetwarzać dane, które są przesyłane do nieznanymi grup multicastowych , wybierając spośród "Forward" (przesyłaj) lub "Discard" (odrzuć). Domyślnym ustawieniem jest Forward.</p> <p>Nieznane grupy multicastowe to grupy niepasujące do żadnej z grup przedstawionych we wcześniejszych raportach przynależności IGMP, a zatem nie ma ich na tablicy przekierowań ruchu multicastowego przełącznika.</p> <p><i>Uwaga:</i> IGMP Snooping i MLD Snooping współdzielą ustawienie Unknown Multicast Groups, dlatego konieczne jest przejście w tym samym czasie do strony L2 FEATURES &gt; Multicast &gt; MLD Snooping &gt; Global Config i globalne uruchomienie funkcji MLD Snooping.</p> |
| Header Validation        | <p>Włącz lub wyłącz Header Validation. Domyślnie opcja jest wyłączona.</p> <p>Dla pakietów IGMP wartością TTL powinno być 1, pola ToS 0xC0, a opcji Router Alert 0x94040000. Pola, które muszą być uzupełnione, zależą od wersji IGMP. IGMPv1 wymaga jedynie pola TTL. IGMPv2 wymaga pól TTL oraz Router Alert. IGMPv3 wymaga natomiast pól TTL, ToS oraz Router Alert. Pakiety, które nie przejdą pomyślnie procesu weryfikacji zostaną odrzucone.</p>                                                                                                                                                                                                                                                                            |

2) Kliknij **Apply**.

## 2.1.2 Konfiguracja IGMP Snooping dla VLAN-ów

Przed konfiguracją IGMP Snooping dla VLAN-ów, wybierz VLAN-y, do których przynależą porty routera i porty przełącznika. Szczegółowe informacje znajdziesz w rozdziale *Konfiguracja 802.1Q VLAN*.

Przełącznik umożliwia konfigurację IGMP Snooping dla poszczególnych VLAN-ów. Po globalnym uruchomieniu IGMP Snooping konieczne jest także włączenie IGMP Snooping i skonfigurowanie odpowiednich parametrów VLAN-ów, do których przynależą porty routera i porty przełącznika.

Wybierz z menu **L2 FEATURES > Multicast > IGMP Snooping > Global Config** i kliknij  przy wybranej pozycji VLAN-u w sekcji **IGMP VLAN Config**, aby wyświetlić poniższą stronę.

Rys. 2-2 Konfiguracja IGMP Snooping dla VLAN-u

Configure IGMP Snooping for VLAN

VLAN ID:

IGMP Snooping Status:  Enable

Fast Leave:  Enable

Report Suppression:  Enable

Member Port Aging Time:  seconds (60-600)

Router Port Aging Time:  seconds (60-600)

Leave Time:  seconds (1-30)

IGMP Snooping Querier:  Enable

Static Router Ports

Wykonaj poniższe kroki, aby skonfigurować IGMP Snooping dla określonych VLAN-ów:

1) Włącz IGMP Snooping dla VLAN-u i skonfiguruj odpowiednie parametry.

|                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| VLAN ID              | Identyfikator VLAN-u.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| IGMP Snooping Status | Włącz lub wyłącz IGMP Snooping dla VLAN-u.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Fast Leave           | <p>Włącz lub wyłącz funkcję szybkiego przełączania dla VLAN-u. IGMPv1 nie obsługuje Fast Leave.</p> <p>Wyłączona funkcja Fast Leave oznacza, że gdy odbiorca wysła komunikat leave IGMP, przełącznik prześle ten komunikat do urządzenia warstwy 3 (querier).</p> <p>Z punktu widzenia urządzenia odpytującego port łączący się z przełącznikiem jest portem przynależącym do odpowiedniej grupy multicastowej. Po otrzymaniu od przełącznika komunikatu leave, urządzenie odpytujące przesyła ustaloną liczbę zapytań (Last Member Query Count) dla określonych grup na tym porcie w ustalonym interwale czasowym (Last Member Query Interval), a następnie czeka na raporty dotyczące przynależności do grup IGMP. Jeżeli z przełącznikiem łączą się w tym czasie także inni odbiorcy, odpowiedzi na te zapytania prześlą przed wygaśnięciem Last Member Query Interval. Jeżeli żaden raport nie zostanie wysłany przed wygaśnięciem ostatniego zapytania, urządzenie odpytujące usunie port z listy przekierowań odpowiedniej grupy multicastowej.</p> <p>Jeżeli z przełącznikiem łączą się także inni odbiorcy, ten, który wysła komunikat leave musi poczekać aż port z listy przekierowań przełącznika odpowiedniej grupy multicastowej utraci ważność (maksymalny czas oczekiwania zależy od Member Port Aging Time).</p> <p>Przy włączonej dla VLAN-u opcji Fast Leave przełącznik usunie pozycję (Multicast Group, Port, VLAN) z tablicy przekierowań ruchu multicastowego przed przekazaniem komunikatu leave do urządzenia odpytującego. Pomaga to ograniczyć straty dostępnej przepustowości, ponieważ przełącznik zaprzestaje przesyłania strumieni multicastowych do VLAN-u portu od razu, gdy port otrzymuje z VLAN-u komunikat leave.</p> |



---

|                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Report Suppression     | <p>Włącz lub wyłącz ograniczanie wysyłania raportów dla VLAN-u.</p> <p>Przy włączonej opcji przełącznik przesyła urządzeniu odpytującemu tylko pierwszy raport IGMP dla każdej grupy multicastowej i hamuje przesył kolejnych raportów dla tych samych grup multicastowych w ramach jednego interwału zapytań. Pozwala to uniknąć wysyłania do IGMP querier zdublowanych komunikatów.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Member Port Aging Time | <p>Podaj czas utraty ważności portów przynależących do VLAN-u.</p> <p>Gdy przełącznik otrzymuje z portu raport IGMP, od razu dodaje on ten port do listy portów przynależących do określonej grupy multicastowej. Pozyskane w ten sposób porty nazywane są portami dynamicznymi.</p> <p>Jeżeli przełącznik nie otrzymuje z portu dynamicznego żadnych raportów IGMP dla określonej grupy multicastowej przed utratą ważności portu, usuwa on ten port z listy przekierowań ruchu multicastowego, ponieważ nie uznaje go już za port przynależący do określonej grupy multicastowej.</p>                                                                                                                                                                                                                                                                                                                                  |
| Router Port Aging Time | <p>Podaj czas utraty ważności portów routera przynależących do VLAN-u.</p> <p>Gdy przełącznik otrzymuje z portu komunikat z zapytaniem IGMP, dodaje on ten porty do listy portów routera. Pozyskane w ten sposób porty routera nazywane są dynamicznymi portami routera.</p> <p>Jeżeli przełącznik nie otrzymuje z portu dynamicznego routera żadnych komunikatów z zapytaniem IGMP przed utratą ważności portu, usuwa on ten port z listy portów routera, ponieważ nie uznaje go już za port routera.</p>                                                                                                                                                                                                                                                                                                                                                                                                               |
| Leave Time             | <p>Podaj czas opuszczenia grupy dla VLAN-u.</p> <p>Gdy przełącznik otrzymuje z portu komunikat o zamiarze opuszczenia grupy multicastowej, nie usuwa go od razu z grupy multicastowej, tylko czeka na określony Leave Time. Jeżeli w tym czasie przełącznik otrzyma komunikat z portu, nie zostanie on usunięty z grupy multicastowej. Wyjątkami są następujące sytuacje:</p> <ul style="list-style-type: none"><li>• Jeżeli port utraci ważność przed upływem Leave Time i żaden raport nie zostanie wysłany, port zostanie usunięty z grupy multicastowej po upływie Member Port Aging Time.</li><li>• Mechanizm Leave Time nie ma zastosowania, gdy włączona jest funkcja Fast Leave.</li></ul> <p>Podanie odpowiedniej wartości Leave Time pozwala uniknąć omyłkowego usuwania z grupy multicastowej innych hostów łączących się z tym samym portem przełącznika, podczas gdy tylko niektóre chcą opuścić grupę.</p> |
| IGMP Snooping Querier  | <p>Włącz lub wyłącz funkcję IGMP Snooping Querier dla VLAN-u.</p> <p>Włączona funkcja oznacza, że przełącznik pełni rolę IGMP Snooping Querier dla hostów należących do tego VLAN-u. Urządzenie odpytujące cyklicznie rozsyła zapytanie w sieci, aby uzyskać informacje o przynależności, a następnie, po otrzymaniu od hostów komunikatów leave, rozsyła zapytania do grup.</p> <p><i>Uwaga:</i></p> <p>Aby możliwe było włączenie IGMP Snooping Querier dla VLAN-u, funkcja IGMP Snooping powinna być uruchomiona zarówno globalnie, jak i dla VLAN-u.</p>                                                                                                                                                                                                                                                                                                                                                             |

---

|                            |                                                                                                                                                                                                                                                                                                                                                                                                                               |
|----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Query Interval             | Gdy włączysz funkcję IGMP Snooping Querier, podaj interwał wysyłania przez przełącznik zapytań ogólnych.                                                                                                                                                                                                                                                                                                                      |
| Maximum Response Time      | Gdy włączysz funkcję IGMP Snooping Querier, podaj maksymalny czas odpowiedzi hostów na zapytania ogólne.                                                                                                                                                                                                                                                                                                                      |
| Last Member Query Interval | Włączona funkcja IGMP Snooping Querier oznacza, że gdy przełącznik otrzymuje komunikat leave IGMP, pozyskuje on z komunikatu adres grupy multicastowej, którą host chce opuścić. Następnie przełącznik wysyła określone zapytania bezpośrednio do tej grupy multicastowej na porcie odbierającym komunikaty leave. Ten parametr jest wartością interwału pomiędzy zapytaniami przesyłanymi bezpośrednio do grup.              |
| Last Member Query Count    | Gdy włączysz funkcję IGMP Snooping Querier, podaj liczbę zapytań, które mają być przesłane bezpośrednio do grup. Jeżeli ustalona liczba zapytań zostanie wysłana, ale w odpowiedzi żaden raport nie zostanie przesłany, przełącznik usunie adres tego ruchu multicastowego z listy przekierowań ruchu multicastowego.                                                                                                         |
| General Query Source IP    | Gdy włączysz funkcję IGMP Snooping Querier, podaj źródłowy adres IP zapytań ogólnych, wysyłanych przez przełącznik. Wartość powinna być adresem unicast.                                                                                                                                                                                                                                                                      |
| Static Router Ports        | Wybierz jeden lub więcej portów, które mają być statycznymi portami routera w sieci VLAN. Statyczne porty routera nie tracą ważności.<br><br>Strumienie multicastowe i pakiety IGMP będą przesyłane na statycznych portach routera do wszystkich grup tego VLAN-u. Strumienie multicastowe i pakiety IGMP grup, do których przynależą porty dynamiczne routera, będą przesyłane na odpowiednich dynamicznych portach routera. |
| Forbidden Router Ports     | Wybierz porty, które nie będą mogły być portami routera w sieci VLAN.                                                                                                                                                                                                                                                                                                                                                         |

2) Kliknij **Save**.

## 2.1.3 Konfiguracja IGMP Snooping dla portów

Wybierz z menu **L2 FEATURES > Multicast > IGMP Snooping > Port Config**, aby wyświetlić poniższą stronę.

Rys. 2-3 Konfiguracja IGMP Snooping dla portów

The screenshot shows the 'Port Config' interface. At the top, there are tabs for 'UNIT1' and 'LAGS'. Below them is a table with columns: 'Port', 'IGMP Snooping', 'Fast Leave', and 'LAG'. The first row (1/0/1) is selected, indicated by a checkmark in the first column. The 'IGMP Snooping' column for all rows is 'Enabled', and the 'Fast Leave' column is 'Disabled'. The 'LAG' column shows '---' for all ports. At the bottom, there is a summary bar: 'Total: 10', '1 entry selected.', and two buttons: 'Cancel' and 'Apply'.

| <input type="checkbox"/>            | Port   | IGMP Snooping | Fast Leave | LAG |
|-------------------------------------|--------|---------------|------------|-----|
| <input checked="" type="checkbox"/> | 1/0/1  | Enabled       | Disabled   | --- |
| <input type="checkbox"/>            | 1/0/2  | Enabled       | Disabled   | --- |
| <input type="checkbox"/>            | 1/0/3  | Enabled       | Disabled   | --- |
| <input type="checkbox"/>            | 1/0/4  | Enabled       | Disabled   | --- |
| <input type="checkbox"/>            | 1/0/5  | Enabled       | Disabled   | --- |
| <input type="checkbox"/>            | 1/0/6  | Enabled       | Disabled   | --- |
| <input type="checkbox"/>            | 1/0/7  | Enabled       | Disabled   | --- |
| <input type="checkbox"/>            | 1/0/8  | Enabled       | Disabled   | --- |
| <input type="checkbox"/>            | 1/0/9  | Enabled       | Disabled   | --- |
| <input type="checkbox"/>            | 1/0/10 | Enabled       | Disabled   | --- |

Total: 10      1 entry selected.           

Wykonaj poniższe kroki, aby skonfigurować IGMP Snooping dla portów:

- 1) Włącz IGMP Snooping dla portu i włącz Fast Leave, jeżeli z portem połączony jest tylko jeden odbiorca.

|               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|---------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| IGMP Snooping | Włącz lub wyłącz IGMP Snooping dla portu.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Fast Leave    | <p>Włącz lub wyłącz Fast Leave na porcie. IGMPv1 nie obsługuje tej funkcji.</p> <p>Funkcja Fast Leave może działać dla poszczególnych portów lub VLAN-ów. Włączenie funkcji dla poszczególnych portów oznacza, że przełącznik usunie port z odpowiedniej grupy multicastowej wszystkich VLAN-ów przed przesłaniem komunikatu leave do urządzenia odpytującego.</p> <p>Włączenie funkcji Fast Leave dla portu zalecane jest w sytuacji, gdy do portu podłączony jest tylko jeden odbiorca. Więcej informacji o funkcji Fast Leave znajdziesz w rozdziale 2.1.2 Konfiguracja IGMP Snooping dla VLAN-ów.</p> |
| LAG           | Grupa agregacji łączy, do której należy port.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |

- 2) Kliknij **Apply**.

## 2.1.4 Konfiguracja statycznego dołączania hostów do grup

Hosty lub porty warstwy 2 dołączają zwykle dynamicznie do grup multicastowych, ale możliwe jest także statyczne przyłączanie się hostów do grup.

Wybierz z menu **L2 FEATURES > Multicast > IGMP Snooping > Static Group Config** i kliknij **+ Add**, aby wyświetlić poniższą stronę.

Rys. 2-4 Konfiguracja statycznego dołączania hostów do grup

Wykonaj poniższe kroki, aby skonfigurować statyczne dołączanie hostów do grup:

- 1) Podaj adres IP i VLAN ID ruchu multicastowego. Zaznacz porty, które mają statycznie przynależać do grupy multicastowej.

|              |                                                                                                                                      |
|--------------|--------------------------------------------------------------------------------------------------------------------------------------|
| Multicast IP | Podaj adres grupy multicastowej, do której mają dołączyć hosty.                                                                      |
| VLAN ID      | Określ VLAN hostów.                                                                                                                  |
| Member Ports | Zaznacz porty, z którymi hosty są połączone. Te porty będą statycznie przynależać do grupy multicastowej i nie będą tracić ważności. |

- 2) Kliknij **Create**.

## 2.1.5 Konfiguracja funkcji IGMP Accounting i IGMP Authentication

Funkcjami IGMP accounting i IGMP authentication możesz zarządzać stosownie do swoich potrzeb. IGMP accounting konfiguruje się globalnie, natomiast funkcja IGMP authentication włączana jest dla każdego portu osobno.

Aby korzystać z tych funkcji, konieczna jest konfiguracja serwera RADIUS dla przełącznika, którą można przeprowadzić przechodząc do SECURITY > AAA > RADIUS Config.

Wybierz z menu **L2 FEATURES > Multicast > IGMP Snooping > IGMP Authentication**, aby wyświetlić poniższą stronę.

Rys. 2-5 Konfiguracja IGMP Accounting i IGMP Authentication

**Global Config**

---

Accounting:  Enable Apply

**Port Config**

---

UNIT1

LAGS

|                                     | ID | Port   | IGMP Authentication | LAG |
|-------------------------------------|----|--------|---------------------|-----|
| <input checked="" type="checkbox"/> | 1  | 1/0/1  | Disabled            | --- |
| <input type="checkbox"/>            | 2  | 1/0/2  | Disabled            | --- |
| <input type="checkbox"/>            | 3  | 1/0/3  | Disabled            | --- |
| <input type="checkbox"/>            | 4  | 1/0/4  | Disabled            | --- |
| <input type="checkbox"/>            | 5  | 1/0/5  | Disabled            | --- |
| <input type="checkbox"/>            | 6  | 1/0/6  | Disabled            | --- |
| <input type="checkbox"/>            | 7  | 1/0/7  | Disabled            | --- |
| <input type="checkbox"/>            | 8  | 1/0/8  | Disabled            | --- |
| <input type="checkbox"/>            | 9  | 1/0/9  | Disabled            | --- |
| <input type="checkbox"/>            | 10 | 1/0/10 | Disabled            | --- |

Total: 10
1 entry selected.

Cancel
Apply

Wykonaj poniższe kroki, aby włączyć IGMP accounting:

- 1) W sekcji **Global Config** włącz globalnie IGMP Accounting.

---

Accounting Włącz lub wyłącz IGMP Accounting.

---

- 2) Kliknij **Apply**.

Wykonaj poniższe kroki, aby skonfigurować IGMP Authentication na portach:

- 1) W sekcji **Port Config** zaznacz porty i włącz IGMP Authentication.

---

IGMP Authentication Włącz lub wyłącz IGMP Authentication dla portu.

---

- 2) Kliknij **Apply**.

## 2.2 Przez CLI

### 2.2.1 Globalna konfiguracja IGMP Snooping

Wykonaj poniższe kroki, aby globalnie skonfigurować IGMP Snooping:

---

|        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Krok 1 | <b>configure</b><br>Uruchom tryb konfiguracji globalnej.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Krok 2 | <b>ip igmp snooping</b><br>Włącz globalnie IGMP Snooping.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Krok 3 | <b>ip igmp snooping version {v1   v2   v3}</b><br>Podaj wersję IGMP.<br><br>v1: Przełącznik działa w trybie IGMPv1 Snooping. Może przetwarzać wyłącznie otrzymane od hosta komunikaty IGMPv1. Komunikaty innych wersji są ignorowane.<br><br>v2: Przełącznik działa w trybie IGMPv2 Snooping. Może przetwarzać zarówno komunikaty IGMPv1, jak i IGMPv2, otrzymane od hosta. Komunikaty IGMPv3 są ignorowane.<br><br>v3: Przełącznik działa w trybie IGMPv3 Snooping. Może przetwarzać otrzymane od hosta komunikaty wszystkich wersji: IGMPv1, IGMPv2 oraz IGMPv3.                                                                                                                                                                                                                 |
| Krok 4 | <b>ip igmp snooping drop-unknown</b><br><br>(Opcjonalnie) Ustaw sposób, w jaki przełącznik ma przetwarzać strumienie multicastowe, które są przesyłane do nieznanymi grup multicastowych, wybierając "Discard" (odrzuć). Domyślnym ustawieniem jest Forward.<br><br>Nieznane grupy multicastowe to grupy niepasujące do żadnej z grup przedstawionych we wcześniejszych raportach przynależności IGMP, a zatem nie ma ich na tablicy przekierowań ruchu multicastowego przełącznika.<br><br><i>Uwaga:</i> IGMP Snooping i MLD Snooping współdzielą ustawienie Unknown Multicast Groups, dlatego konieczne jest upewnienie się, że funkcja MLD Snooping jest uruchomiona globalnie. Aby to zrobić, skorzystaj z polecenia <b>ipv6 mld snooping</b> w trybie konfiguracji globalnej. |
| Krok 5 | <b>ip igmp snooping header-validation</b><br><br>(Opcjonalnie) Włącz funkcję Header Validation.<br><br>Dla pakietów IGMP wartością TTL powinno być 1, pola ToS 0xC0, a opcji Router Alert 0x94040000. Pola, które muszą być uzupełnione, zależą od wersji IGMP. IGMPv1 wymaga jedynie pola TTL. IGMPv2 wymaga pól TTL oraz Router Alert. IGMPv3 wymaga natomiast pól TTL, ToS oraz Router Alert. Pakiety, które nie przejdą pomyślnie procesu weryfikacji zostaną odrzucone.                                                                                                                                                                                                                                                                                                       |
| Krok 6 | <b>show ip igmp snooping</b><br>Przejrzyj podstawową konfigurację IGMP Snooping.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Krok 7 | <b>end</b><br>Powróć do trybu uprzywilejowanego (privileged EXEC mode).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |

---

---

**Krok 8      `copy running-config startup-config`**

Zapisz ustawienia w pliku konfiguracyjnym.

---

Poniższy schemat przedstawia sposób globalnego uruchamiania IGMP Snooping i Header Validation, ustawiania wersji IGMP Snooping jako IGMPv3 oraz przetwarzania przez przełącznik strumieni multicastowych wysyłanych do nieznanymi grup multicastowych jako discard.

**Switch#configure****Switch(config)#ip igmp snooping****Switch(config)#ip igmp snooping version v3****Switch(config)#ipv6 mld snooping****Switch(config)#ip igmp snooping drop-unknown****Switch(config)#ip igmp snooping header-validation****Switch(config)#show ip igmp snooping**

IGMP Snooping           :Enable

IGMP Version            :V3

Unknown Multicast       :Discard

Header Validation        :Enable

...

**Switch(config)#end****Switch#copy running-config startup-config**

## 2.2.2 Konfiguracja IGMP Snooping dla VLAN-ów

Przed konfiguracją IGMP Snooping dla VLAN-ów, wybierz VLAN-y, do których przynależą porty routera i porty przełącznika. Szczegółowe informacje znajdziesz w rozdziale [Konfiguracja 802.1Q VLAN](#).

Przełącznik umożliwia konfigurację IGMP Snooping dla poszczególnych VLAN-ów. Po globalnym uruchomieniu IGMP Snooping konieczne jest także włączenie IGMP Snooping i skonfigurowanie odpowiednich parametrów VLAN-ów, do których przynależą porty routera i porty przełącznika.

Wykonaj poniższe kroki, aby skonfigurować IGMP Snooping dla VLAN-ów:

---

**Krok 1      `configure`**

Uruchom tryb konfiguracji globalnej.

---

**Krok 2** `ip igmp snooping vlan-config vlan-id-list mtime member-time`

Włącz IGMP Snooping dla określonych VLAN-ów i ustal czas utraty ważności portów dla VLAN-ów.

*vlan-id-list*: Podaj ID lub listę ID VLAN-u(-ów).

*member-time*: Podaj czas utraty ważności portów w określonych VLAN-ach. Prawidłowe wartości wahają się od 60 do 600 sekund. Domyślną wartością jest 260 sekund.

Gdy przełącznik otrzymuje z portu raport IGMP, od razu dodaje on ten port do listy portów przynależących do określonej grupy multicastowej. Pozyskane w ten sposób porty nazywane są portami dynamicznymi.

Jeżeli przełącznik nie otrzymuje z portu dynamicznego żadnych raportów IGMP dla określonej grupy multicastowej przed utratą ważności portu, usuwa on ten port z listy przekierowań ruchu multicastowego, ponieważ nie uznaje go już za port przynależący do określonej grupy multicastowej.

---

**Krok 3** `ip igmp snooping vlan-config vlan-id-list rtime router-time`

Podaj czas utraty ważności portów routera przynależących do VLAN-u.

*vlan-id-list*: Podaj ID lub listę ID VLAN-u(-ów).

*router-time*: Podaj czas utraty ważności portów routera w określonych VLAN-ach. Prawidłowe wartości wahają się od 60 do 600 sekund. Domyślną wartością jest 300 sekund.

Gdy przełącznik otrzymuje z portu komunikat z zapytaniem IGMP, dodaje on ten port do listy portów routera. Pozyskane w ten sposób porty routera nazywane są dynamicznymi portami routera.

Jeżeli przełącznik nie otrzymuje z portu dynamicznego routera żadnych komunikatów z zapytaniem IGMP przed utratą ważności portu, usuwa on ten port z listy portów routera, ponieważ nie uznaje go już za port routera.

---

**Krok 4** `ip igmp snooping vlan-config vlan-id-list ltime leave-time`

Podaj czas opuszczenia grupy dla VLAN-ów.

*vlan-id-list*: Podaj ID lub listę ID VLAN-u(-ów).

*leave-time*: Podaj czas opuszczania grupy dla VLAN-u(-ów). Prawidłowe wartości wahają się od 1 do 30 sekund. Domyślną wartością jest 1 sekunda.

Gdy przełącznik otrzymuje z portu komunikat o zamiarze opuszczenia grupy multicastowej, nie usuwa go od razu z grupy multicastowej, tylko czeka na określony Leave Time. Jeżeli w tym czasie przełącznik otrzyma komunikat z portu, nie zostanie on usunięty z grupy multicastowej. Wyjątkami są następujące sytuacje:

- Jeżeli port utraci ważność przed upływem Leave Time i żaden raport nie zostanie wysłany, port zostanie usunięty z grupy multicastowej po upływie Member Port Aging Time.
- Mechanizm Leave Time nie ma zastosowania, gdy włączona jest funkcja Fast Leave.

Podanie odpowiedniej wartości Leave Time pozwala uniknąć omyłkowego usuwania z grupy multicastowej innych hostów łączących się z tym samym portem przełącznika, podczas gdy tylko niektóre chcą opuścić grupę.

---



---

**Krok 5** **ip igmp snooping vlan-config *vlan-id-list* report-suppression**

(Opcjonalnie) Włącz lub wyłącz ograniczanie wysyłania raportów dla VLAN-ów. Domyślnie opcja jest wyłączona.

Przy włączonej opcji przełącznik przesyła urządzeniu odpytującemu tylko pierwszy raport IGMP dla każdej grupy multicastowej i hamuje przesył kolejnych raportów dla tych samych grup multicastowych w ramach jednego interwału zapytań. Pozwala to uniknąć wysyłania do IGMP querier zdublowanych komunikatów.

*vlan-id-list*: Podaj ID lub listę ID VLAN-u(-ów).

---

**Krok 6** **ip igmp snooping vlan-config *vlan-id-list* immediate-leave**

(Opcjonalnie) Włącz funkcję szybkiego przełączania dla VLAN-ów. IGMPv1 nie obsługuje Fast Leave.

Wyłączona funkcja Fast Leave oznacza, że gdy odbiorca wysła komunikat IGMP o opuszczeniu grupy multicastowej, przełącznik prześle ten komunikat do urządzenia warstwy 3 (querier).

Z punktu widzenia urządzenia odpytującego port łączący się z przełącznikiem jest portem przynależącym do odpowiedniej grupy multicastowej. Po otrzymaniu od przełącznika komunikatu leave, urządzenie odpytujące przesyła ustaloną liczbę zapytań (Last Member Query Count) dla określonych grup na tym porcie w ustalonym interwale czasowym (Last Member Query Interval), a następnie czeka na raporty dotyczące przynależności do grup IGMP. Jeżeli z przełącznikiem łączą się w tym czasie także inni odbiorcy, odpowiedzi na te zapytania prześlą przed wygaśnięciem Last Member Query Interval. Jeżeli żaden raport nie zostanie wysłany przed wygaśnięciem ostatniego zapytania, urządzenie odpytujące usunie port z listy przesyłu odpowiedniej grupy multicastowej.

Jeżeli z przełącznikiem łączą się także inni odbiorcy, ten, który wysła komunikat leave musi poczekać aż port z listy przesyłu przełącznika odpowiedniej grupy multicastowej utraci ważność (maksymalny czas oczekiwania zależy od Member Port Aging Time).

Przy włączonej dla VLAN-u opcji Fast Leave przełącznik usunie pozycję (Multicast Group, Port, VLAN) z tablicy przekierowań ruchu multicastowego przed przekazaniem komunikatu leave do urządzenia odpytującego. Pomaga to ograniczyć straty dostępnej przepustowości, ponieważ przełącznik zaprzestaje przesyłania strumieni multicastowych do VLAN-u portu od razu, gdy port otrzymuje z VLAN-u komunikat leave.

Przez funkcji Fast Leave dla VLAN-u jest zalecane tylko, gdy do tego VLAN-u przynależy tylko jeden odbiorca na każdym porcie VLAN-u.

*vlan-id-list*: Podaj ID lub listę ID VLAN-u(-ów).

---

**Krok 7** **ip igmp snooping vlan-config *vlan-id-list* rport interface { fastEthernet *port-list* | gigabitEthernet *port-list* | ten-gigabitEthernet *port-list* | port-channel *lag-list* }**

(Opcjonalnie) Wybierz jeden lub więcej portów, które mają być statycznymi portami routera dla VLAN-ów. Statyczne porty routera nie tracą ważności.

*vlan-id-list*: Podaj ID lub listę ID VLAN-u(-ów).

*port-list*: Numery lub lista portów Ethernet, które mają być statycznymi portami routera.

*lag-list*: ID lub lista grup agregacji łączy (LAG), które mają być statycznymi portami routera.

Krok 8 **ip igmp snooping vlan-config *vlan-id-list* router-ports-forbidden interface { fastEthernet *port-list* | gigabitEthernet *port-list* | ten-gigabitEthernet *port-list* | port-channel *lag-list* }**

Opcjonalnie) Wybierz porty, które nie będą mogły być portami routera dla VLAN-ów.

*vlan-id-list*: Podaj ID lub listę ID VLAN-u(-ów).

*port-list*: Numery lub lista portów Ethernet, które nie będą mogły być portami routera.

*lag-list*: ID lub lista LAG, które nie będą mogłyby być portami routera.

Krok 9 **ip igmp snooping vlan-config *vlan-id-list* querier**

(Opcjonalnie) Włącz IGMP Snooping Querier dla VLAN-u. Domyślnie funkcja jest wyłączona.

Włączona funkcja oznacza, że przełącznik pełni rolę IGMP Snooping Querier dla hostów należących do tego VLAN-u. Urządzenie odpytuje cyklicznie rozsyła zapytanie w sieci, aby uzyskać informacje o przynależności, a następnie, po otrzymaniu od hostów komunikatów leave, rozsyła zapytania do grup.

*vlan-id-list*: Podaj ID lub listę ID VLAN-u(-ów).

*Uwaga:*

Aby możliwe było włączenie IGMP Snooping Querier dla VLAN-u, funkcja IGMP Snooping powinna być uruchomiona zatówn globalnie, jak i dla VLAN-u.

Po włączeniu funkcji IGMP Snooping Querier, konieczne jest uzupełnienie odpowiednich parametrów, w tym Last Member Query Count, Last Member Query Interval, Maximum Response Time, Query Interval i General Query Source IP. Skorzystaj z poniższego polecenia w trybie konfiguracji globalnej, aby skonfigurować te parametry:

**ip igmp snooping vlan-config *vlan-id-list* querier { max-response-time *response-time* | query-interval *interval* | general-query source-ip *ip-addr* | last-member-query-count *num* | last-member-query-interval *interval* }**

*vlan-id-list*: Podaj ID lub listę ID VLAN-u(-ów).

*response-time*: Podaj maksymalny czas odpowiedzi hostów na zapytania ogólne. Prawidłowe wartości wahają się od 1 do 25 sekund, a wartością domyślną jest 10 sekund.

*query-interval interval*: Podaj interwał pomiędzy zapytaniami ogólnymi przesyłanymi przez przełącznik. Prawidłowe wartości wahają się od 10 do 300 sekund, a wartością domyślną jest 60 sekund.

*ip-addr*: Podaj źródłowy adres IP zapytań ogólnych wysyłanych przez przełącznik. Wartość powinna być adresem unicast. Domyślną wartością jest 0.0.0.0.

*num*: Podaj liczbę zapytań, które mają być przesłane bezpośrednio do grup. Włączona funkcja IGMP Snooping Querier oznacza, że gdy przełącznik otrzymuje komunikat leave IGMP, pozyskuje on z komunikatu adres grupy multicastowej, którą host chce opuścić. Następnie przełącznik wysyła określone zapytania bezpośrednio do tej grupy multicastowej na porcie odbierającym komunikaty leave. Jeżeli ustalona liczba zapytań zostanie wysłana bez odpowiedzi zwrotnej pod postacią komunikatu, przełącznik usunie adresy ruchu multicastowego z tablicy przekierowań ruchu multicastowego. Prawidłowe wartości wahają się od 1 do 5, a wartością domyślną jest 2.

*last-member-query-interval interval*: Podaj interwał wysyłania zapytań do określonych grup. Prawidłowe wartości wahają się od 1 do 5 sekund, a wartością domyślną jest 1 sekunda.

Krok 10 **show ip igmp snooping vlan *vlan-id***

Przejrzyj podstawową konfigurację IGMP Snooping dla wybranego VLAN-u.

---

Krok 11    **end**  
Powróć do trybu privileged EXEC.

---

Krok 12    **copy running-config startup-config**  
Zapisz ustawienia w pliku konfiguracyjnym.

---

Poniższy schemat przedstawia przykładowy sposób włączania IGMP Snooping dla VLAN 1, ustawiania czasu utraty ważności portu jako 300 sekund, czasu utraty ważności portu routera jako 320 sekund, a następnie włączania funkcji Fast Leave i Report Suppression dla VLAN-u:

**Switch#configure**

**Switch(config)#ip igmp snooping vlan-config 1 mtime 300**

**Switch(config)#ip igmp snooping vlan-config 1 rtime 320**

**Switch(config)#ip igmp snooping vlan-config 1 immediate-leave**

**Switch(config)#ip igmp snooping vlan-config 1 report-suppression**

**Switch(config)#show ip igmp snooping vlan 1**

Vlan Id: 1

Vlan IGMP Snooping Status: Enable

Fast Leave: Enable

Report Suppression: Enable

Router Time:320

Member Time: 300

Querier: Disable

...

**Switch(config)#end**

**Switch#copy running-config startup-config**

Poniższy schemat przedstawia przykładowy sposób włączania IGMP Snooping querier dla VLAN 1, ustawiania interwału wysyłania zapytań jako 100 sekund, maksymalnego czasu odpowiedzi jako 15 sekund, interwału last member query jako 2 seconds, wartości last member query count jako 3 i ogólnego źródłowego IP dla zapytań jako 192.168.0.5:

**Switch#configure**

**Switch(config)#ip igmp snooping vlan-config 1 querier**

**Switch(config)#ip igmp snooping vlan-config 1 querier query-interval 100**

**Switch(config)#ip igmp snooping vlan-config 1 querier max-response-time 15**

```

Switch(config)#ip igmp snooping vlan-config 1 querier last-member-query-interval 2
Switch(config)#ip igmp snooping vlan-config 1 querier last-member-query-count 3
Switch(config)#ip igmp snooping vlan-config 1 querier general-query source-
ip192.168.0.5

Switch(config)#show ip igmp snooping vlan 1

Vlan Id: 1

...

Querier:

Maximum Response Time: 15
Query Interval: 100
Last Member Query Interval: 2
Last Member Query Count: 3
General Query Source IP: 192.168.0.5

...

Switch(config)#end

Switch#copy running-config startup-config

```

### 2.2.3 Konfiguracja IGMP Snooping dla portów

Wykonaj poniższe kroki, aby skonfigurować IGMP Snooping dla portów

|        |                                                                                                                                                                                                                                                                                                                                                                     |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Krok 1 | <b>configure</b><br>Uruchom tryb konfiguracji globalnej.                                                                                                                                                                                                                                                                                                            |
| Krok 2 | <b>interface {fastEthernet <i>port</i>   range fastEthernet <i>port-list</i>   gigabitEthernet <i>port</i>   range gigabitEthernet <i>port-list</i>   ten-gigabitEthernet <i>port</i>   range ten-gigabitEthernet <i>port-list</i>} port-channel <i>port-channel-id</i>   range port-channel <i>port-channel-list</i>}</b><br>Uruchom tryb konfiguracji interfejsu. |
| Krok 3 | <b>ip igmp snooping</b><br>Włącz IGMP Snooping dla portu. Domyślnie funkcja jest włączona.                                                                                                                                                                                                                                                                          |

**Krok 4 ip igmp snooping immediate-leave**

(Opcjonalnie) Włącz Fast Leave na określonym porcie.

Funkcja Fast Leave może działać dla poszczególnych portów lub VLAN-ów. Włączenie funkcji dla poszczególnych portów oznacza, że przełącznik usunie port z odpowiedniej grupy multicastowej wszystkich VLAN-ów przed przestaniem komunikatu leave do urządzenia odpytującego.

Przez funkcji Fast Leave dla portu jest zalecane tylko, gdy do portu podłączony jest tylko jeden odbiorca. Więcej informacji o funkcji Fast Leave znajdziesz w rozdziale [2.1.2 Konfiguracja IGMP Snooping dla VLAN-ów](#).

**Krok 5 show ip igmp snooping interface [fastEthernet [ port-list ] | gigabitEthernet [ port-list ] | ten-gigabitEthernet [ port-list ] | port-channel [port-channel-list] ] basic-config**

Przejrzyj podstawową konfigurację IGMP Snooping poszczególnych lub wszystkich portów.

**Krok 6 end**

Powróć do trybu privileged EXEC.

**Krok 7 copy running-config startup-config**

Zapisz ustawienia w pliku konfiguracyjnym.

Poniższy schemat przedstawia przykładowy sposób włączania funkcji IGMP Snooping i Fast Leave dla portu 1/0/1-3:

```
Switch#configure
```

```
Switch(config)#interface range fastEthernet 1/0/1-3
```

```
Switch(config-if-range)#ip igmp snooping
```

```
Switch(config-if-range)#ip igmp snooping immediate-leave
```

```
Switch(config-if-range)#show ip igmp snooping interface gigabitEthernet 1/0/1-3
```

| Port    | IGMP-Snooping | Fast-Leave |
|---------|---------------|------------|
| -----   | -----         | -----      |
| Gi1/0/1 | enable        | enable     |
| Gi1/0/2 | enable        | enable     |
| Gi1/0/3 | enable        | enable     |

```
Switch(config-if-range)#end
```

```
Switch#copy running-config startup-config
```

## 2.2.4 Konfiguracja statycznego dołączania hostów do grup

Hosty lub porty warstwy 2 dołączają zwykle dynamicznie do grup multicastowych, ale możliwe jest także statyczne przyłączenie się hostów do grup.

Wykonaj poniższe kroki, aby skonfigurować statyczne dołączanie hostów do grup:

|        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Krok 1 | <b>configure</b><br>Uruchom tryb konfiguracji globalnej.                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Krok 2 | <b>ip igmp snooping vlan-config <i>vlan-id-list</i> static <i>ip</i> interface { <i>fastEthernet port-list</i>   <i>gigabitEthernet port-list</i>   <i>ten-gigabitEthernet port-list</i>   <i>port-channel lag-list</i> }</b><br><br><i>vlan-id-list</i> : Podaj ID lub listę ID VLAN-u(-ów).<br><i>ip</i> : Podaj adres IP grupy multicastowej, do której mają dołączyć hosty.<br><i>port-list</i> / <i>lag-list</i> : Zaznacz porty, z którymi hosty są połączone. Te porty będą statycznie przynależać do grupy. |
| Krok 3 | <b>show ip igmp snooping groups static</b><br>Przejrzyj statyczną konfigurację MLD Snooping.                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Krok 4 | <b>end</b><br>Powróć do trybu privileged EXEC.                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Krok 5 | <b>copy running-config startup-config</b><br>Zapisz ustawienia w pliku konfiguracyjnym.                                                                                                                                                                                                                                                                                                                                                                                                                             |

Poniższy schemat przedstawia przykładowy sposób konfiguracji statycznego dołączania portu 1/0/1-3 w sieci VLAN 2 do grupy multicastowej 239.1.2.3:

**Switch#configure**

**Switch(config)#ip igmp snooping vlan-config 2 static 239.1.2.3 interface gigabitEthernet 1/0/1-3**

**Switch(config)#show ip igmp snooping groups static**

| Multicast-ip | VLAN-id | Addr-type | Switch-port |
|--------------|---------|-----------|-------------|
| -----        | -----   | -----     | -----       |
| 239.1.2.3    | 2       | static    | Gi1/0/1-3   |

**Switch(config)#end**

**Switch#copy running-config startup-config**

## 2.2.5 Konfiguracja funkcji IGMP Accounting i IGMP Authentication

Funkcjami IGMP accounting i IGMP authentication możesz zarządzać stosownie do swoich potrzeb. IGMP accounting konfiguruje się globalnie, natomiast funkcja IGMP authentication włączana jest dla każdego portu osobno.

Aby korzystać z tych funkcji, konieczna jest konfiguracja serwera RADIUS dla przełącznika.

Wykonaj poniższe kroki, aby dodać serwer RADIUS i włączyć globalnie IGMP accounting:

|        |                                                          |
|--------|----------------------------------------------------------|
| Krok 1 | <b>configure</b><br>Uruchom tryb konfiguracji globalnej. |
|--------|----------------------------------------------------------|

- 
- Krok 2     **radius-server host *ip-address* [ **auth-port** *port-id* ] [ **acct-port** *port-id* ] [ **timeout** *time* ] [ **retransmit** *number* ] [ **nas-id** *nas-id* ] **key** { [ 0 ] *string* | 7 *encrypted-string* }**
- Dodaj serwer RADIUS i skonfiguruj odpowiednie parametry.
- host *ip-address***: Wprowadź adres IP serwera działającego z wykorzystaniem protokołu RADIUS.
- auth-port *port-id***: Określ port docelowy UDP na serwerze RADIUS dla żądań authentication. Wartością domyślną jest 1812.
- acct-port *port-id***: Określ port docelowy UDP na serwerze RADIUS dla żądań accounting. Wartością domyślną jest 1813. Parametr ten stosuje się zwykle z funkcją 802.1X.
- timeout *time***: Określ czas oczekiwania przełącznika na odpowiedź serwera przed ponownym wysłaniem żądania. Prawidłowa wartość musi mieścić się w przedziale 1 - 9 sekund. Wartością domyślną jest 5 sekund.
- retransmit *number***: Określ liczbę ponownie wysłanych żądań w przypadku braku odpowiedzi serwera. Prawidłowa wartość musi mieścić się w przedziale 1 - 3. Wartością domyślną jest 2.
- nas-id *nas-id***: Określ nazwę NAS (Network Access Server), która ma znajdować się w pakietach RADIUS w celach identyfikacyjnych. Nazwa ta musi zawierać od 1 do 31 znaków. Wartością domyślną jest adres MAC przełącznika. Zasadniczo NAS określa sam przełącznik.
- key { [ 0 ] *string* | 7 *encrypted-string* }**: Określ klucz dzielony. 0 i 7 oznaczają typy szyfrowania. 0 oznacza klucz nieszyfrowany. 7 wskazuje na klucz szyfrowany symetrycznie o stałej długości. Domyślnie wybranym typem jest 0. *string* to dzielony klucz przełącznika i serwera, który składa się maksymalnie z 31 znaków. *encrypted-string* to klucz symetryczny o stałej długości, który można skopiować z pliku konfiguracyjnego innego przełącznika. Konfigurowany tutaj klucz lub klucz szyfrowania wyświetlać się będzie w formie szyfrowanej.
- 
- Krok 3     **ip igmp snooping accounting**
- Włącz globalnie IGMP accounting.
- 
- Krok 4     **show ip igmp snooping**
- Pokaż podstawową konfigurację IGMP Snooping.
- 
- Krok 5     **end**
- Powróć do trybu privileged EXEC.
- 
- Krok 6     **copy running-config startup-config**
- Zapisz ustawienia w pliku konfiguracyjnym.
- 

Wykonaj poniższe kroki, aby włączyć IGMP authentication dla portów:

- 
- Krok 1     **configure**
- Uruchom tryb konfiguracji globalnej.
- 
- Krok 2     **interface {*fastEthernet port* | range *fastEthernet port-list* | *gigabitEthernet port* | range *gigabitEthernet port-list* | *ten-gigabitEthernet port* | range *ten-gigabitEthernet port-list*} **port-channel** *port-channel-id* | range **port-channel** *port-channel-list*}**
- Uruchom tryb konfiguracji interfejsu.
-

- 
- Krok 3     **ip igmp snooping authentication**  
Włącz IGMP Snooping authentication dla portu. Domyślnie funkcja jest włączona.
- 
- Krok 4     **show ip igmp snooping interface [fastEthernet [ *port-list* ] | gigabitEthernet [ *port-list* ] | ten-gigabitEthernet [ *port-list* ] | port-channel [*port-channel-list*] ] authentication**  
Pokaż podstawową konfigurację IGMP Snooping określonego portu lub wszystkich portów.
- 
- Krok 5     **end**  
Powróć do trybu privileged EXEC.
- 
- Krok 6     **copy running-config startup-config**  
Zapisz ustawienia w pliku konfiguracyjnym.
- 

Poniższy schemat przedstawia przykładowy sposób globalnego włączania funkcji IGMP accounting:

**Switch#configure**

**Switch(config)#ip igmp snooping accounting**

**Switch(config)#show ip igmp snooping**

...

Global Authentication Accounting: Enable

Enable Port: Gi1/0/1-28, Po1-14

Enable VLAN:

**Switch(config)#end**

**Switch#copy running-config startup-config**

Poniższy schemat przedstawia przykładowy sposób włączania funkcji IGMP authentication na porcie 1/0/1-3:

**Switch#configure**

**Switch(config)#interface range gigabitEthernet 1/0/1-3**

**Switch(config-if-range)#ip igmp snooping authentication**

**Switch(config-if-range)#show ip igmp snooping interface gigabitEthernet 1/0/1-3 authentication**



| Port    | IGMP-Authentication |
|---------|---------------------|
| -----   | -----               |
| Gi1/0/1 | enable              |
| Gi1/0/2 | enable              |
| Gi1/0/3 | enable              |

**Switch(config)#end**

**Switch#copy running-config startup-config**

# 3 Konfiguracja MLD Snooping

Wykonaj poniższe kroki, aby przeprowadzić konfigurację MLD Snooping:

- 1) Uruchom globalnie funkcję MLD Snooping i skonfiguruj parametry globalne.
- 2) Skonfiguruj MLD Snooping dla VLAN-ów.
- 3) Skonfiguruj MLD Snooping dla portów.
- 4) Skonfiguruj statyczne dołączanie hostów do grup (opcjonalnie).

## Uwaga:

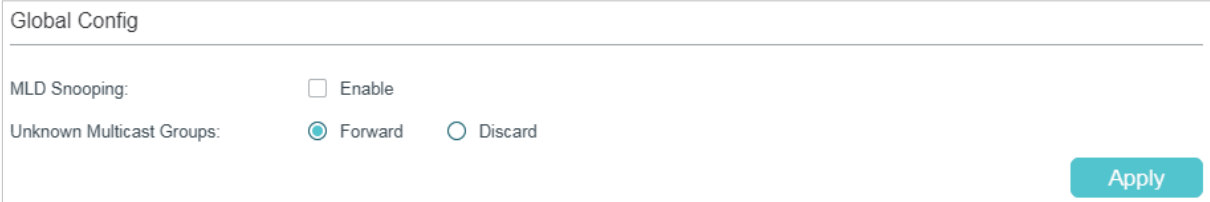
Funkcja MLD Snooping działa wyłącznie przy uruchomieniu globalnym - dla VLAN-u oraz odpowiednich portów.

## 3.1 Przez GUI

### 3.1.1 Konfiguracja globalna MLD Snooping

Wybierz z menu **L2 FEATURES > Multicast > MLD Snooping > Global Config**, aby wyświetlić poniższą stronę.

Rys. 3-1 Konfiguracja globalna MLD Snooping



Wykonaj poniższe kroki, aby skonfigurować globalnie MLD Snooping:

- 1) W sekcji **Global Config** włącz MLD Snooping i skonfiguruj globalnie funkcję Unknown Multicast Groups.

|                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|--------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| MLD Snooping             | Włącz lub wyłącz globalnie MLD Snooping.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Unknown Multicast Groups | <p>Zdecyduj w jaki sposób przełącznik ma przetwarzać dane, które są przesyłane do nieznanymi grup multicastowych, wybierając spośród "Forward" (przesyłaj) lub "Discard" (odrzuć). Domyślnym ustawieniem jest Forward.</p> <p>Nieznane grupy multicastowe to grupy niepasujące do żadnej z grup przedstawionych we wcześniejszych raportach przynależności IGMP, a zatem nie ma ich na tablicy przekierowań ruchu multicastowego przełącznika.</p> <p><i>Uwaga:</i> IGMP Snooping i MLD Snooping współdzielą ustawienie Unknown Multicast Groups, dlatego konieczne jest przejście w tym samym czasie do strony <b>L2 FEATURES &gt; Multicast &gt; IGMP Snooping &gt; Global Config</b> i globalne uruchomienie funkcji IGMP Snooping.</p> |

- 2) Kliknij **Apply**.

### 3.1.2 Konfiguracja MLD Snooping dla VLAN-ów

Przed konfiguracją MLD Snooping dla VLAN-ów, wybierz VLAN-y, do których przynależą porty routera i porty przełącznika. Szczegółowe informacje znajdziesz w rozdziale *Konfiguracja 802.1Q VLAN*.

Przełącznik umożliwia konfigurację MLD Snooping dla poszczególnych VLAN-ów. Po globalnym uruchomieniu IGMP Snooping konieczne jest także włączenie IGMP Snooping i skonfigurowanie odpowiednich parametrów VLAN-ów, do których przynależą porty routera i porty przełącznika.

Wybierz z menu **L2 FEATURES > Multicast > MLD Snooping > Global Config** i kliknij  przy wybranej pozycji VLAN-u w sekcji **MLD VLAN Config**, aby wyświetlić poniższą stronę.

Rys. 3-2 Konfiguracja MLD Snooping dla VLAN-u

Configure MLD Snooping for VLAN

VLAN ID:

MLD Snooping Status:  Enable

Fast Leave:  Enable

Report Suppression:  Forward  Discard

Member Port Aging Time:  seconds (60-600)

Router Port Aging Time:  seconds (60-600)

Leave Time:  seconds (1-30)

MLD Snooping Querier:  Enable

Static Router Ports

Wykonaj poniższe kroki, aby skonfigurować MLD Snooping dla określonych VLAN-ów:

1) Włącz MLD Snooping dla VLAN-u i skonfiguruj odpowiednie parametry.

|                     |                                           |
|---------------------|-------------------------------------------|
| VLAN ID             | Identyfikator VLAN-u.                     |
| MLD Snooping Status | Włącz lub wyłącz MLD Snooping dla VLAN-u. |

---

|                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Fast Leave             | <p>Włącz lub wyłącz funkcję szybkiego przełączania dla VLAN-u. IGMPv1 nie obsługuje Fast Leave.</p> <p>Wyłączona funkcja Fast Leave oznacza, że gdy odbiorca wysła komunikat leave IGMP, przełącznik prześle ten komunikat do urządzenia warstwy 3 (querier).</p> <p>Z punktu widzenia urządzenia odpytującego port łączący się z przełącznikiem jest portem przynależącym do odpowiedniej grupy multicastowej. Po otrzymaniu od przełącznika komunikatu done, urządzenie odpytujące przesyła ustaloną liczbę zapytań (Last Listener Query Count) dla określonych adresów ruchu multicastowego (MASQs) na tym porcie w ustalonym interwale czasowym (Last Listener Query Interval), a następnie czeka na raporty MLD. Jeżeli z przełącznikiem łączą się w tym czasie także inni odbiorcy, odpowiedzi na zapytania MASQs prześlą przed upływem Last Listener Query Interval. Jeżeli żaden raport nie zostanie wysłany przed wygaśnięciem ostatniego zapytania, urządzenie odpytujące usunie port z listy przekierowań odpowiedniej grupy multicastowej.</p> <p>Jeżeli z przełącznikiem łączą się także inni odbiorcy, ten, który wysła komunikat done musi poczekać aż port z listy przekierowań przełącznika odpowiedniej grupy multicastowej utraci ważność (maksymalny czas oczekiwania zależy od Member Port Aging Time).</p> <p>Przy włączonej dla VLAN-u opcji Fast Leave przełącznik usunie pozycję (Multicast Group, Port, VLAN) z tablicy przekierowań ruchu multicastowego przed przekazaniem komunikatu done do urządzenia odpytującego. Pomaga to ograniczyć straty dostępnej przepustowości, ponieważ przełącznik zaprzestaje przesyłania strumieni multicastowych do VLAN-u portu od razu, gdy port otrzymuje z VLAN-u komunikat done.</p> |
| Report Suppression     | <p>Włącz ograniczanie wysyłania raportów dla VLAN-u.</p> <p>Przy włączonej opcji przełącznik przesyła urządzeniu odpytującemu tylko pierwszy raport MLD dla każdej grupy multicastowej i hamuje przesył kolejnych raportów dla tych samych grup multicastowych w ramach jednego interwału zapytań. Pozwala to uniknąć wysyłania do MLD querier zdublowanych komunikatów.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Member Port Aging Time | <p>Podaj czas utraty ważności portów przynależących do VLAN-u.</p> <p>Gdy przełącznik otrzymuje z portu raport MLD, od razu dodaje on ten port do listy portów przynależących do określonej grupy multicastowej. Pozyskane w ten sposób porty nazywane są portami dynamicznymi.</p> <p>Jeżeli przełącznik nie otrzymuje z portu dynamicznego żadnych raportów MLD dla określonej grupy multicastowej przed utratą ważności portu, usuwa on ten port z listy przekierowań ruchu multicastowego, ponieważ nie uznaje go już za port przynależący do określonej grupy multicastowej.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Router Port Aging Time | <p>Podaj czas utraty ważności portów routera przynależących do VLAN-u.</p> <p>Gdy przełącznik otrzymuje z portu komunikat z zapytaniem MLD, dodaje on ten port do listy portów routera. Pozyskane w ten sposób porty routera nazywane są dynamicznymi portami routera.</p> <p>Jeżeli przełącznik nie otrzymuje z portu dynamicznego routera żadnych komunikatów z zapytaniem MLD przed utratą ważności portu, usuwa on ten port z listy portów routera, ponieważ nie uznaje go już za port routera.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |

---

|                              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Leave Time                   | <p>Podaj czas opuszczenia grupy dla VLAN-u.</p> <p>Gdy przełącznik otrzymuje z portu komunikat o zamiarze opuszczenia grupy multicastowej, nie usuwa go od razu z grupy multicastowej, tylko czeka na określony Leave Time. Jeżeli w tym czasie przełącznik otrzyma komunikat z portu, nie zostanie on usunięty z grupy multicastowej. Wyjątkami są następujące sytuacje:</p> <ul style="list-style-type: none"> <li>• Jeżeli port utraci ważność przed upływem Leave Time i żaden raport nie zostanie wysłany, port zostanie usunięty z grupy multicastowej po upływie Member Port Aging Time.</li> <li>• Mechanizm Leave Time nie ma zastosowania, gdy włączona jest funkcja Fast Leave.</li> </ul> <p>Podanie odpowiedniej wartości Leave Time pozwala uniknąć omyłkowego usuwania z grupy multicastowej innych hostów łączących się z tym samym portem przełącznika, podczas gdy tylko niektóre chcą opuścić grupę.</p> |
| MLD Snooping Querier         | <p>Włącz lub wyłącz funkcję MLD Snooping Querier dla VLAN-u.</p> <p>Włączona funkcja oznacza, że przełącznik pełni rolę MLD Snooping Querier dla hostów należących do tego VLAN-u. Urządzenie odpytuje cyklicznie rozsyła zapytanie w sieci, aby uzyskać informacje o przynależności, a następnie, po otrzymaniu od hostów komunikatów done, rozsyła zapytania MASQs.</p> <p><i>Uwaga:</i></p> <p>Aby możliwe było włączenie MLD Snooping Querier dla VLAN-u, funkcja MLD Snooping powinna być uruchomiona zatrwno globalnie, jak i dla VLAN-u.</p>                                                                                                                                                                                                                                                                                                                                                                         |
| Query Interval               | <p>Gdy włączysz funkcję MLD Snooping Querier, podaj interwał wysyłania przez przełącznik zapytań ogólnych.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Maximum Response Time        | <p>Gdy włączysz funkcję MLD Snooping Querier, podaj maksymalny czas odpowiedzi hostów na zapytania ogólne.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Last Listener Query Interval | <p>Włączona funkcja MLD Snooping Querier oznacza, że gdy przełącznik otrzymuje komunikat done, pozyskuje on z komunikatu adres grupy multicastowej, którą host chce opuścić. Następnie przełącznik wysyła zapytania MASQs bezpośrednio do tej grupy multicastowej na porcie odbierającym komunikaty done. Ten parametr jest wartością interwału pomiędzy przesyłanymi zapytaniami MASQs.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Last Listener Query Count    | <p>Gdy włączysz funkcję MLD Snooping Querier, podaj liczbę zapytań MASQs, które mają być przesłane. Jeżeli ustalona liczba zapytań zostanie wysłana, ale w odpowiedzi żaden raport nie zostanie przesłany, przełącznik usunie adres tego ruchu multicastowego z listy przekierowań ruchu multicastowego.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| General Query Source IP      | <p>Gdy włączysz funkcję MLD Snooping Querier, podaj źródłowy adres IPv6 zapytań ogólnych, wysyłanych przez przełącznik. Wartość powinna być adresem unicast.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Static Router Ports          | <p>Wybierz jeden lub więcej portów, które mają być statycznymi portami routera w sieci VLAN. Statyczne porty routera nie tracą ważności.</p> <p>Strumienie multicastowe i pakiety MLD będą przesyłane na statycznych portach routera do wszystkich grup tego VLAN-u. Strumienie multicastowe i pakiety MLD grup, do których przynależą porty dynamiczne routera, będą przesyłane na odpowiednich dynamicznych portach routera.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |

Forbidden  
Router Ports

Wybierz porty, które nie będą mogły być portami routera w sieci VLAN.

2) Kliknij **Save**.

### 3.1.3 Konfiguracja MLD Snooping dla portów

Wybierz z menu L2 FEATURES > Multicast > MLD Snooping > Port Config, aby wyświetlić poniższą stronę.

Rys. 3-3 Konfiguracja MLD Snooping dla portów

Port Config

---

UNIT1

LAGS

| <input type="checkbox"/>            | Port   | MLD Snooping | Fast Leave | LAG |
|-------------------------------------|--------|--------------|------------|-----|
| <input checked="" type="checkbox"/> | 1/0/1  | Enabled      | Disabled   | --- |
| <input type="checkbox"/>            | 1/0/2  | Enabled      | Disabled   | --- |
| <input type="checkbox"/>            | 1/0/3  | Enabled      | Disabled   | --- |
| <input type="checkbox"/>            | 1/0/4  | Enabled      | Disabled   | --- |
| <input type="checkbox"/>            | 1/0/5  | Enabled      | Disabled   | --- |
| <input type="checkbox"/>            | 1/0/6  | Enabled      | Disabled   | --- |
| <input type="checkbox"/>            | 1/0/7  | Enabled      | Disabled   | --- |
| <input type="checkbox"/>            | 1/0/8  | Enabled      | Disabled   | --- |
| <input type="checkbox"/>            | 1/0/9  | Enabled      | Disabled   | --- |
| <input type="checkbox"/>            | 1/0/10 | Enabled      | Disabled   | --- |

Total: 10
1 entry selected.

Cancel
Apply

Wykonaj poniższe kroki, aby skonfigurować MLD Snooping dla portów:

1) Włącz MLD Snooping dla portu i włącz Fast Leave, jeżeli z portem połączony jest tylko jeden odbiorca.

**MLD Snooping** Włącz lub wyłącz MLD Snooping dla portu.

**Fast Leave** Włącz lub wyłącz Fast Leave na porcie.

Funkcja Fast Leave może działać dla poszczególnych portów lub VLAN-ów. Włączenie funkcji dla poszczególnych portów oznacza, że przełącznik usunie port z odpowiedniej grupy multicastowej wszystkich VLAN-ów przed przesłaniem komunikatu done do urządzenia odpytującego.

Przez funkcji Fast Leave dla portu jest zalecane tylko, gdy do portu podłączony jest tylko jeden odbiorca. Więcej informacji o funkcji Fast Leave znajdziesz w rozdziale [3.1.2 Konfiguracja MLD Snooping dla VLAN-ów](#).

**LAG** Grupa agregacji łączy, do której należy port.

2) Kliknij **Apply**.

### 3.1.4 Konfiguracja statycznego dołączania hostów do grup

Hosty lub porty warstwy 2 dołączają zwykle dynamicznie do grup multicastowych, ale możliwe jest także statyczne przyłączenie się hostów do grup.

Wybierz z menu **L2 FEATURES > Multicast > MLD Snooping > Static Group Config** i kliknij **+ Add**, aby wyświetlić poniższą stronę.

Rys. 3-4 Konfiguracja statycznego dołączania hostów do grup

Wykonaj poniższe kroki, aby skonfigurować statyczne dołączanie hostów do grup:

- 1) Podaj adres IPv6 i VLAN ID ruchu multicastowego. Zaznacz porty, które mają statycznie przynależeć do grupy multicastowej.

|              |                                                                                                                                      |
|--------------|--------------------------------------------------------------------------------------------------------------------------------------|
| Multicast IP | Podaj adres IPv6 grupy multicastowej, do której mają dołączyć hosty.                                                                 |
| VLAN ID      | Określ VLAN hostów.                                                                                                                  |
| Member Ports | Zaznacz porty, z którymi hosty są połączone. Te porty będą statycznie przynależeć do grupy multicastowej i nie będą tracić ważności. |

- 2) Kliknij **Create**.

## 3.2 Przez CLI

### 3.2.1 Globalna konfiguracja MLD Snooping

Wykonaj poniższe kroki, aby globalnie skonfigurować MLD Snooping:

|        |                                                          |
|--------|----------------------------------------------------------|
| Krok 1 | <b>configure</b><br>Uruchom tryb konfiguracji globalnej. |
|--------|----------------------------------------------------------|

---

|        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Krok 2 | <p><b>ipv6 mld snooping</b></p> <p>Włącz globalnie MLD Snooping.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Krok 3 | <p><b>ipv6 mld snooping drop-unknown</b></p> <p>(Opcjonalnie) Ustaw sposób, w jaki przełącznik ma przetwarzać strumienie multicastowe, które są przesyłane do nieznanymi grup, wybierając Discard. Domyślnym ustawieniem jest Forward.</p> <p>Nieznane grupy multicastowe to grupy niepasujące do żadnej z grup przedstawionych we wcześniejszych raportach przynależności MLD, a zatem nie ma ich na tablicy przekierowań ruchu multicastowego przełącznika.</p> <p><i>Uwaga:</i> IGMP Snooping i MLD Snooping współdzielą ustawienie Unknown Multicast Groups, dlatego konieczne jest upewnienie się, że funkcja IGMP Snooping jest uruchomiona globalnie. Aby to zrobić, skorzystaj z polecenia <b>ip igmp snooping</b> w trybie konfiguracji globalnej.</p> |
| Krok 4 | <p><b>show ipv6 mld snooping</b></p> <p>Pokaż podstawową konfigurację IGMP Snooping.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Krok 5 | <p><b>end</b></p> <p>Powróć do trybu privileged EXEC.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Krok 6 | <p><b>copy running-config startup-config</b></p> <p>Zapisz ustawienia w pliku konfiguracyjnym.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |

---

Poniższy schemat przedstawia przykładowy sposób globalnego włączania MLD Snooping oraz przetwarzania przez przełącznik strumieni multicastowych wysyłanych do nieznanymi grup multicastowych jako discard.

**Switch#configure**

**Switch(config)#ipv6 mld snooping**

**Switch(config)#ipv6 mld snooping**

**Switch(config)#ipv6 mld snooping drop-unknown**

**Switch(config)#show ipv6 mld snooping**

MLD Snooping                   :Enable

Unknown Multicast            :Discard

...

**Switch(config)#end**

**Switch#copy running-config startup-config**

### 3.2.2 Konfiguracja MLD Snooping dla VLAN-ów

Przed konfiguracją MLD Snooping dla VLAN-ów, wybierz VLAN-y, do których przynależą porty routera i porty przełącznika. Szczegółowe informacje znajdziesz w części *Konfiguracja 802.1Q VLAN*.

Przełącznik umożliwia konfigurację MLD Snooping dla poszczególnych VLAN-ów. Po globalnym uruchomieniu MLD Snooping konieczne jest także włączenie IGMP Snooping i



skonfigurowanie odpowiednich parametrów VLAN-ów, do których przynależą porty routera i porty przełącznika.

Wykonaj poniższe kroki, aby skonfigurować MLD Snooping dla VLAN-ów:

---

|        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Krok 1 | <b>configure</b><br>Uruchom tryb konfiguracji globalnej.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Krok 2 | <b>ipv6 mld snooping vlan-config <i>vlan-id-list</i> mtime <i>member-time</i></b><br>Włącz MLD Snooping dla określonych VLAN-ów i ustal czas utraty ważności portów dla VLAN-ów.<br><i>vlan-id-list</i> : Podaj ID lub listę ID VLAN-u(-ów).<br><i>member-time</i> : Podaj czas utraty ważności portów w określonych VLAN-ach. Prawidłowe wartości wahają się od 60 do 600 sekund. Domyślną wartością jest 260 sekund.<br>Gdy przełącznik otrzymuje z portu raport MLD, od razu dodaje on ten port do listy portów przynależących do określonej grupy multicastowej. Pozyskane w ten sposób porty nazywane są portami dynamicznymi.<br><br>Jeżeli przełącznik nie otrzymuje z portu dynamicznego żadnych raportów MLD dla określonej grupy multicastowej przed utratą ważności portu, usuwa on ten port z listy przekierowań ruchu multicastowego, ponieważ nie uznaje go już za port przynależący do określonej grupy.                                                                                                                                                                                                                                                                                           |
| Krok 3 | <b>ipv6 mld snooping vlan-config <i>vlan-id-list</i> rtime <i>router-time</i></b><br>Podaj czas utraty ważności portów routera przynależących do VLAN-u.<br><i>vlan-id-list</i> : Podaj ID lub listę ID VLAN-u(-ów).<br><i>router-time</i> : Podaj czas utraty ważności portów routera w określonych VLAN-ach. Prawidłowe wartości wahają się od 60 do 600 sekund. Domyślną wartością jest 300 sekund.<br>Gdy przełącznik otrzymuje z portu komunikat z zapytaniem MLD, dodaje on ten port do listy portów routera. Pozyskane w ten sposób porty routera nazywane są dynamicznymi portami routera.<br><br>Jeżeli przełącznik nie otrzymuje z portu dynamicznego routera żadnych komunikatów z zapytaniem MLD przed utratą ważności portu, usuwa on ten port z listy portów routera, ponieważ nie uznaje go już za port routera.                                                                                                                                                                                                                                                                                                                                                                                   |
| Krok 4 | <b>ipv6 mld snooping vlan-config <i>vlan-id-list</i> ltime <i>leave-time</i></b><br>Podaj czas opuszczenia grupy dla VLAN-ów.<br><i>vlan-id-list</i> : Podaj ID lub listę ID VLAN-u(-ów).<br><i>leave-time</i> : Podaj czas opuszczania grupy dla VLAN-u(-ów). Prawidłowe wartości wahają się od 1 do 30 sekund. Domyślną wartością jest 1 sekunda.<br>Gdy przełącznik otrzymuje z portu komunikat o zamiarze opuszczenia grupy multicastowej, nie usuwa go od razu z grupy multicastowej, tylko czeka na określony Leave Time. Jeżeli w tym czasie przełącznik otrzyma komunikat z portu, nie zostanie on usunięty z grupy multicastowej. Wyjątkami są następujące sytuacje: <ul style="list-style-type: none"><li>• Jeżeli port utraci ważność przed upływem Leave Time i żaden raport nie zostanie wysłany, port zostanie usunięty z grupy multicastowej po upływie Member Port Aging Time.</li><li>• Mechanizm Leave Time nie ma zastosowania, gdy włączona jest funkcja Fast Leave.</li></ul> Podanie odpowiedniej wartości Leave Time pozwala uniknąć omyłkowego usuwania z grupy multicastowej innych hostów łączących się z tym samym portem przełącznika, podczas gdy tylko niektóre chcą opuścić grupę. |

---

---

**Krok 5** **ipv6 mld snooping vlan-config *vlan-id-list* report-suppression**

(Opcjonalnie) Włącz lub wyłącz ograniczanie wysyłania raportów dla VLAN-ów. Domyślnie opcja jest wyłączona.

Przy włączonej opcji przełącznik przesyła urządzeniu odpytującemu tylko pierwszy raport MLD dla każdej grupy multicastowej i hamuje przesył kolejnych raportów dla tych samych grup multicastowych w ramach jednego interwału zapytań. Pozwala to uniknąć wysyłania do MLD querier zdublowanych komunikatów.

*vlan-id-list*: Podaj ID lub listę ID VLAN-u(-ów).

---

**Krok 6** **ipv6 mld snooping vlan-config *vlan-id-list* immediate-leave**

(Opcjonalnie) Włącz funkcję szybkiego przełączania dla VLAN-ów. Domyślnie funkcja jest wyłączona.

Wyłączona funkcja Fast Leave oznacza, że gdy odbiorca wysyła komunikat done MLD (równoważny komunikatowi leave IGMP), przełącznik prześle ten komunikat do urządzenia warstwy 3 (querier).

Z punktu widzenia urządzenia odpytującego port łączący się z przełącznikiem jest portem przynależącym do odpowiedniej grupy multicastowej. Po otrzymaniu od przełącznika komunikatu done, urządzenie odpytujące przesyła ustaloną liczbę zapytań (Last Listener Query Count) dla określonych adresów ruchu multicastowego (MASQs) na tym porcie w ustalonym interwale czasowym (Last Listener Query Interval), a następnie czeka na raporty MLD. Jeżeli z przełącznikiem łączą się w tym czasie także inni odbiorcy, odpowiedzi na zapytania MASQs prześlą przed upływem Last Listener Query Interval. Jeżeli żaden raport nie zostanie wysłany przed wygaśnięciem ostatniego zapytania, urządzenie odpytujące usunie port z listy przekierowań odpowiedniej grupy multicastowej.

Jeżeli z przełącznikiem łączą się także inni odbiorcy, ten, który wysyła komunikat done musi poczekać aż port z listy przekierowań przełącznika odpowiedniej grupy multicastowej utraci ważność (maksymalny czas oczekiwania zależy od Member Port Aging Time).

Przy włączonej dla VLAN-u opcji Fast Leave przełącznik usunie pozycję (Multicast Group, Port, VLAN) z tablicy przekierowań ruchu multicastowego przed przekazaniem komunikatu done do urządzenia odpytującego. Pomaga to ograniczyć straty dostępnej przepustowości, ponieważ przełącznik zaprzestaje przesyłania strumieni multicastowych do VLAN-u portu od razu, gdy port otrzymuje z VLAN-u komunikat done.

*vlan-id-list*: Podaj ID lub listę ID VLAN-u(-ów).

---

**Krok 7** **ipv6 mld snooping vlan-config *vlan-id-list* rport interface { fastEthernet *port-list* | gigabitEthernet *port-list* | ten-gigabitEthernet *port-list* | port-channel *lag-list* }**

(Opcjonalnie) Wybierz jeden lub więcej portów, które mają być statycznymi portami routera dla VLAN-ów. Statyczne porty routera nie tracą ważności.

*vlan-id-list*: Podaj ID lub listę ID VLAN-u(-ów).

*port-list*: Numery lub lista portów Ethernet, które mają być statycznymi portami routera.

*lag-list*: ID lub lista grup agregacji łączy (LAG), które mają być statycznymi portami routera.

---

- 
- Krok 8 **ipv6 mld snooping vlan-config *vlan-id-list* router-ports-forbidden interface { fastEthernet *port-list* | gigabitEthernet *port-list* | ten-gigabitEthernet *port-list* | port-channel *lag-list* }**
- (Opcjonalnie) Wybierz porty, które nie będą mogły być portami routera dla VLAN-ów.
- vlan-id-list*: Podaj ID lub listę ID VLAN-u(-ów).
- port-list*: Numery lub lista portów Ethernet, które nie będą mogłyby być portami routera.
- lag-list*: ID lub lista LAG, które nie będą mogłyby być portami routera.
- 
- Krok 9 **ipv6 mld snooping vlan-config *vlan-id-list* querier**
- (Opcjonalnie) Włącz funkcję MLD Snooping Querier dla VLAN-u. Domyślnie funkcja jest wyłączona.
- Włączona funkcja oznacza, że przełącznik pełni rolę MLD Snooping Querier dla hostów należących do tego VLAN-u. Urządzenie odpytuje cyklicznie rozsyła zapytanie w sieci, aby uzyskać informacje o przynależności, a następnie, po otrzymaniu od hostów komunikatów done, rozsyła zapytania MASQs.
- vlan-id-list*: Podaj ID lub listę ID VLAN-u(-ów).
- Uwaga*:
- Aby możliwe było włączenie MLD Snooping Querier dla VLAN-u, funkcja MLD Snooping powinna być uruchomiona zarówno globalnie, jak i dla VLAN-u.
- Po włączeniu funkcji MLD Snooping Querier, konieczne jest uzupełnienie odpowiednich parametrów, w tym Last Member Query Count, Last Member Query Interval, Maximum Response Time, Query Interval i General Query Source IP. Skorzystaj z poniższego polecenia w trybie konfiguracji globalnej, aby skonfigurować te parametry:
- ipv6 mld snooping vlan-config *vlan-id-list* querier { max-response-time *response-time* | query-interval *interval* | general-query source-ip *ip-addr* | last-listener-query-count *num* | last-listener-query-interval *interval* }**
- vlan-id-list*: Podaj ID lub listę ID VLAN-u(-ów).
- response-time*: Podaj maksymalny czas odpowiedzi hostów na zapytania ogólne.
- query-interval *interval***: Podaj interwał pomiędzy zapytaniami ogólnymi przesyłanymi przez przełącznik.
- ip-addr*: Podaj źródłowy adres IP zapytań ogólnych wysyłanych przez przełącznik. Wartość powinna być adresem unicast.
- num*: Podaj liczbę zapytań, które mają być przesłane bezpośrednio do grup. Włączona funkcja MLD Snooping Querier oznacza, że gdy przełącznik otrzymuje komunikat done, pozyskuje on z komunikatu adres grupy multicastowej, którą host chce opuścić. Następnie przełącznik wysyła zapytania MASQs bezpośrednio do tej grupy multicastowej na porcie odbierającym komunikaty done. Jeżeli ustalona liczba zapytań MASQs zostanie wysłana bez odpowiedzi zwrotnej pod postacią komunikatu, przełącznik usunie adresy ruchu multicastowego z tablicy przekierowań ruchu multicastowego.
- last-listener-query-interval *interval***: Podaj interwał wysyłania zapytań MASQs.
- 
- Krok 10 **show ipv6 mld snooping vlan *vlan-id***
- Przejrzyj podstawową konfigurację MLD Snooping dla wybranego VLAN-u.
- 
- Krok 11 **end**
- Powróć do trybu privileged EXEC.
-

**Krok 12    copy running-config startup-config**

Zapisz ustawienia w pliku konfiguracyjnym.

Poniższy schemat przedstawia przykładowy sposób włączania MLD Snooping dla VLAN 1, ustawiania czasu utraty ważności portu jako 300 sekund, czasu utraty ważności portu routera jako 320 sekund, a następnie włączania funkcji Fast Leave i Report Suppression dla VLAN-u:

**Switch#configure****Switch(config)#ipv6 mld snooping vlan-config 1 mtime 300****Switch(config)#ipv6 mld snooping vlan-config 1 rtime 320****Switch(config)#ipv6 mld snooping vlan-config 1 immediate-leave****Switch(config)#ipv6 mld snooping vlan-config 1 report-suppression****Switch(config)#show ipv6 mld snooping vlan 1**

Vlan Id: 1

Vlan MLD Snooping Status: Enable

Fast Leave: Enable

Report Suppression: Enable

Router Time: Enable

Member Time: Enable

Querier: Disable

...

**Switch(config)#end****Switch#copy running-config startup-config**

Poniższy schemat przedstawia przykładowy sposób włączania MLD Snooping querier dla VLAN 1, ustawiania interwału wysyłania zapytań jako 100 sekund, maksymalnego czasu odpowiedzi jako 15 sekund, interwału last listener query jako 2 seconds, wartości last member query count jako 3 i ogólnego źródłowego IP dla zapytań jako FE80::1:

**Switch#configure****Switch(config)#ipv6 mld snooping vlan-config 1 querier****Switch(config)#ipv6 mld snooping vlan-config 1 querier query-interval 100****Switch(config)#ipv6 mld snooping vlan-config 1 querier max-response-time 15****Switch(config)#ipv6 mld snooping vlan-config 1 querier last-listener-query-interval 2****Switch(config)#ipv6 mld snooping vlan-config 1 querier last-listener-query-count 3**

```
Switch(config)#ipv6 mld snooping vlan-config 1 querier general-query source-ip FE80::1
```

```
Switch(config)#show ipv6 mld snooping vlan 1
```

```
Vlan Id: 1
```

```
...
```

```
Querier: Enable
Maximum Response Time: 15
Query Interval: 100
Last Member Query Interval: 2
Last Member Query Count: 3
General Query Source IP: fe80::1
```

```
...
```

```
Switch(config)#end
```

```
Switch#copy running-config startup-config
```

### 3.2.3 Konfiguracja MLD Snooping dla portów

Wykonaj poniższe kroki, aby skonfigurować MLD Snooping dla portów:

|        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Krok 1 | <b>configure</b><br>Uruchom tryb konfiguracji globalnej.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Krok 2 | <b>interface {fastEthernet <i>port</i>   range fastEthernet <i>port-list</i>   gigabitEthernet <i>port</i>   range gigabitEthernet <i>port-list</i>   ten-gigabitEthernet <i>port</i>   range ten-gigabitEthernet <i>port-list</i>} port-channel <i>port-channel-id</i>   range port-channel <i>port-channel-list</i>}</b><br>Uruchom tryb konfiguracji interfejsu.                                                                                                                                                                                                                                                      |
| Krok 3 | <b>ipv6 mld snooping</b><br>Włącz MLD Snooping dla portu. Domyślnie funkcja jest włączona.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Krok 4 | <b>ipv6 mld snooping immediate-leave</b><br>(Opcjonalnie) Włącz Fast Leave na określonym porcie.<br>Funkcja Fast Leave może działać dla poszczególnych portów lub VLAN-ów. Włączenie funkcji dla poszczególnych portów oznacza, że przełącznik usunie port z odpowiedniej grupy multicastowej wszystkich VLAN-ów przed przestaniem komunikatu done do urządzenia odpytującego.<br>Przez funkcji Fast Leave dla portu jest zalecane tylko, gdy do portu podłączony jest tylko jeden odbiorca. Więcej informacji o funkcji Fast Leave znajdziesz w rozdziale <a href="#">3.1.2 Konfiguracja MLD Snooping dla VLAN-ów</a> . |

Krok 5 **show ipv6 mld snooping interface [fastEthernet [ *port-list* ] | gigabitEthernet [ *port-list*] | ten-gigabitEthernet [ *port-list*] | port-channel [*port-channel-list*]] basic-config**

Przejrzyj podstawową konfigurację MLD Snooping poszczególnych lub wszystkich portów.

Krok 6 **end**

Powróć do trybu privileged EXEC.

Krok 7 **copy running-config startup-config**

Zapisz ustawienia w pliku konfiguracyjnym.

Poniższy schemat przedstawia przykładowy sposób włączania funkcji MLD Snooping i Fast Leave dla portu 1/0/1-3:

**Switch#configure**

**Switch(config)#interface range fastEthernet 1/0/1-3**

**Switch(config-if-range)#ipv6 mld snooping**

**Switch(config-if-range)#ipv6 mld snooping immediate-leave**

**Switch(config-if-range)#show ipv6 mld snooping interface gigabitEthernet 1/0/1-3**

| Port    | MLD-Snooping | Fast-Leave |
|---------|--------------|------------|
| -----   | -----        | -----      |
| Gi1/0/1 | enable       | enable     |
| Gi1/0/2 | enable       | enable     |
| Gi1/0/3 | enable       | enable     |

**Switch(config-if-range)#end**

**Switch#copy running-config startup-config**

### 3.2.4 Konfiguracja statycznego dołączania hostów do grup

Hosty lub porty warstwy 2 dołączają zwykle dynamicznie do grup multicastowych, ale możliwe jest także statyczne przyłączenie się hostów do grup.

Wykonaj poniższe kroki, aby skonfigurować statyczne dołączanie hostów do grup:

Krok 1 **configure**

Uruchom tryb konfiguracji globalnej.

Krok 2 **ipv6 mld snooping vlan-config *vlan-id-list* static *ip* interface {fastEthernet *port-list* | gigabitEthernet *port-list* | ten-gigabitEthernet *port-list* | port-channel *lag-list*}**

*vlan-id-list*: Podaj ID lub listę ID VLAN-u(-ów).

*ip*: Podaj adres IP grupy multicastowej, do której mają dołączyć hosty.

*port-list* / *lag-list*: Zaznacz porty, z którymi hosty są połączone. Te porty będą statycznie przynależą do grupy.

---

Krok 3     **show ipv6 mld snooping groups static**  
Przejrzyj statyczną konfigurację MLD Snooping.

---

Krok 4     **end**  
Powróć do trybu privileged EXEC.

---

Krok 5     **copy running-config startup-config**  
Zapisz ustawienia w pliku konfiguracyjnym.

---

Poniższy schemat przedstawia przykładowy sposób konfiguracji statycznego dołączania portu 1/0/1-3 w sieci VLAN 2 do grupy multicastowej FF80::1234:01:

**Switch#configure**

**Switch(config)#ipv6 mld snooping vlan-config 2 static FF80::1234:01 interface gigabitEthernet 1/0/1-3**

**Switch(config)#show ipv6 mld snooping groups static**

| Multicast-ip  | VLAN-id | Addr-type | Switch-port |
|---------------|---------|-----------|-------------|
| -----         | -----   | -----     | -----       |
| ff80::1234:01 | 2       | static    | Gi1/0/1-3   |

**Switch(config)#end**

**Switch#copy running-config startup-config**

# 4 Konfiguracja MVR

Wykonaj poniższe kroki, aby przeprowadzić konfigurację MVR:

- 1) Skonfiguruj sieci 802.1Q VLAN.
- 2) Skonfiguruj MVR globalnie.
- 3) Dodaj grupy multicastowe do MVR.
- 4) Skonfiguruj MVR dla portów.
- 5) Skonfiguruj statyczne dodawanie portów do grup MVR (opcjonalnie).

## Wskazówki dotyczące konfiguracji

- MVR nie obsługuje komunikatów IGMPv3.
- Nie konfiguruj MVR na prywatnych portach VLAN-u, w innym przypadku MVR nie będzie działać.
- MVR działa na podstawowym mechanizmie IGMP Snooping, ale funkcje te działają niezależnie od siebie. Możliwe jest włączenie na porcie obydwu protokołów jednocześnie. Uruchomienie obydwu funkcji spowoduje, że MVR będzie nasłuchiwać raportów i zostawiać komunikaty przeznaczone tylko dla grup multicastowych skonfigurowanych za pomocą tego protokołu. Wszystkie inne grupy multicastowe będą zarządzane przez IGMP Snooping.

## 4.1 Przez GUI

### 4.1.1 Konfiguracja VLAN-ów standardu 802.1Q

Przed rozpoczęciem konfiguracji MVR, utwórz 802.1Q VLAN jako VLAN multicastowy. Dodaj wszystkie porty źródłowe (porty uplink, które odbierają dane ruchu multicastowego z routera) do VLAN-u multicastowego jako porty tagowane. Skonfiguruj sieci 802.1Q VLAN dla portów odbierających (porty, które łączą się z hostami), zgodnie z wymaganiami sieci. Pamiętaj, że porty odbierające mogą należeć tylko do jednej sieci VLAN i nie mogą być dodane do VLAN-u multicastowego. Szczegółowe informacje znajdziesz w rozdziale *Konfiguracja 802.1Q VLAN*.



## 4.1.2 Globalna konfiguracja MVR

Wybierz z menu **L2 FEATURES > Multicast > MVR > MVR Config**, aby wyświetlić poniższą stronę.

Rys. 4-1 Globalna konfiguracja MVR

MVR Config

---

MVR:  Enable

MVR Mode:  Compatible  Dynamic

Multicast VLAN ID:  (1-4094)

Query Response Time:  tenths of a second (1-100)

Maximum Multicast Groups: 256

Current Multicast Groups: 0

Apply


Wykonaj poniższe kroki, aby skonfigurować MVR globalnie:

1) Uruchom MVR globalnie i i skonfiguruj parametry globalne.

|                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|--------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| MVR                      | Włącz lub wyłącz MVR globalnie.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| MVR Mode                 | Wybierz tryb MVR spośród "compatible" i "dynamic".                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|                          | <p><b>Compatible:</b> W tym trybie przełącznik nie przesyła do IGMP querier raportów, ani komunikatów leave od hostów. To oznacza, że IGMP querier nie może nauczyć się przynależności do grup multicastowych z przełącznika. IGMP querier musi mieć statyczną konfigurację, aby móc transmitować wszystkie strumienie multicastowe do przełącznika poprzez VLAN multicastowy.</p> <p><b>Dynamic:</b> W tym trybie, po otrzymaniu raportów lub komunikatów leave od hostów, przełącznik przesyła je do IGMP querier poprzez VLAN multicastowy (z odpowiednią translacją VLAN ID). IGMP querier może uczyć się przynależności do grup multicastowych poprzez otrzymane raporty lub komunikaty leave i transmitować strumienie multicastowe do przełącznika poprzez VLAN multicastowy, zgodnie z tablicą przekierowań ruchu multicastowego.</p> |
| Multicast VLAN ID        | Ustaw istniejącą sieć 802.1Q VLAN jako VLAN multicastowy.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Query Response Time      | Podaj maksymalny czas oczekiwania na porcie odbierającym na raport IGMP przed usunięciem portu z grupy multicastowej.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Maximum Multicast Groups | Maksymalna liczba grup multicastowych dla przełącznika.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Current Multicast Groups | Aktualna liczba skonfigurowanych na przełączniku grup multicastowych.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |

2) Kliknij **Apply**.

### 4.1.3 Dodawanie grup multicastowych do MVR

Dodawanie grup multicastowych do MVR odbywa się ręcznie. Wybierz z menu **L2 FEATURES > Multicast > MVR > MVR Group Config** i kliknij  **Add**, aby wyświetlić poniższą stronę.

Rys. 4-2 Dodawanie grup multicastowych do MVR

**MVR Group IP**

MVR Group IP:  (Format: 235.0.0.1)

MVR Group Count:  (1-256)

Cancel
Create

Wykonaj poniższe kroki, aby dodać grupy multicastowe do MVR:

1) Podaj adres IP grup multicastowych.

**MVR Group IP /  
MVR Group Count**





Podaj początkowy adres IP i liczbę następujących po sobie grup multicastowych.

Dane ruchu multicastowego przesłane na podany tutaj adres zostaną także przesłane do wszystkich portów źródłowych przełącznika i do wszystkich portów odbierających, które wysłały żądanie otrzymywania danych z tego adresu multicastowego.

2) Kliknij **Create**.

Dodane grupy multicastowe pojawią się w tabeli grup MVR, tak jak pokazano poniżej:

Rys. 4-3 Tabela grup MVR

| MVR Group Config                                                                          |       |              |          |         |                                                                                              |
|-------------------------------------------------------------------------------------------|-------|--------------|----------|---------|----------------------------------------------------------------------------------------------|
|                                                                                           | Index | MVR Group IP | Status   | Members | Operation                                                                                    |
|  Add |       |              |          |         |  Delete |
| <input type="checkbox"/>                                                                  | 1     | 239.1.2.3    | Inactive |         |         |
| <input type="checkbox"/>                                                                  | 2     | 239.1.2.4    | Inactive |         |         |
| Total: 2                                                                                  |       |              |          |         |                                                                                              |

**MVR Group IP**

Adres IP grupy multicastowej.

|        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Status | <p>Stan grupy MVR. W trybie "compatible", wszystkie grupy MVR są dodawane ręcznie, dlatego ich stanem jest zawsze "active". W trybie "dynamii" możliwe są dwa stany:</p> <p><b>Inactive:</b> Grupa MVR group została dodana poprawnie, ale na port źródłowy nie zostały przesłane żadne zapytania z tej grup multicastowej.</p> <p><b>Active:</b> Grupa MVR została dodana poprawnie, a na port źródłowy zostały przesłane zapytania z tej grup multicastowej.</p> |
| Member | Porty danej grupy MVR.                                                                                                                                                                                                                                                                                                                                                                                                                                             |

#### 4.1.4 Konfiguracja MVR dla portów

Wybierz z menu **L2 FEATURES > Multicast > MVR > Port Config**, aby wyświetlić poniższą stronę.

Rys. 4-4 Konfiguracja MVR dla portu

| Port Config                         |        |         |      |                 |            |
|-------------------------------------|--------|---------|------|-----------------|------------|
| UNIT1                               |        |         |      |                 |            |
| <input type="checkbox"/>            | Port   | Mode    | Type | Status          | Fast Leave |
| <input checked="" type="checkbox"/> | 1/0/1  | Disable | None | Inactive/InVLAN | Disable    |
| <input type="checkbox"/>            | 1/0/2  | Disable | None | Inactive/InVLAN | Disable    |
| <input type="checkbox"/>            | 1/0/3  | Disable | None | Inactive/InVLAN | Disable    |
| <input type="checkbox"/>            | 1/0/4  | Disable | None | Inactive/InVLAN | Disable    |
| <input type="checkbox"/>            | 1/0/5  | Disable | None | Inactive/InVLAN | Disable    |
| <input type="checkbox"/>            | 1/0/6  | Disable | None | Inactive/InVLAN | Disable    |
| <input type="checkbox"/>            | 1/0/7  | Disable | None | Inactive/InVLAN | Disable    |
| <input type="checkbox"/>            | 1/0/8  | Disable | None | Inactive/InVLAN | Disable    |
| <input type="checkbox"/>            | 1/0/9  | Disable | None | Inactive/InVLAN | Disable    |
| <input type="checkbox"/>            | 1/0/10 | Disable | None | Inactive/InVLAN | Disable    |

Total: 10      1 entry selected.     

Wykonaj poniższe kroki, aby dodać grupy multicastowe do MVR:

- 1) Wybierz jeden lub więcej portów do konfiguracji.
- 2) Włącz MVR i skonfiguruj typ portu oraz funkcję Fast Leave dla portu.

|      |                                            |
|------|--------------------------------------------|
| Mode | Włącz lub wyłącz MVR dla wybranych portów. |
|------|--------------------------------------------|

|            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Type       | <p>Skonfiguruj typ portu.</p> <p><b>None:</b> Port nie jest portem MVR. Jeżeli podejmiesz próbę konfiguracji takiego portu korzystając z właściwości MVR, ta operacja zakończy się niepowodzeniem.</p> <p><b>Source:</b> Ustaw porty uplink, które otrzymują i przesyłają dane ruchu multicastowego poprzez VLAN multicastowy jako porty źródłowe ("source ports"). Takie porty powinny należeć do VLAN-u multicastowego. W trybie "compatible" porty źródłowe są automatycznie dodawane do wszystkich grup multicastowych, natomiast w trybie "dynamic" konieczne jest ręczne dodawanie ich do odpowiednich grup multicastowych.</p> <p><b>Receiver:</b> Skonfiguruj porty, które łączą się z hostami jako porty odbierające. Port odbierający może należeć tylko do jednego VLAN-u, z wykluczeniem VLAN-u multicastowego. W obydwu trybach przełącznik dodaje porty odbierające do odpowiednich grup multicastowych lub je usuwa na podstawie raportów i wiadomości leave, otrzymanych od hostów.</p> |
| Status     | <p>Stan portu.</p> <p><b>Active/InVLAN:</b> Port jest fizycznie włączony i przynależy do jednego lub kilku VLAN-ów.</p> <p><b>Active/NotInVLAN:</b> Port jest fizycznie włączony, ale nie przynależy do żadnego VLAN-u.</p> <p><b>Inactive/InVLAN:</b> Port jest fizycznie wyłączony, ale przynależy do jednego lub kilku VLAN-ów.</p> <p><b>Inactive/NotInVLAN:</b> Port jest fizycznie wyłączony i nie przynależy do żadnego VLAN-u.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Fast Leave | <p>Włącz lub wyłącz Fast Leave dla wybranych portów. Tylko porty odbierające obsługują Fast Leave. Przed włączeniem Fast Leave dla portu, upewnij się, że z portem połączone jest tylko jedno urządzenie odbierające.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |

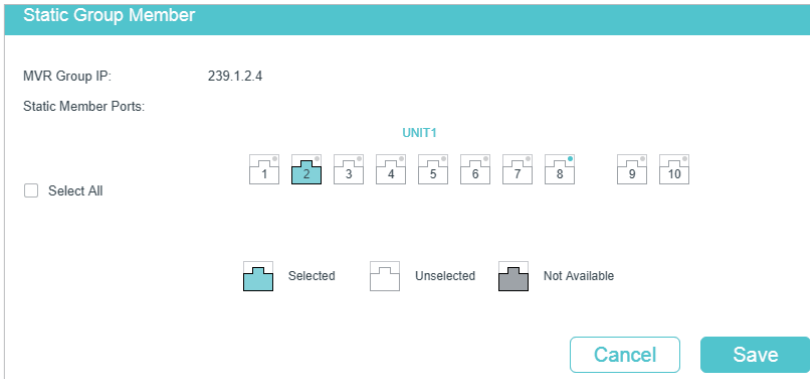
3) Kliknij **Apply**.

#### 4.1.5 (Opcjonalnie) Statyczne dodawanie portów do grup MVR

Tylko porty odbierające mogą być dodawane do grup MVR statycznie. Przełącznik dodaje porty do odpowiednich grup multicastowych lub usuwa je na podstawie raportów i komunikatów leave, otrzymanych od hostów.

Wybierz z menu **L2 FEATURES > Multicast > MVR > Static Group Members** i kliknij  przy wybranej pozycji z grupą MVR, aby wyświetlić poniższą stronę.

Rys. 4-5 Konfiguracja statycznego dołączania hostów do grupy MVR



Wykonaj poniższe kroki, aby statycznie dodać porty do grupy MVR:

- 1) Wybierz porty, aby dodać je do grupy MVR.
- 2) Kliknij **Save**.

## 4.2 Przez CLI

### 4.2.1 Konfiguracja sieci 802.1Q VLAN

Przed rozpoczęciem konfiguracji MVR, utwórz 802.1Q VLAN jako VLAN multicastowy. Dodaj wszystkie porty źródłowe do VLAN-u multicastowego jako porty tagowane. Skonfiguruj sieci 802.1Q VLAN dla portów odbierających, zgodnie z wymaganiami sieci. Pamiętaj, że porty odbierające mogą należeć tylko do jednej sieci VLAN i nie mogą być dodane do VLAN-u multicastowego. Szczegółowe informacje znajdziesz w części [Konfiguracja 802.1Q VLAN](#).

### 4.2.2 Globalna konfiguracja MVR

Wykonaj poniższe kroki, aby skonfigurować MVR globalnie:

|        |                                                          |
|--------|----------------------------------------------------------|
| Krok 1 | <b>configure</b><br>Uruchom tryb konfiguracji globalnej. |
| Krok 2 | <b>mvr</b><br>Włącz MVR globalnie.                       |

- 
- Krok 3     **mvr mode { compatible | dynamic }**  
Wybierz tryb MVR spośród "compatible" i "dynamic".
- compatible:** W tym trybie przełącznik nie przesyła do IGMP querier raportów, ani komunikatów leave od hostów. To oznacza, że IGMP querier nie może nauczyć się przynależności do grup multicastowych z przełącznika. IGMP querier musi mieć statyczną konfigurację, aby móc transmitować wszystkie strumienie multicastowe do przełącznika poprzez VLAN multicastowy.
- dynamic:** W tym trybie, po otrzymaniu raportów lub komunikatów leave od hostów, przełącznik przesyła je do IGMP querier poprzez VLAN multicastowy (z odpowiednią translacją VLAN ID). IGMP querier może uczyć się przynależności do grup multicastowych poprzez otrzymane raporty lub komunikaty leave i transmitować strumienie multicastowe do przełącznika poprzez VLAN multicastowy, zgodnie z tablicą przekierowań ruchu multicastowego.
- 
- Krok 4     **mvr vlan *vlan-id***  
Określ VLAN multicastowy.
- vlan-id:** Podaj ID VLAN-u multicastowego. Prawidłowe wartości wahają się od 1 do 4094.
- 
- Krok 5     **mvr querytime *time***  
Podaj maksymalny czas oczekiwania na porcie odbierającym na raport IGMP przed usunięciem portu z grupy multicastowej.
- time:** Podaj maksymalny czas odpowiedzi. Poprawne wartości wahają się od 1 do 100 dziesiątych części sekundy, a wartością domyślną jest 5 dziesiątych sekundy.
- 
- Krok 6     **mvr group *ip-addr count***  
Dodaj grupę multicastową do MVR.
- ip-addr:** Podaj początkowy adres IP następujących po sobie grup multicastowych.
- count:** Podaj liczbę grup multicastowych, które mają być dodane do MVR. Prawidłowe wartości wahają się od 1 do 256.
- 
- Krok 7     **show mvr**  
Przejrzyj globalną konfigurację MVR.
- show mvr members**  
Przejrzyj istniejące grupy MVR.
- 
- Krok 8     **end**  
Powróć do trybu privileged EXEC.
- 
- Krok 9     **copy running-config startup-config**  
Zapisz ustawienia w pliku konfiguracyjnym.
- 

Poniższy schemat przedstawia przykładowy sposób globalnego włączania MVR, ustawiania trybu MVR jako compatible, VLAN-u multicastowego jako VLAN 2, czasu odpowiedzi na zapytanie jako 5 dziesiątych sekundy oraz dodawania 239.1.2.3-239.1.2.5 do grupy MVR.

## Switch#configure

```
Switch(config)#mvr mode compatible
```

```
Switch(config)#mvr vlan 2
```

```
Switch(config)#mvr querytime 5
```

```
Switch(config)#mvr group 239.1.2.3 3
```

```
Switch(config)#show mvr
```

```
MVR :Enable
MVR Multicast Vlan :2
MVR Max Multicast Groups :256
MVR Current Multicast Groups :3
MVR Global Query Response Time :5 (tenths of sec)
MVR Mode Type :Compatible
```

```
Switch(config)#show mvr members
```

```
MVR Group IP status Members

239.1.2.3 active
239.1.2.4 active
239.1.2.5 active
```

```
Switch(config)#end
```

```
Switch#copy running-config startup-config
```

### 4.2.3 Konfiguracja MVR dla portów

Wykonaj poniższe kroki, aby skonfigurować MVR dla portów:

|        |                                                                                                                                                                                                                                                                                  |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Krok 1 | <b>configure</b><br>Uruchom tryb konfiguracji globalnej.                                                                                                                                                                                                                         |
| Krok 2 | <b>interface {fastEthernet <i>port</i>   range fastEthernet <i>port-list</i>   gigabitEthernet <i>port</i>   range gigabitEthernet <i>port-list</i>   ten-gigabitEthernet <i>port</i>   range ten-gigabitEthernet <i>port-list</i>}</b><br>Uruchom tryb konfiguracji interfejsu. |
| Krok 3 | <b>mvr</b><br>Włącz MVR dla portu.                                                                                                                                                                                                                                               |

- 
- Krok 4     **mvr type { source | receiver }**
- Skonfiguruj typ portu MVR. Domyślnie wybranym portem jest port non-MVR. Jeżeli podejmiesz próbę konfiguracji takiego portu korzystając z właściwości MVR, ta operacja zakończy się niepowodzeniem.
- source*: Ustaw porty uplink, które otrzymują i przesyłają dane ruchu multicastowego poprzez VLAN multicastowy jako porty źródłowe. Takie porty powinny należeć do VLAN-u multicastowego.
- receiver*: Skonfiguruj porty, które łączą się z hostami jako porty odbierające. Port odbierający może należeć tylko do jednego VLAN-u, z wykluczeniem VLAN-u multicastowego.
- 
- Krok 5     **mvr immediate**
- (Opcjonalnie) Włącz Fast Leave dla portu. Tylko porty odbierające obsługują Fast Leave. Przed włączeniem Fast Leave dla portu, upewnij się, że z portem połączone jest tylko jedno urządzenie odbierające.
- 
- Krok 6     **mvr vlan *vlan-id* group *ip-addr***
- (Opcjonalnie) Dodaj port do grupy MVR statycznie. Taki port może odbierać transmisję ruchu multicastowego przesłanego na adres IP multicastowy poprzez VLAN multicastowy.
- Tylko porty odbierające mogą być dodawane do grup MVR statycznie. Przełącznik dodaje porty do odpowiednich grup multicastowych lub usuwa je na podstawie raportów i komunikatów leave, otrzymanych od hostów.
- vlan-id*: Podaj ID VLAN-u multicastowego.
- ip-addr*: Podaj adres IP grupy multicastowej.
- 
- Krok 7     **show mvr interface {fastEthernet [*port-list*] | gigabitEthernet [*port-list*] | ten-gigabitEthernet [*port-list*] }**
- Przejrzyj konfigurację MVR określonych interfejsów.
- show mvr members**
- Przejrzyj informacje o przynależności do wszystkich grup MVR.
- 
- Krok 8     **end**
- Powróć do trybu privileged EXEC.
- 
- Krok 9     **copy running-config startup-config**
- Zapisz ustawienia w pliku konfiguracyjnym.
- 

Poniższy schemat przedstawia przykładowy sposób ustawiania portu 1/0/7 jako source port, portów 1/0/1-3 jako receiver ports, statycznego dodawania portu 1/0/1-3 do grupy 239.1.2.3 i włączania Fast Leave dla tych portów. VLAN-em multicastowym jest VLAN 2.

**Switch#configure**

**Switch(config)#interface gigabitEthernet 1/0/7**

**Switch(config-if)#mvr**

**Switch(config-if)#mvr type source**



```
Switch(config-if)#exit
```

```
Switch(config)#interface range gigabitEthernet 1/0/1-3
```

```
Switch(config-if-range)#mvr
```

```
Switch(config-if-range)#mvr type receiver
```

```
Switch(config-if-range)#mvr immediate
```

```
Switch(config-if-range)#mvr vlan 2 group 239.1.2.3
```

```
Switch(config-if-range)#show mvr interface fastEthernet 1/0/1-3,1/0/7
```

| Port    | Mode   | Type     | Status          | Immediate Leave |
|---------|--------|----------|-----------------|-----------------|
| Gi1/0/1 | Enable | Receiver | INACTIVE/InVLAN | Enable          |
| Gi1/0/2 | Enable | Receiver | INACTIVE/InVLAN | Enable          |
| Gi1/0/3 | Enable | Receiver | INACTIVE/InVLAN | Enable          |
| Gi1/0/7 | Enable | Source   | INACTIVE/InVLAN | Disable         |

```
Switch(config-if-range)#show mvr members
```

| MVR Group IP | status | Members          |
|--------------|--------|------------------|
| 239.1.2.3    | active | Gi1/0/1-3, 1/0/7 |

```
Switch(config)#end
```

```
Switch#copy running-config startup-config
```

# 5 Konfiguracja filtrowania pakietów multicastu

Wykonaj poniższe kroki, aby przeprowadzić proces konfiguracji filtrowania pakietów multicastu:


- 1) Utwórz profil IGMP lub profil MLD.
- 2) Wybierz, do których grup multicastowych można dołączać porty i skonfiguruj działania w przypadku zbyt wielu grup.

## 5.1 Przez GUI

### 5.1.1 Tworzenie profili multicast

Możesz tworzyć profile multicast zarówno dla sieci IPv4, jak i IPv6. Korzystając z profilu multicast przełącznik może tworzyć czarne i białe listy grup multicastowych, co pozwala filtrować źródła pakietów multicastu.

Tworzenie profili multicastu wygląda w ten sam sposób dla IPv4 i IPv6. Dla przykładu utworzymy profil IPv4.

Wybierz z menu **L2 FEATURES > Multicast > Multicast Filtering > IPv4 Profile** i kliknij  Add , aby wyświetlić poniższą stronę.

---

 **Uwaga:**

Aby utworzyć profil multicast dla IPv6, wybierz z menu **L2 FEATURES > Multicast > Multicast Filtering > IPv6 Profile**.

---

Rys. 5-1 Konfiguracja profilu IPv4

### General Config

Profile ID:  (1-999)

Mode:  Permit  Deny


### IP-Range

+ Add - Delete


| <input type="checkbox"/>  | Index | Start IP Address | End IP Address | Operation |
|---------------------------|-------|------------------|----------------|-----------|
| No entries in this table. |       |                  |                |           |
| Total: 0                  |       |                  |                |           |


### Bind Ports


UNIT1




LAGS



 Selected

 Unselected

 Not Available

Discard
Save

Wykonaj poniższe kroki, aby utworzyć profil.

- 1) W sekcji **General Config** wybierz ID profilu i tryb filtrowania.

|                   |                                                                                                                                                                                                                                                                                                                                            |
|-------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Profile ID</b> | Podaj ID, wybierając wartość z przedziału 1 - 999.                                                                                                                                                                                                                                                                                         |
| <b>Mode</b>       | Ustal tryb filtrowania, wybierając <b>Permit</b> lub <b>Deny</b> .<br><br><b>Permit:</b> Pełni funkcję białej listy, zezwalając tylko określonym portom na dołączenie do wybranych grup multicastowych.<br><br><b>Deny:</b> Pełni funkcję czarnej listy, uniemożliwiając określonym portom na dołączanie do wybranych grup multicastowych. |

- 2) W sekcji **IP-Range** kliknij + Add , aby wyświetlić poniższą stronę. Skonfiguruj początkowy adres IP i końcowy adres IP grup multicastowych, które mają podlegać filtrowaniu i kliknij **Create**.

Rys. 5-2 Konfiguracja filtrowania grup multicastowych

IP-Range

Start IP Address:  (Format: 235.0.0.1)

End IP Address:  (Format: 235.0.0.1)

3) W sekcji **Bind Ports** wybierz porty, które chcesz powiązać z profilem.

4) Kliknij **Save**.

## 5.1.2 Konfiguracja filtrowania pakietów multicastu dla portów

Mapowanie relacji między portami i profilami możesz modyfikować partami. Masz także możliwość konfiguracji liczby grup, do których port może dołączyć oraz działań w przypadku zbyt wielu grup.

Konfiguracja filtrowania pakietów multicastu dla portów jest taka sama dla IPv4 i IPv6. Dla przykładu skonfigurujemy filtrowanie w sieci IPv4.

Wybierz z menu **L2 FEATURES > Multicast > Multicast Filtering > IPv4 Port Config**, aby wyświetlić poniższą stronę.

### Uwaga:

Dla IPv6 wybierz z menu **L2 FEATURES > Multicast > Multicast Filtering > IPv6 Port Config**.

Rys. 5-3 Konfiguracja filtrowania pakietów multicastu dla portów

Port Config

UNIT1

LAGS

|                                     | Port   | Profile ID | Maximum Groups | Overflow Action | LAG | Operation     |
|-------------------------------------|--------|------------|----------------|-----------------|-----|---------------|
| <input checked="" type="checkbox"/> | 1/0/1  |            | 511            | Drop            | --- | Clear Profile |
| <input type="checkbox"/>            | 1/0/2  |            | 511            | Drop            | --- | Clear Profile |
| <input type="checkbox"/>            | 1/0/3  |            | 511            | Drop            | --- | Clear Profile |
| <input type="checkbox"/>            | 1/0/4  |            | 511            | Drop            | --- | Clear Profile |
| <input type="checkbox"/>            | 1/0/5  |            | 511            | Drop            | --- | Clear Profile |
| <input type="checkbox"/>            | 1/0/6  |            | 511            | Drop            | --- | Clear Profile |
| <input type="checkbox"/>            | 1/0/7  |            | 511            | Drop            | --- | Clear Profile |
| <input type="checkbox"/>            | 1/0/8  |            | 511            | Drop            | --- | Clear Profile |
| <input type="checkbox"/>            | 1/0/9  |            | 511            | Drop            | --- | Clear Profile |
| <input type="checkbox"/>            | 1/0/10 |            | 511            | Drop            | --- | Clear Profile |

Total: 10
1 entry selected.

Wykonaj poniższe kroki, aby powiązać profil z portami i skonfigurować odpowiednie parametry dla portów:

- 1) Wybierz jeden lub kilka portów do konfiguracji.
- 2) Wybierz profil, z którym chcesz powiązać porty i skonfiguruj maksymalną liczbę grup, do których port może dołączyć oraz działania w przypadku zbyt wielu grup.

|                 |                                                                                                                                                                                                                                                                                                                                                                                                                      |
|-----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Profile ID      | Podaj ID istniejącego profilu, aby powiązać go z wybranymi portami. Jeden port może być powiązany tylko z jednym profilem.                                                                                                                                                                                                                                                                                           |
| Maximum Groups  | Podaj liczbę grup multicastowych, do których port może dołączyć. Prawidłowe wartości wahają się od 1 do 511.                                                                                                                                                                                                                                                                                                         |
| Overflow Action | Wybierz działanie, które podejmie przełącznik względem nowych grup multicastowych, gdy port dołączy do zbyt wielu grup multicastowych.<br><br><b>Drop:</b> Zaprzestanie wysyłania kolejnych komunikatów o członkowstwie, aby zapobiec dołączaniu portu do nowych grup multicastowych.<br><br><b>Replace:</b> Zastąpienie istniejącej grupy multicastowej o najniższym adresie MAC multicast nową grupą multicastową. |
| LAG             | Grupa agregacji łączy, do której należy port.                                                                                                                                                                                                                                                                                                                                                                        |
| Operation       | Kliknij <b>Clear Profile</b> , aby usunąć powiązanie między profilem a portem.                                                                                                                                                                                                                                                                                                                                       |

- 3) Kliknij **Apply**.

## 5.2 Przez CLI

### 5.2.1 Tworzenie profili multicast

Możesz tworzyć profile multicast zarówno dla sieci IPv4, jak i IPv6. Korzystając z profilu multicast przełącznik może tworzyć czarne i białe listy grup multicastowych, co pozwala filtrować źródła pakietów multicastu.

#### Tworzenie profilu IGMP (Profil multicast dla IPv4)

|        |                                                                                             |
|--------|---------------------------------------------------------------------------------------------|
| Krok 1 | <b>configure</b><br>Uruchom tryb konfiguracji globalnej.                                    |
| Krok 2 | <b>ip igmp profile <i>id</i></b><br>Utwórz nowy profil i uruchom tryb konfiguracji profilu. |

**Krok 3 Permit**

Ustaw dla profilu tryb filtrowania jako permit. Profil będzie pełnił funkcję białej listy, zezwalając tylko określonym portom na dołączenie do wybranych grup multicastowych.

**deny**

Ustaw dla profilu tryb filtrowania jako deny. Profil będzie pełnił funkcję czarnej listy, uniemożliwiając określonym portom na dołączanie do wybranych grup multicastowych.

**Krok 4 range start-ip end-ip**

Skonfiguruj zakres adresów IP grup multicastowych, które mają podlegać filtrowaniu.

*start-ip / end-ip*: Podaj początkowy adres IP i końcowy adres IP.

**Krok 5 show ip igmp profile [/id]**

Przejrzyj szczegóły konfiguracji profilu IGMP.

**Krok 6 end**

Powróć do trybu privileged EXEC.

**Krok 7 copy running-config startup-config**

Zapisz ustawienia w pliku konfiguracyjnym.

Poniższy schemat przedstawia przykładowy sposób konfiguracji Profile 1, tak aby przełącznik filtrował strumienie multicastowe przesyłane na adres 226.0.0.5-226.0.0.10:

**Switch#configure****Switch(config)#ip igmp snooping****Switch(config)#ip igmp profile 1****Switch(config-igmp-profile)#deny****Switch(config-igmp-profile)#range 226.0.0.5 226.0.0.10****Switch(config-igmp-profile)#show ip igmp profile**

IGMP Profile 1

deny

range 226.0.0.5 226.0.0.10

Switch(config)#end

Switch#copy running-config startup-config

**Tworzenie profilu MLD (profil multicast dla IPv6)****Krok 1 configure**

Uruchom tryb konfiguracji globalnej.

|        |                                                                                                                                                                                                                                                                                                                                                                                                  |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Krok 2 | <b>ipv6 mld profile <i>id</i></b><br>Utwórz nowy profil i uruchom tryb konfiguracji profilu.                                                                                                                                                                                                                                                                                                     |
| Krok 3 | <b>Permit</b><br>Ustaw dla profilu tryb filtrowania jako permit. Profil będzie pełnić funkcję białej listy, zezwalając tylko określonym portom na dołączenie do wybranych grup multicastowych.<br><br><b>deny</b><br>Ustaw dla profilu tryb filtrowania jako deny. Profil będzie pełnić funkcję czarnej listy, uniemożliwiając określonym portom na dołączanie do wybranych grup multicastowych. |
| Krok 4 | <b>range <i>start-ip end-ip</i></b><br>Skonfiguruj zakres adresów IP grup multicastowych, które mają podlegać filtrowaniu.<br><i>start-ip / end-ip</i> : Podaj początkowy adres IP i końcowy adres IP.                                                                                                                                                                                           |
| Krok 5 | <b>show ipv6 mld profile [<i>id</i>]</b><br>Przejrzyj szczegóły konfiguracji profilu MLD.                                                                                                                                                                                                                                                                                                        |
| Krok 6 | <b>end</b><br>Powróć do trybu privileged EXEC.                                                                                                                                                                                                                                                                                                                                                   |
| Krok 7 | <b>copy running-config startup-config</b><br>Zapisz ustawienia w pliku konfiguracyjnym.                                                                                                                                                                                                                                                                                                          |

Poniższy schemat przedstawia przykładowy sposób konfiguracji Profile 1, tak aby przełącznik filtrował strumienie multicastowe przesyłane na adres ff01::1234:5-ff01::1234:8:

```
Switch#configure
```

```
Switch(config)#ipv6 mld snooping
```

```
Switch(config)#ipv6 mld profile 1
```

```
Switch(config-mld-profile)#deny
```

```
Switch(config-mld-profile)#range ff01::1234:5 ff01::1234:8
```

```
Switch(config-mld-profile)#show ipv6 mld profile
```

```
MLD Profile 1
```

```
deny
```

```
range ff01::1234:5 ff01::1234:8
```

```
Switch(config)#end
```

```
Switch#copy running-config startup-config
```

## 5.2.2 Tworzenie powiązań portów z profilami

Możesz już tworzyć powiązania pomiędzy portami a utworzonymi profilami IGMP lub MLD. Masz także możliwość konfiguracji liczby grup, do których port może dołączyć oraz działań w przypadku zbyt wielu grup.

### Wiązanie portów z profilem IGMP

|        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Krok 1 | <b>configure</b><br>Uruchom tryb konfiguracji globalnej.                                                                                                                                                                                                                                                                                                                                                                                                             |
| Krok 2 | <b>interface {fastEthernet <i>port</i>   range fastEthernet <i>port-list</i>   gigabitEthernet <i>port</i>   range gigabitEthernet <i>port-list</i>   ten-gigabitEthernet <i>port</i>   range ten-gigabitEthernet <i>port-list</i>   port-channel <i>port-channel-id</i>   range port-channel <i>port-channel-list</i>}</b><br>Uruchom tryb konfiguracji interfejsu.                                                                                                 |
| Krok 3 | <b>ip igmp filter <i>profile-id</i></b><br>Powiąż profil IGMP z wybranymi portami.<br><br><i>profile-id</i> : Podaj ID istniejącego profilu, aby powiązać go z wybranymi portami.                                                                                                                                                                                                                                                                                    |
| Krok 4 | <b>ip igmp snooping max-groups <i>maxgroup</i></b><br>Podaj liczbę grup multicastowych, do których port może dołączyć.<br><br><i>maxgroup</i> : Podaj maksymalną liczbę grup multicastowych. Prawidłowe wartości wahają się od 1 do 511.                                                                                                                                                                                                                             |
| Krok 5 | <b>ip igmp snooping max-groups action {drop   replace}</b><br>Wybierz działanie, które podejmie przełącznik względem nowych grup multicastowych, gdy port dołączy do zbyt wielu grup multicastowych.<br><br>drop: Zaprzestanie wysyłania kolejnych komunikatów o członkowstwie, aby zapobiec dołączaniu portu do nowych grup multicastowych.<br><br>replace: Zastąpienie istniejącej grupy multicastowej o najniższym adresie MAC multicast nową grupą multicastową. |
| Krok 6 | <b>show ip igmp profile [<i>id</i>]</b><br>Przejrzyj szczegóły konfiguracji profilu IGMP.<br><br><b>show ip igmp snooping interface [fastEthernet [<i>port-list</i>]   gigabitEthernet [<i>port-list</i>]   ten-gigabitEthernet [<i>port-list</i>]   port-channel [<i>port-channel-list</i>]] max-groups</b><br>Przejrzyj limity grup multicastowych dla wybranych portów lub dla wszystkich portów.                                                                 |
| Krok 7 | <b>end</b><br>Powróć do trybu privileged EXEC.                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Krok 8 | <b>copy running-config startup-config</b><br>Zapisz ustawienia w pliku konfiguracyjnym.                                                                                                                                                                                                                                                                                                                                                                              |



Poniższy schemat przedstawia przykładowy sposób wiązania istniejącego Profile 1 z portem 1/0/2, ustawiania maksymalnej liczby grup multicastowych, do których port 1/0/2 może dołączyć jako 50 i Overflow Action jako Drop:

```
Switch#configure
```

```
Switch(config)#interface gigabitEthernet 1/0/2
```

```
Switch(config-if)#ip igmp snooping
```

```
Switch(config-if)#ip igmp filter 1
```

```
Switch(config-if)#ip igmp snooping max-groups 50
```

```
Switch(config-if)#ip igmp snooping max-groups action drop
```

```
Switch(config-if)#show ip igmp profile
```

```
IGMP Profile 1
```

```
...
```

```
Binding Port(s)
```

```
Gi1/0/2
```

```
Switch(config-if)#show ip igmp snooping interface gigabitEthernet 1/0/2 max-groups
```

| Port    | Max-Groups | Overflow-Action |
|---------|------------|-----------------|
| -----   | -----      | -----           |
| Gi1/0/2 | 50         | Drops           |

```
Switch(config)#end
```

```
Switch#copy running-config startup-config
```

## Wiązanie portów z profilem MLD

Krok 1     **configure**

Uruchom tryb konfiguracji globalnej.

Krok 2     **interface {fastEthernet *port* | range fastEthernet *port-list* | gigabitEthernet *port* | range gigabitEthernet *port-list* | ten-gigabitEthernet *port* | range ten-gigabitEthernet *port-list* | port-channel *port-channel-id* | range port-channel *port-channel-list*}**

Uruchom tryb konfiguracji interfejsu.

Krok 3     **ipv6 mld filter *profile-id***

Powiąz profil MLD z wybranymi portami.

*profile-id*: Podaj ID istniejącego profilu, aby powiązać go z wybranymi portami.

**Krok 4**    **ipv6 mld snooping max-groups** *maxgroup*

Podaj liczbę grup multicastowych, do których port może dołączyć.

*maxgroup*: odaj maksymalną liczbę grup multicastowych. Prawidłowe wartości wahają się od 1 do 511.

**Krok 5**    **ipv6 mld snooping max-groups action** {drop | replace}

Wybierz działanie, które podejmie przełącznik względem nowych grup multicastowych, gdy port dołączy do zbyt wielu grup multicastowych.

*drop*: Zaprzestanie wysyłania kolejnych komunikatów o członkowstwie, aby zapobiec dołączaniu portu do nowych grup multicastowych.

*replace*: Zastąpienie istniejącej grupy multicastowej o najniższym adresie MAC multicast nową grupą multicastową.

**Krok 6**    **show ipv6 mld profile** [*id*]

Przejrzyj szczegóły konfiguracji profilu MLD.

**show ipv6 mld snooping interface** [*fastEthernet* [*port-list*] | *gigabitEthernet* [*port-list*] | *ten-gigabitEthernet* [*port-list*] | *port-channel* [*port-channel-list*]] **max-groups**

Przejrzyj limity grup multicastowych dla wybranych portów lub dla wszystkich portów.

**Krok 7**    **end**

Powróć do trybu uprzywilejowanego (privileged EXEC mode).

**Krok 8**    **copy running-config startup-config**

Zapisz ustawienia w pliku konfiguracyjnym.

Poniższy schemat przedstawia przykładowy sposób wiązania istniejącego Profile 1 z portem 1/0/2, ustawiania maksymalnej liczby grup multicastowych, do których port 1/0/2 może dołączyć jako 50 i Overflow Action jako Drop:

```
Switch#configure
```

```
Switch(config)#interface gigabitEthernet 1/0/2
```

```
Switch(config-if)#ipv6 mld snooping
```

```
Switch(config-if)#ipv6 mld filter 1
```

```
Switch(config-if)#ipv6 mld snooping max-groups 50
```

```
Switch(config-if)#ipv6 mld snooping max-groups action drop
```

```
Switch(config-if)#show ipv6 mld profile
```

```
MLD Profile 1
```

```
...
```

```
Binding Port(s)
```

Gi1/0/2

**Switch(config-if)#show ipv6 mld snooping interface gigabitEthernet 1/0/2 max-groups**

| Port    | Max-Groups | Overflow-Action |
|---------|------------|-----------------|
| -----   | -----      | -----           |
| Gi1/0/2 | 50         | Drops           |

**Switch(config)#end**

**Switch#copy running-config startup-config**

# 6 Przeglądanie informacji Multicast Snooping

Możesz przeglądać następujące informacje dotyczące Multicast Snooping:

- Tablica adresów IPv4 multicast.
- Statystyki pakietów IPv4 multicast na każdym porcie.
- Tablica adresów IPv6 multicast.
- Statystyki pakietów IPv6 multicast na każdym porcie.

## 6.1 Przez GUI

### 6.1.1 Przeglądanie tablicy adresów IPv4 multicast

Wybierz z menu **L2 FEATURES > Multicast > Multicast Info > IPv4 Multicast Table**, aby wyświetlić poniższą stronę:

Rys. 6-1 Tablica adresów IPv4 multicast

| Index                     | Multicast IP | VLAN ID | Source | Type | Forward Ports |
|---------------------------|--------------|---------|--------|------|---------------|
| No entries in this table. |              |         |        |      |               |
| Total: 0                  |              |         |        |      |               |

Tablica adresów IP multicast zawiera wszystkie aktualne pozycje IP-VLAN-Port multicast:

|              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|--------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Multicast IP | Źródłowy adres IP multicast.                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| VLAN ID      | ID sieci VLAN, do której przynależy grupa multicastowa.                                                                                                                                                                                                                                                                                                                                                                                                              |
| Source       | Źródło wpisu ruchu multicastowego.<br><b>IGMP Snooping:</b> IGMP Snooping uczy się wpisu ruchu multicastowego.<br><b>MVR:</b> MVR uczy się wpisu ruchu multicastowego.                                                                                                                                                                                                                                                                                               |
| Type         | Metody generowania wpisów ruchu multicastowego.<br><b>Dynamic:</b> Wpis jest przyswajany dynamicznie. Wszystkie porty członkowskie dodawane są dynamicznie do grupy multicastowej.<br><b>Static:</b> Wpis jest dodawany ręcznie. Wszystkie porty członkowskie dodawane są ręcznie do grupy multicastowej.<br><b>Mix:</b> Wpis jest przyswajany dynamicznie (lub ręcznie) i niektóre porty członkowskie dodawane są ręcznie (lub dynamicznie) do grupy multicastowej. |

Forward Ports

Wszystkie porty grupy multicastowej, w tym porty routera i porty przełącznika.

## 6.1.2 Przeglądanie statystyk pakietów IPv4 na poszczególnych portach

Wybierz z menu **L2 FEATURES > Multicast > Multicast Info > IPv4 Multicast Statistics**, aby wyświetlić poniższą stronę

Rys. 6-2 Statystyki pakietów IPv4

**Auto Refresh**

Auto Refresh:

Refresh Interval:  seconds (3-300)

[Apply](#)

---

**Port Statistics**

**UNIT1**

**LAGS**

Refresh

| ID        | Port   | Query Packets | Report Packets (v1) | Report Packets (v2) | Report Packets (v3) | Leave Packets | Error Packets |
|-----------|--------|---------------|---------------------|---------------------|---------------------|---------------|---------------|
| 1         | 1/0/1  | 0             | 0                   | 0                   | 0                   | 0             | 0             |
| 2         | 1/0/2  | 0             | 0                   | 0                   | 0                   | 0             | 0             |
| 3         | 1/0/3  | 0             | 0                   | 0                   | 0                   | 0             | 0             |
| 4         | 1/0/4  | 0             | 0                   | 0                   | 0                   | 0             | 0             |
| 5         | 1/0/5  | 0             | 0                   | 0                   | 0                   | 0             | 0             |
| 6         | 1/0/6  | 0             | 0                   | 0                   | 0                   | 0             | 0             |
| 7         | 1/0/7  | 0             | 0                   | 0                   | 0                   | 0             | 0             |
| 8         | 1/0/8  | 0             | 0                   | 0                   | 0                   | 0             | 0             |
| 9         | 1/0/9  | 0             | 0                   | 0                   | 0                   | 0             | 0             |
| 10        | 1/0/10 | 0             | 0                   | 0                   | 0                   | 0             | 0             |
| Total: 10 |        |               |                     |                     |                     |               |               |

Wykonaj poniższe kroki, aby wyświetlić statystyki pakietów IPv4 na każdym porcie:

- 1) Aby zobaczyć statystyki w czasie rzeczywistym, włącz **Auto Refresh** lub kliknij **Refresh**.

Auto Refresh

Włącz lub wyłącz Auto Refresh. Włączenie opcji spowoduje automatyczne odświeżanie statystyk przez przełącznik.

Refresh Interval

Gdy włączysz **Auto Refresh**, podaj interwał odświeżania statystyk.

- 2) W sekcji **Port Statistics** możesz przeglądać statystyki pakietów IPv4 na każdym porcie.

Query Packets

Liczba pakietów zapytań odebranych na porcie.

Report Packets (v1)

Liczba pakietów raportów IGMPv1 odebranych na porcie.

|                     |                                                       |
|---------------------|-------------------------------------------------------|
| Report Packets (v2) | Liczba pakietów raportów IGMPv2 odebranych na porcie. |
| Report Packets (v3) | Liczba pakietów raportów IGMPv3 odebranych na porcie. |
| Leave Packets       | Liczba pakietów leave odebranych na porcie.           |
| Error Packets       | Liczba pakietów error odebranych na porcie.           |

### 6.1.3 Przeglądanie tablicy adresów IPv6 multicast

Wybierz z menu **L2 FEATURES > Multicast > Multicast Info > IPv6 Multicast Table**, aby wyświetlić poniższą stronę:

Rys. 6-3 Tablica adresów IPv6 multicast

| Index                     | Multicast IP | VLAN ID | Source | Type | Forward Ports |
|---------------------------|--------------|---------|--------|------|---------------|
| No entries in this table. |              |         |        |      |               |
| Total: 0                  |              |         |        |      |               |

Tablica adresów IP multicast zawiera wszystkie aktualne wpisy IP-VLAN-Port multicast:

|              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|--------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Multicast IP | Źródłowy adres IP multicast.                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| VLAN ID      | ID sieci VLAN, do której przynależy grupa multicastowa.                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Source       | Źródło wpisu ruchu multicastowego.<br><b>MLD Snooping:</b> MLD Snooping uczy się wpisu ruchu multicastowego.                                                                                                                                                                                                                                                                                                                                                                     |
| Type         | Metody generowania wpisów ruchu multicastowego.<br><br><b>Dynamic:</b> Wpis jest przyswajany dynamicznie. Wszystkie porty członkowskie dodawane są dynamicznie do grupy multicastowej.<br><br><b>Static:</b> Wpis jest dodawany ręcznie. Wszystkie porty członkowskie dodawane są ręcznie do grupy multicastowej.<br><br><b>Mix:</b> Wpis jest przyswajany dynamicznie (lub ręcznie) i niektóre porty członkowskie dodawane są ręcznie (lub dynamicznie) do grupy multicastowej. |
| Forward Port | Wszystkie porty grupy multicastowej, w tym porty routera i porty przełącznika.                                                                                                                                                                                                                                                                                                                                                                                                   |

## 6.1.4 Przeglądanie statystyk pakietów IPv6 na poszczególnych portach

Wybierz z menu **L2 FEATURES > Multicast > Multicast Info > IPv6 Multicast Statistics**, aby wyświetlić poniższą stronę:

Rys. 6-4 Statystyki pakietów IPv6

**Auto Refresh**

Auto Refresh:

Refresh Interval:  seconds (3-300)

[Apply](#)

**Port Statistics**

UNIT1
LAGS

↻ Refresh

| ID        | Port   | Query Packets | Report Packets (v1) | Report Packets (v2) | Done Packets | Error Packets |
|-----------|--------|---------------|---------------------|---------------------|--------------|---------------|
| 1         | 1/0/1  | 0             | 0                   | 0                   | 0            | 0             |
| 2         | 1/0/2  | 0             | 0                   | 0                   | 0            | 0             |
| 3         | 1/0/3  | 0             | 0                   | 0                   | 0            | 0             |
| 4         | 1/0/4  | 0             | 0                   | 0                   | 0            | 0             |
| 5         | 1/0/5  | 0             | 0                   | 0                   | 0            | 0             |
| 6         | 1/0/6  | 0             | 0                   | 0                   | 0            | 0             |
| 7         | 1/0/7  | 0             | 0                   | 0                   | 0            | 0             |
| 8         | 1/0/8  | 0             | 0                   | 0                   | 0            | 0             |
| 9         | 1/0/9  | 0             | 0                   | 0                   | 0            | 0             |
| 10        | 1/0/10 | 0             | 0                   | 0                   | 0            | 0             |
| Total: 28 |        |               |                     |                     |              |               |

Wykonaj poniższe kroki, aby wyświetlić statystyki pakietów IPv6 na każdym porcie:

- 1) Aby zobaczyć statystyki w czasie rzeczywistym, włącz **Auto Refresh** lub kliknij **Refresh**.

**Auto Refresh**      Włącz lub wyłącz Auto Refresh. Włączenie opcji spowoduje automatyczne odświeżanie statystyk przez przełącznik.

**Refresh Interval**      Gdy włączysz **Auto Refresh**, podaj interwał odświeżania statystyk.

- 2) W sekcji **Port Statistics** możesz przeglądać statystyki pakietów IPv6 na każdym porcie.

**Query Packets**      Liczba pakietów zapytań odebranych przez port.

**Report Packets (v1)**      Liczba pakietów raportów MLDv1 odebranych na porcie.

**Report Packets (v2)**      Liczba pakietów raportów MLDv2 odebranych na porcie.

**Done Packets**      Liczba pakietów done odebranych na porcie.

---

|               |                                             |
|---------------|---------------------------------------------|
| Error Packets | Liczba pakietów error odebranych na porcie. |
|---------------|---------------------------------------------|

---

## 6.2 Przez CLI

### 6.2.1 Przeglądanie informacji o Multicast Snooping IPv4

---

**show ip igmp snooping groups [ vlan *vlan-id* ] [count | dynamic | dynamic count | static | static count ]**

Polecenie pokazuje informacje o określonych grupach multicastowych we wszystkich VLAN-ach lub tylko w wybranych VLAN-ach.

count: Liczba grup multicastowych.

dynamic: Informacje o wszystkich dynamicznych grupach multicastowych.

dynamic count: Liczba dynamicznych grup multicastowych.

static: Informacje o wszystkich statycznych grupach multicastowych.

static count: Liczba statycznych grup multicastowych.

---

**show ip igmp snooping interface [ fastEthernet [ *port-list* ] | gigabitEthernet [ *port-list* ] | ten-gigabitEthernet [ *port-list* ] ] packet-stat**

Statystyki pakietów na wybranych portach lub na wszystkich portach.

---

**clear ip igmp snooping statistics**

Wyczyść statystyki wszystkich pakietów IGMP.

### 6.2.2 Przeglądanie informacji o Multicast Snooping IPv6

---

**show ipv6 mld snooping groups [vlan *vlan-id* ] [count | dynamic | dynamic count | static | static count ]**

Polecenie pokazuje informacje o określonych grupach multicastowych we wszystkich VLAN-ach lub tylko w wybranych VLAN-ach.

count: Liczba grup multicastowych.

dynamic: Informacje o wszystkich dynamicznych grupach multicastowych.

dynamic count: Liczba dynamicznych grup multicastowych.

static: Informacje o wszystkich statycznych grupach multicastowych.

static count: Liczba statycznych grup multicastowych.

---

**show ipv6 mld snooping interface [ fastEthernet [ *port-list* ] | gigabitEthernet [ *port-list* ] | ten-gigabitEthernet [ *port-list* ] ] packet-stat**

Statystyki pakietów na wybranych portach lub na wszystkich portach.

---

**clear ipv6 mld snooping statistics**

Wyczyść statystyki wszystkich pakietów MLD.

---



# 7 Przykłady konfiguracji

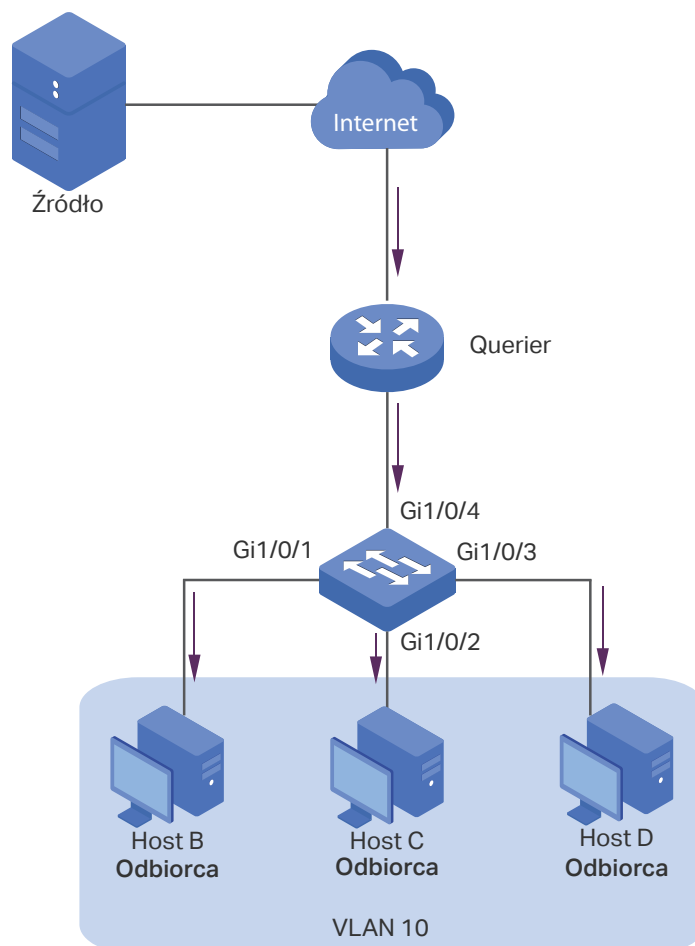
## 7.1 Przykład podstawowej konfiguracji IGMP Snooping

### 7.1.1 Wymagania sieciowe

Host B, host C i host D są w tej samej sieci VLAN przełącznika. Każdy z hostów chce odbierać strumień multicastowy przesłany do grupy multicastowej 225.1.1.1.

Jak pokazano na poniższym schemacie, host B, host C i host D są odpowiednio podłączeni do portu 1/0/1, portu 1/0/2 i portu 1/0/3. Port 1/0/4 to port router, połączony z urządzeniem odpytującym (multicast querier).

Rys. 7-1 Topologia sieci dla podstawowej konfiguracji IGMP Snooping



### 7.1.2 Schemat konfiguracji

- Dodaj trzy porty przynależące i port router do sieci VLAN, a następnie ustaw ich PVID.
- Włącz IGMP Snooping globalnie i w sieci VLAN.

- Włącz IGMP Snooping na portach.

W poniższych podrozdziałach opisano dwa sposoby przeprowadzenia procedury konfiguracji: przez GUI oraz przez CLI.

### 7.1.3 Przez GUI

- 1) Wybierz z menu **L2 FEATURES > VLAN > 802.1Q VLAN > VLAN Config** i kliknij **+ Add** aby wyświetlić poniższą stronę. Utwórz VLAN 10 i dodaj nietagowany port 1/0/1-3 oraz tagowany port 1/0/4 do tej sieci.

Rys. 7-2 Tworzenie VLAN 10

**VLAN Config**

VLAN ID:  (2-4094, format: 2,4-5,8)

VLAN Name:  (1-16 characters)

**Untagged Ports**

Port:  (Format: 1/0/1, input or choose below)

UNIT1 LAGS

Select All

1 2 3 4 5 6 7 8 9 10

Selected  Unselected  Not Available

**Tagged Ports**

Port:  (Format: 1/0/1, input or choose below)

UNIT1 LAGS

Select All

1 2 3 4 5 6 7 8 9 10

- 2) Wybierz z menu **L2 FEATURES > VLAN > 802.1Q VLAN > Port Config**, aby wyświetlić poniższą stronę. Ustaw PVID portów 1/0/1-4 jako 10.

Rys. 7-3 Ustawianie PVID dla portów

Port Config

UNIT1 LAGS

| <input type="checkbox"/>            | Port   | PVID | Ingress Checking | Acceptable Frame Types | LAG | Detail                 |
|-------------------------------------|--------|------|------------------|------------------------|-----|------------------------|
| <input checked="" type="checkbox"/> | 1/0/1  | 10   | Enabled          | Admit All              | --- | <a href="#">Detail</a> |
| <input checked="" type="checkbox"/> | 1/0/2  | 10   | Enabled          | Admit All              | --- | <a href="#">Detail</a> |
| <input checked="" type="checkbox"/> | 1/0/3  | 10   | Enabled          | Admit All              | --- | <a href="#">Detail</a> |
| <input checked="" type="checkbox"/> | 1/0/4  | 10   | Enabled          | Admit All              | --- | <a href="#">Detail</a> |
| <input type="checkbox"/>            | 1/0/5  | 1    | Enabled          | Admit All              | --- | <a href="#">Detail</a> |
| <input type="checkbox"/>            | 1/0/6  | 1    | Enabled          | Admit All              | --- | <a href="#">Detail</a> |
| <input type="checkbox"/>            | 1/0/7  | 3    | Enabled          | Admit All              | --- | <a href="#">Detail</a> |
| <input type="checkbox"/>            | 1/0/8  | 3    | Enabled          | Admit All              | --- | <a href="#">Detail</a> |
| <input type="checkbox"/>            | 1/0/9  | 1    | Enabled          | Admit All              | --- | <a href="#">Detail</a> |
| <input type="checkbox"/>            | 1/0/10 | 1    | Enabled          | Admit All              | --- | <a href="#">Detail</a> |

Total: 10 4 entries selected. Cancel Apply

- 3) Wybierz z menu **L2 FEATURES > Multicast > IGMP Snooping > Global Config**, aby wyświetlić poniższą stronę. W sekcji **Global Config** włącz globalnie IGMP Snooping. Ustaw wersję IGMP jako v3, aby przełącznik mógł przetwarzać wszystkie wersje komunikatów IGMP. Następnie kliknij **Apply**.

Rys. 7-4 Konfiguracja globalna IGMP Snooping

Global Config

IGMP Snooping:  Enable

IGMP Version:  v1  v2  v3

Unknown Multicast Groups:  Forward  Discard

Header Validation:  Enable

Apply

IGMP VLAN Config

VLAN ID

| VLAN ID | IGMP Snooping Status | Fast Leave | Report Suppression | IGMP Snooping Querier | Dynamic Router Ports | Static Router Ports | Forbidden Router Ports | Operation                                    |
|---------|----------------------|------------|--------------------|-----------------------|----------------------|---------------------|------------------------|----------------------------------------------|
| 1       | Disabled             | Disabled   | Disabled           | Disabled              |                      |                     |                        | <a href="#">Edit</a> <a href="#">Refresh</a> |
| 10      | Disabled             | Disabled   | Disabled           | Disabled              |                      |                     |                        | <a href="#">Edit</a> <a href="#">Refresh</a> |

Total: 2

- 4) W sekcji **IGMP VLAN Config** kliknij [Edit](#) przy VLAN 10, aby wyświetlić poniższą stronę. Włącz IGMP Snooping dla VLAN 10.

Rys. 7-5 Włączanie IGMP Snooping dla VLAN 10

**Configure IGMP Snooping for VLAN**

VLAN ID: 10

IGMP Snooping Status:  Enable

Fast Leave:  Enable

Report Suppression:  Enable

Member Port Aging Time: 260 seconds (60-600)

Router Port Aging Time: 300 seconds (60-600)

IGMP Snooping Querier:  Enable

Static Router Ports

- 5) Wybierz z menu **L2 FEATURES > Multicast > IGMP Snooping > Port Config**, aby wyświetlić poniższą stronę. Włącz IGMP Snooping dla portów 1/0/1-4.


Rys. 7-6 Włączanie IGMP Snooping dla portów

Port Config

UNIT1 LAGS

| <input type="checkbox"/>            | Port   | IGMP Snooping | Fast Leave | LAG  |
|-------------------------------------|--------|---------------|------------|------|
| <input checked="" type="checkbox"/> | 1/0/1  | Enabled       | Disabled   | ---  |
| <input checked="" type="checkbox"/> | 1/0/2  | Enabled       | Disabled   | ---  |
| <input checked="" type="checkbox"/> | 1/0/3  | Enabled       | Disabled   | ---  |
| <input checked="" type="checkbox"/> | 1/0/4  | Enabled       | Disabled   | ---  |
| <input type="checkbox"/>            | 1/0/5  | Enabled       | Disabled   | ---  |
| <input type="checkbox"/>            | 1/0/6  | Enabled       | Disabled   | ---  |
| <input type="checkbox"/>            | 1/0/7  | Enabled       | Disabled   | LAG1 |
| <input type="checkbox"/>            | 1/0/8  | Enabled       | Disabled   | LAG1 |
| <input type="checkbox"/>            | 1/0/9  | Enabled       | Disabled   | ---  |
| <input type="checkbox"/>            | 1/0/10 | Enabled       | Disabled   | ---  |

Total: 10 4 entries selected. Cancel Apply

- 6) Kliknij  Save, aby zapisać ustawienia.

## 7.1.4 Przez CLI

- 1) Utwórz VLAN 10.

```
Switch#configure
```

```
Switch(config)#vlan 10
```

```
Switch(config-vlan)#name vlan10
```

```
Switch(config-vlan)#exit
```

- 2) Dodaj port 1/0/1-3 do VLAN 10 i ustaw jego typ łącza jako untagged. Dodaj port 1/0/4 do VLAN 10 i ustaw jego typ łącza jako tagged.

```
Switch(config)#interface range fastEthernet 1/0/1-3
```

```
Switch(config-if-range)#switchport general allowed vlan 10 untagged
```

```
Switch(config-if-range)#exit
```

```
Switch(config)#interface fastEthernet 1/0/4
```

```
Switch(config-if)#switchport general allowed vlan 10 tagged
```

```
Switch(config-if)#exit
```

- 3) Ustaw PVID portu 1/0/1-4 jako 10.

```
Switch(config)#interface range fastEthernet 1/0/1-4
```

```
Switch(config-if-range)#switchport pvid 10
```

```
Switch(config-if-range)#exit
```

- 4) Włącz globalnie IGMP Snooping.

```
Switch(config)#ip igmp snooping
```

- 5) Włącz IGMP Snooping w sieci VLAN 10.

```
Switch(config)#ip igmp snooping vlan-config 10
```

- 6) Włącz IGMP Snooping na porcie 1/0/1-4.

```
Switch(config)#interface range fastEthernet 1/0/1-4
```

```
Switch(config-if-range)#ip igmp snooping
```

```
Switch(config-if-range)#exit
```

- 7) Zapisz ustawienia.

```
Switch(config)#end
```

```
Switch#copy running-config startup-config
```

## Sprawdzanie konfiguracji

Sprawdzanie portów przynależących do VLAN:

```
Switch(config)#show vlan brief
```

| VLAN | Name        | Status | Ports                                                                             |
|------|-------------|--------|-----------------------------------------------------------------------------------|
| 1    | System-VLAN | active | Gi1/0/1, Gi1/0/2, Gi1/0/3, Gi1/0/4,<br>Gi1/0/5, Gi1/0/6, Gi1/0/7, Gi1/0/8,<br>... |

```
10 vlan10 active Gi1/0/1, Gi1/0/2, Gi1/0/3, Gi1/0/4
```

Sprawdzanie stanu IGMP Snooping globalnie, na portach i w sieci VLAN:

```
Switch(config)#show ip igmp snooping
```

```
IGMP Snooping :Enable
```

```
IGMP Version :V3
```

```
Header Validation :Disable
```

```
Global Authentication Accounting :Disable
```

```
Enable Port : Gi1/0/1-4
```

```
Enable VLAN:10
```

## 7.2 Przykład konfiguracji MVR

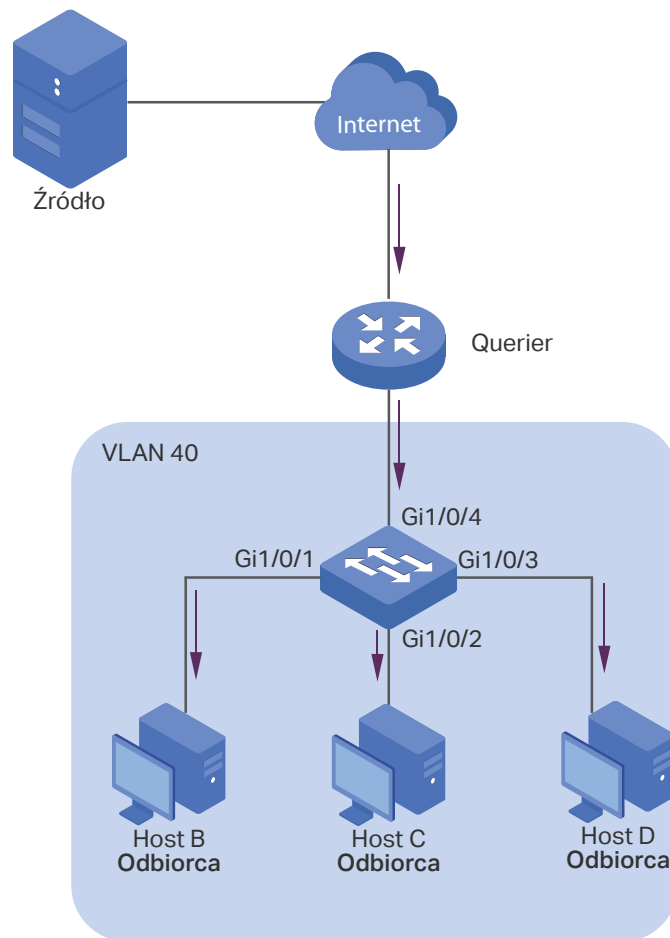
### 7.2.1 Wymagania sieciowe

Host B, host C i host D należą do trzech różnych sieci VLAN przełącznika. Każdy z hostów chce odbierać strumienie multicastowe przesłane do grupy multicastowej 225.1.1.1.

### 7.2.2 Topologia sieci

Jak pokazano na poniższym schemacie, host B, host C i host D są odpowiednio podłączeni do portu 1/0/1, portu 1/0/2 i portu 1/0/3. Port 1/0/1, port 1/0/2 i port 1/0/3 należą odpowiednio do VLAN 10, VLAN 20 i VLAN 30. Port 1/0/4 jest podłączony do sieci multicast w górnej warstwie sieci.

Rys. 7-7 Topologia sieci dla VLAN-u multicastowego



### 7.2.3 Schemat konfiguracji

Ze względu na to, że hosty są w różnych sieciach VLAN, Querier w IGMP Snooping musi powielać strumienie multicastowe dla hostów w każdym VLAN-ie. Aby uniknąć przesyłania powielonych strumieni multicastowych pomiędzy Querier a przełącznikiem, skonfiguruj na przełączniku MVR.

Przełącznik może działać zarówno w trybie kompatybilności MVR lub w trybie dynamicznym MVR. Gdy uruchomisz tryb kompatybilności, skonfiguruj statycznie Querier w celu przesyłania strumieni grupy multicastowej 225.1.1.1 do przełącznika poprzez VLAN multicastowy. Poniższy proces omówimy na przykładzie trybu dynamicznego MVR.

W poniższych podrozdziałach opisano dwa sposoby przeprowadzenia procedury konfiguracji: przez GUI oraz przez CLI.

### 7.2.4 Przez GUI

- 1) Dodaj porty 1/0/1-3 odpowiednio do VLAN 10, VLAN 20 i VLAN 30 jako porty nietagowane i skonfiguruj PVID portu 1/0/1 jako 10, portu 1/0/2 jako 20, portu 1/0/3 jako 30. Upewnij się, że porty 1/0/1-3 wyłącznie należą odpowiednio do VLAN 10, VLAN 20 i VLAN 30. Szczegółowe informacje znajdują się w części *Konfiguracja 802.1Q VLAN*.

Rys. 7-8 Konfiguracja VLAN dla portów 1/0/1-3

| VLAN Config                          |         |             |          |                                             |                          |
|--------------------------------------|---------|-------------|----------|---------------------------------------------|--------------------------|
| <input type="text" value="VLAN ID"/> |         |             |          | <a href="#">+ Add</a>                       | <a href="#">- Delete</a> |
| <input type="checkbox"/>             | VLAN ID | VLAN Name   | Members  | Operation                                   |                          |
| <input type="checkbox"/>             | 1       | System-VLAN | 1/0/4-28 | <a href="#">Edit</a> <a href="#">Delete</a> |                          |
| <input type="checkbox"/>             | 10      | VLAN10      | 1/0/1    | <a href="#">Edit</a> <a href="#">Delete</a> |                          |
| <input type="checkbox"/>             | 20      | VLAN20      | 1/0/2    | <a href="#">Edit</a> <a href="#">Delete</a> |                          |
| <input type="checkbox"/>             | 30      | VLAN30      | 1/0/3    | <a href="#">Edit</a> <a href="#">Delete</a> |                          |
| Total: 4                             |         |             |          |                                             |                          |

Rys. 7-9 PVID dla portu 1/0/1-3

| Port Config              |        |      |                  |                        |     |                        |
|--------------------------|--------|------|------------------|------------------------|-----|------------------------|
| UNIT1                    |        | LAGS |                  |                        |     |                        |
| <input type="checkbox"/> | Port   | PVID | Ingress Checking | Acceptable Frame Types | LAG | Detail                 |
| <input type="checkbox"/> | 1/0/1  | 10   | Enabled          | Admit All              | --- | <a href="#">Detail</a> |
| <input type="checkbox"/> | 1/0/2  | 20   | Enabled          | Admit All              | --- | <a href="#">Detail</a> |
| <input type="checkbox"/> | 1/0/3  | 30   | Enabled          | Admit All              | --- | <a href="#">Detail</a> |
| <input type="checkbox"/> | 1/0/4  | 1    | Enabled          | Admit All              | --- | <a href="#">Detail</a> |
| <input type="checkbox"/> | 1/0/5  | 1    | Enabled          | Admit All              | --- | <a href="#">Detail</a> |
| <input type="checkbox"/> | 1/0/6  | 1    | Enabled          | Admit All              | --- | <a href="#">Detail</a> |
| <input type="checkbox"/> | 1/0/7  | 1    | Enabled          | Admit All              | --- | <a href="#">Detail</a> |
| <input type="checkbox"/> | 1/0/8  | 1    | Enabled          | Admit All              | --- | <a href="#">Detail</a> |
| <input type="checkbox"/> | 1/0/9  | 1    | Enabled          | Admit All              | --- | <a href="#">Detail</a> |
| <input type="checkbox"/> | 1/0/10 | 1    | Enabled          | Admit All              | --- | <a href="#">Detail</a> |
| Total: 10                |        |      |                  |                        |     |                        |

- 2) Wybierz z menu **L2 FEATURES > VLAN > 802.1Q VLAN > VLAN Config** i kliknij [+ Add](#) aby wyświetlić poniższą stronę. Utwórz VLAN 40 i dodaj port 1/0/4 do tej sieci jako port tagowany.



Rys. 7-10 Tworzenie VLAN-u multicastowego

### VLAN Config

VLAN ID:  (2-4094, format: 2,4-5,8)

VLAN Name:  (1-16 characters)

**Untagged Ports**

Port:  (Format: 1/0/1, input or choose below)

**UNIT1**

1
  2
  3
  4
  5

**LAGS**

6
  7
  8
  9
  10

Select All

Selected

Unselected

Not Available

**Tagged Ports**

Port:  (Format: 1/0/1, input or choose below)

**UNIT1**

1
  2
  3
  4
  5

**LAGS**

6
  7
  8
  9
  10

Select All

Cancel
Create

- 3) Wybierz z menu **L2 FEATURES > Multicast > MVR > MVR Config**, aby wyświetlić poniższą stronę. Włącz globalnie MVR i skonfiguruj tryb MVR jako **Dynamic**, a multicast VLAN ID jako **40**.

Rys. 7-11 Konfiguracja globalna MVR

### MVR Config

MVR:  Enable

MVR Mode:  Compatible  Dynamic

Multicast VLAN ID:  (1-4094)

Query Response Time:  tenths of a second (1-100)

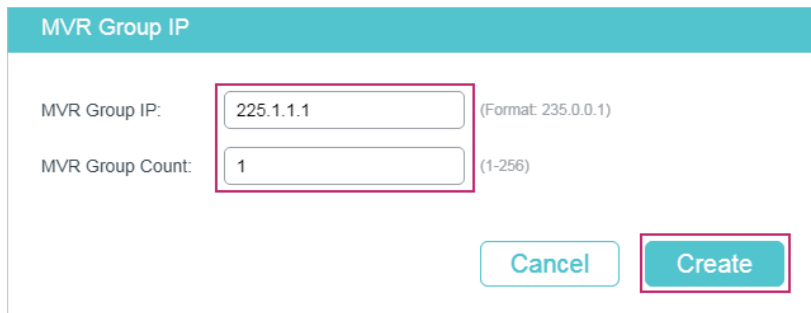
Maximum Multicast Groups: 256

Current Multicast Groups: 0

Apply

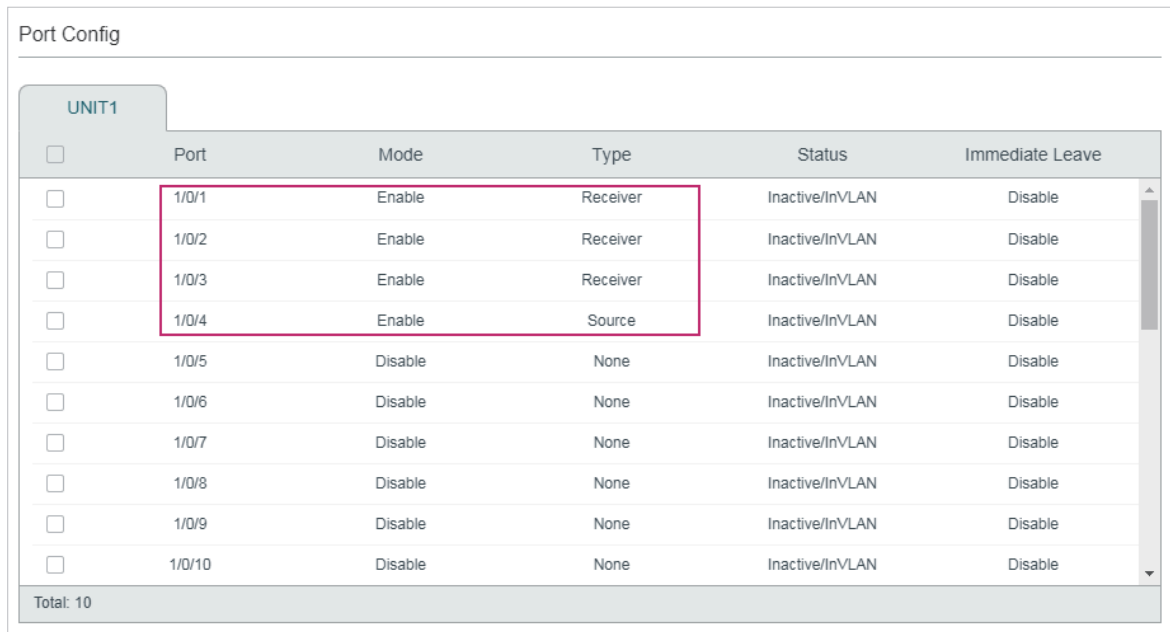
- 4) Wybierz z menu **L2 FEATURES > Multicast > MVR > MVR Group Config** i kliknij  Add aby wyświetlić poniższą stronę. Dodaj grupę multicastową 225.1.1.1 do MVR.

Rys. 7-12 Dodawanie grupy multicastowej do MVR




- 5) Wybierz z menu **L2 FEATURES > Multicast > MVR > Port Config**, aby wyświetlić poniższą stronę. Włącz MVR dla portu 1/0/1-4. Ustaw porty 1/0/1-3 jako **Receiver** i port 1/0/4 jako **Source**.

Rys. 7-13 Konfiguracja MVR dla portów



| <input type="checkbox"/> | Port   | Mode    | Type     | Status          | Immediate Leave |
|--------------------------|--------|---------|----------|-----------------|-----------------|
| <input type="checkbox"/> | 1/0/1  | Enable  | Receiver | Inactive/InVLAN | Disable         |
| <input type="checkbox"/> | 1/0/2  | Enable  | Receiver | Inactive/InVLAN | Disable         |
| <input type="checkbox"/> | 1/0/3  | Enable  | Receiver | Inactive/InVLAN | Disable         |
| <input type="checkbox"/> | 1/0/4  | Enable  | Source   | Inactive/InVLAN | Disable         |
| <input type="checkbox"/> | 1/0/5  | Disable | None     | Inactive/InVLAN | Disable         |
| <input type="checkbox"/> | 1/0/6  | Disable | None     | Inactive/InVLAN | Disable         |
| <input type="checkbox"/> | 1/0/7  | Disable | None     | Inactive/InVLAN | Disable         |
| <input type="checkbox"/> | 1/0/8  | Disable | None     | Inactive/InVLAN | Disable         |
| <input type="checkbox"/> | 1/0/9  | Disable | None     | Inactive/InVLAN | Disable         |
| <input type="checkbox"/> | 1/0/10 | Disable | None     | Inactive/InVLAN | Disable         |

Total: 10

- 6) Kliknij  Save, aby zapisać ustawienia.

## 7.2.5 Przez CLI

- 1) Utwórz VLAN 10, VLAN 20, VLAN 30 i VLAN 40.

```
Switch#configure
```

```
Switch(config)#vlan 10,20,30,40
```

```
Switch(config-vlan)#exit
```

- 2) Dodaj porty 1/0/1-3 odpowiednio do VLAN 10, VLAN 20 i VLAN 30 jako porty nietagowane i ustaw PVID portu 1/0/1 jako 10, portu 1/0/2 jako 20, portu 1/0/3 jako 30. Dodaj port 1/0/4 do VLAN 40 jako port tagowany i ustaw PVID portu 1/0/4 jako 40.

```

Switch(config)#interface fastEthernet 1/0/1
Switch(config-if)#switchport general allowed vlan 10 untagged
Switch(config-if)#switchport pvid 10
Switch(config-if)#exit
Switch(config)#interface fastEthernet 1/0/2
Switch(config-if)#switchport general allowed vlan 20 untagged
Switch(config-if)#switchport pvid 20
Switch(config-if)#exit
Switch(config)#interface fastEthernet 1/0/3
Switch(config-if)#switchport general allowed vlan 30 untagged
Switch(config-if)#switchport pvid 30
Switch(config-if)#exit
Switch(config)#interface fastEthernet 1/0/4
Switch(config-if)#switchport general allowed vlan 40 tagged
Switch(config-if)#switchport pvid 40
Switch(config-if)#exit

```

- 3) Sprawdź, czy porty 1/0/1-3 wyłącznie należą odpowiednio do VLAN 10, VLAN 20 i VLAN 30. Jeśli nie, usuń je z innych VLAN-ów. Domyślnie wszystkie porty należą do VLAN 1, więc konieczne jest ich usunięcie z tej sieci.

```
Switch(config)#show vlan brief
```

| VLAN  | Name        | Status | Ports                                                                             |
|-------|-------------|--------|-----------------------------------------------------------------------------------|
| ----- | -----       | -----  | -----                                                                             |
| 1     | System-VLAN | active | Gi1/0/1, Gi1/0/2, Gi1/0/3, Gi1/0/4,<br>Gi1/0/5, Gi1/0/6, Gi1/0/7, Gi1/0/8,<br>... |
| 10    | VLAN10      | active | Gi1/0/1                                                                           |
| 20    | VLAN20      | active | Gi1/0/2                                                                           |
| 30    | VLAN30      | active | Gi1/0/3                                                                           |
| 40    | VLAN40      | active | Gi1/0/4                                                                           |

```

Switch(config)#interface range fastEthernet 1/0/1-3
Switch(config-if-range)#no switchport general allowed vlan 1

```

```
Switch(config-if-range)#exit
```

- 4) Włącz globalnie MVR i ustaw tryb MVR jako **Dynamic**, a multicast VLAN ID jako **40**. Dodaj grupę multicastową 225.1.1.1 do MVR.

```
Switch(config)#mvr
```

```
Switch(config)#mvr mode dynamic
```

```
Switch(config)#mvr vlan 40
```

```
Switch(config)#mvr group 225.1.1.1 1
```

- 5) Włącz MVR dla portów 1/0/1-4. Ustaw porty 1/0/1-3 jako **Receiver** i port 1/0/4 jako **Source**.

```
Switch(config)#interface range fastEthernet 1/0/1-3
```

```
Switch(config-if-range)#mvr
```

```
Switch(config-if-range)#mvr type receiver
```

```
Switch(config-if-range)#exit
```

```
Switch(config)#interface fastEthernet 1/0/4
```

```
Switch(config-if)#mvr
```

```
Switch(config-if)#mvr type source
```

```
Switch(config-if)#exit
```

- 6) Zapisz ustawienia.

```
Switch(config)#end
```

```
Switch#copy running-config startup-config
```

## Sprawdzanie konfiguracji

Wyświetlanie ogólnych informacji o wszystkich sieciach VLAN:

```
Switch(config)#show vlan brief
```

| VLAN | Name        | Status | Ports                                      |
|------|-------------|--------|--------------------------------------------|
| 1    | System-VLAN | active | Gi1/0/4, Gi1/0/5, Gi1/0/6, Gi1/0/7,<br>... |
| 10   | VLAN10      | active | Gi1/0/1                                    |
| 20   | VLAN20      | active | Gi1/0/2                                    |
| 30   | VLAN30      | active | Gi1/0/3                                    |
| 40   | VLAN40      | active | Gi1/0/4                                    |

Wyświetlanie ogólnych informacji o MVR:

```
Switch(config)#show mvr
```

```
MVR :Enable
MVR Multicast Vlan :40
MVR Max Multicast Groups :256
MVR Current Multicast Groups :1
MVR Global Query Response Time :5 (tenths of sec)
MVR Mode Type :Dynamic
```

Wyświetlanie przynależności do grup MVR:

```
Switch(config)#show mvr members
```

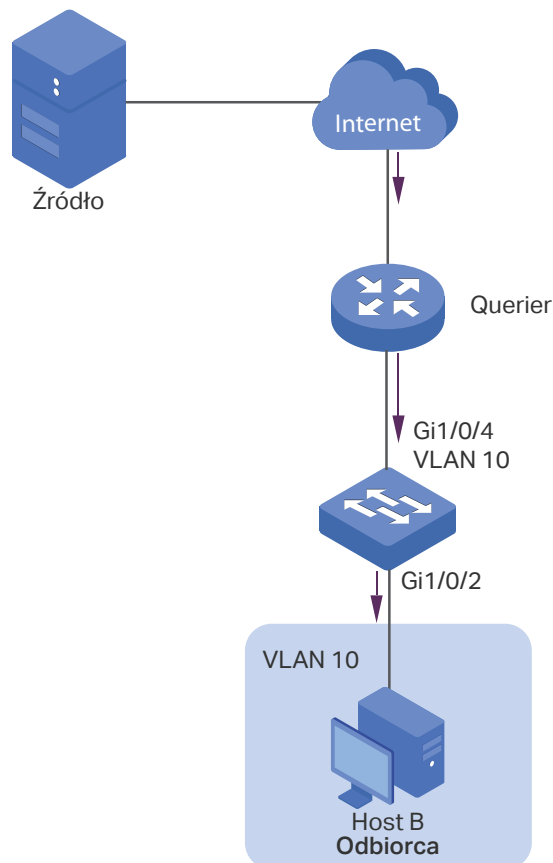
| MVR Group IP | Status | Members |
|--------------|--------|---------|
| -----        | -----  | -----   |
| 225.1.1.1    | active | Gi1/0/4 |

## 7.3 Przykład konfiguracji Unknown Multicast i Fast Leave

### 7.3.1 Wymagania sieciowe

Użytkownik ma problem z opóźnieniami, gdy zmienia kanał w IPTV. Potrzebuje skutecznego rozwiązania. Jak pokazano na poniższym schemacie topologii sieci, port 1/0/4 przełącznika jest podłączony do wyższej warstwy sieci, a port 1/0/2 do hosta B.

Rys. 7-14 Topologia sieci dla Unknow Multicast i Fast Leave



### 7.3.2 Schemat konfiguracji

Po zmianie kanału klient (host B) nadal odbiera nieistotne dane multicastu, dane z poprzedniego kanału i prawdopodobnie także nieznanne dane multicastu, które zwiększają ruch w sieci i skutkują przeciążeniami.

Aby zapobiec odbieraniu nieistotnych danych multicastu przez host B, należy włączyć funkcję Fast Leave na porcie 1/0/2 i skonfigurować przełącznik tak, aby odrzucał nieznanne dane multicastu. W celu zmiany kanału host B wysyła komunikat leave informujący o opuszczeniu kanału. Po włączeniu Fast Leave na porcie 1/0/2 przełącznik będzie odrzucać dane multicastu z poprzedniego kanału, co umożliwi hostowi B odbieranie danych multicastu wyłącznie z nowego kanału oraz wyeliminowanie zakłóceń sieci.

W poniższych podrozdziałach opisano dwa sposoby przeprowadzenia procedury konfiguracji: przez GUI oraz przez CLI.

### 7.3.3 Przez GUI

- 1) Utwórz VLAN 10. Dodaj port 1/0/2 do VLAN jako port nietagowany i port 1/0/4 jako port tagowany. Ustaw PVID obydwu portów jako 10. Szczegółowe informacje znajdują się w części *Konfiguracja 802.1Q VLAN*.
- 2) Wybierz z menu **L2 FEATURES > Multicast > IGMP Snooping > Global Config**, aby wyświetlić poniższą stronę. W sekcji **Global Config** włącz globalnie IGMP Snooping i ustaw Unknown Multicast Groups jako **Discard**.

Rys. 7-15 Konfiguracja globalna IGMP Snooping

**Global Config**

---

IGMP Snooping:  Enable

IGMP Version:  v1  v2  v3

Unknown Multicast Groups:  Forward  Discard

Header Validation:  Enable

Apply

---

**IGMP VLAN Config**

| VLAN ID  | IGMP Snooping Status | Fast Leave | Report Suppression | IGMP Snooping Querier | Dynamic Router Ports | Static Router Ports | Forbidden Router Ports | Operation                                                      |
|----------|----------------------|------------|--------------------|-----------------------|----------------------|---------------------|------------------------|----------------------------------------------------------------|
| 1        | Disabled             | Disabled   | Disabled           | Disabled              |                      |                     |                        |                                                                |
| 10       | Disabled             | Disabled   | Disabled           | Disabled              |                      |                     |                        | <span style="border: 1px solid #00a651; padding: 2px;"></span> |
| Total: 2 |                      |            |                    |                       |                      |                     |                        |                                                                |

**Uwaga:**

Unknown Multicast jest wspólnym ustawieniem dla IGMP Snooping i MLD Snooping, dlatego konieczne jest jednoczesne włączenie globalne MLD Snooping na stronie **L2 FEATURES > Multicast > MLD Snooping > Global Config**.

- 3) W sekcji **IGMP VLAN Config** kliknij przy VLAN 10, aby wyświetlić poniższą stronę. Włącz IGMP Snooping dla VLAN 10.

Rys. 7-16 Włączanie IGMP Snooping dla VLAN 10

**Configure IGMP Snooping for VLAN**

---

VLAN ID: 10

IGMP Snooping Status:  Enable

Fast Leave:  Enable

Report Suppression:  Enable

Member Port Aging Time:  seconds (60-600)

Router Port Aging Time:  seconds (60-600)

IGMP Snooping Querier:  Enable

Static Router Ports

- 4) Wybierz z menu **L2 FEATURES > Multicast > IGMP Snooping > Port Config**, aby wyświetlić poniższą stronę. Włącz IGMP Snooping na porcie 1/0/2 i 1/0/4 oraz włącz Fast Leave na porcie 1/0/2.


Rys. 7-17 Konfiguracja IGMP Snooping na portach

Port Config

UNIT1 LAGS

| <input type="checkbox"/>            | Port   | IGMP Snooping | Fast Leave | LAG |
|-------------------------------------|--------|---------------|------------|-----|
| <input type="checkbox"/>            | 1/0/1  | Enabled       | Disabled   | --- |
| <input checked="" type="checkbox"/> | 1/0/2  | Enabled       | Enabled    | --- |
| <input type="checkbox"/>            | 1/0/3  | Enabled       | Disabled   | --- |
| <input type="checkbox"/>            | 1/0/4  | Enabled       | Disabled   | --- |
| <input type="checkbox"/>            | 1/0/5  | Enabled       | Disabled   | --- |
| <input type="checkbox"/>            | 1/0/6  | Enabled       | Disabled   | --- |
| <input type="checkbox"/>            | 1/0/7  | Enabled       | Disabled   | --- |
| <input type="checkbox"/>            | 1/0/8  | Enabled       | Disabled   | --- |
| <input type="checkbox"/>            | 1/0/9  | Enabled       | Disabled   | --- |
| <input type="checkbox"/>            | 1/0/10 | Enabled       | Disabled   | --- |

Total: 10 1 entry selected. Cancel Apply

- 5) Kliknij , aby zapisać ustawienia.

### 7.3.4 Przez CLI

- 1) Włącz globalnie IGMP Snooping i MLD Snooping.

```
Switch#configure
```

```
Switch(config)#ip igmp snooping
```

```
Switch(config)#ipv6 mld snooping
```

- 2) Ustaw globalnie Unknown Multicast Groups jako Discard.

```
Switch(config)#ip igmp snooping drop-unknown
```

- 3) Włącz IGMP Snooping na porcie 1/0/2 i włącz Fast Leave. Włącz IGM Snooping na porcie 1/0/4.

```
Switch(config)#interface fastEthernet 1/0/2
```

```
Switch(config-if)#ip igmp snooping
```

```
Switch(config-if)#ip igmp snooping immediate-leave
```

```
Switch(config-if)#exit
```

```
Switch(config)#interface fastEthernet 1/0/4
```

```
Switch(config-if)#ip igmp snooping
```

```
Switch(config-if)#exit
```

- 4) Włącz IGMP Snooping w sieci VLAN 10.

```
Switch(config)#ip igmp snooping vlan-config 10
```



5) Zapisz ustawienia.

```
Switch(config)#end
```

```
Switch#copy running-config startup-config
```

## Sprawdzanie konfiguracji

Wyświetlanie globalnych ustawień IGMP Snooping:

```
Switch(config)#show ip igmp snooping
```

```
IGMP Snooping :Enable
```

```
IGMP Version :V3
```

```
Unknown Multicast :Discard
```

...

```
Enable Port: Gi1/0/1-28
```

```
Enable VLAN:10
```

Wyświetlanie ustawień IGMP Snooping na porcie 1/0/2:

```
Switch(config)#show ip igmp snooping interface fastEthernet 1/0/2 basic-config
```

```
Port IGMP-Snooping Fast-Leave
```

```

```

```
Gi1/0/2 enable enable
```

## 7.4 Przykład konfiguracji filtrowania pakietów multicastu

### 7.4.1 Wymagania sieciowe

Host B, host C i host D należą do tej samej podsieci. Host C i host D odbierają tylko dane multicastu przesłane na adres 225.0.0.1, natomiast host B odbiera wszystkie dane multicastu oprócz tych, które zostały przesłane z adresu 225.0.0.2.

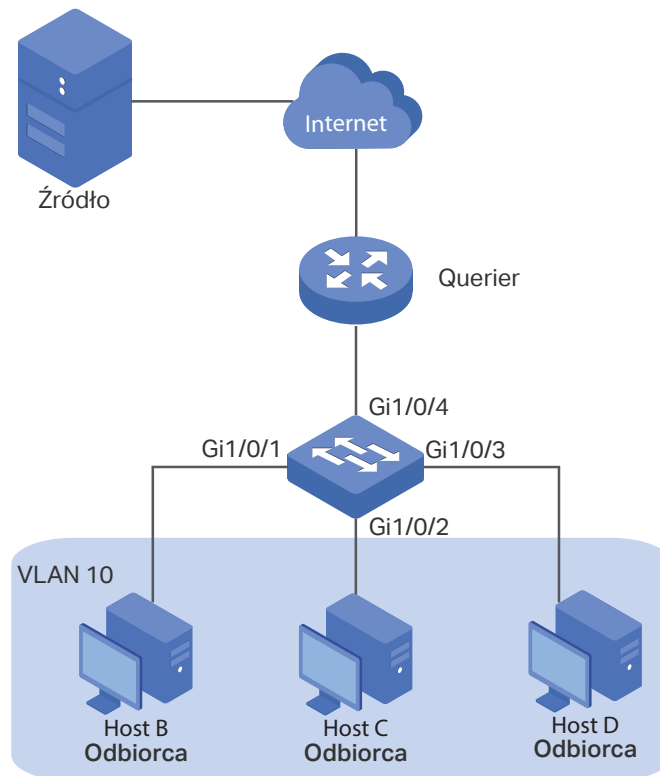
### 7.4.2 Schemat konfiguracji

Korzystając z funkcji do zarządzania grupami multicastowymi oraz mechanizmu białej i czarnej listy (wiązanie profili), przełącznik może zezwolić na dołączanie tylko określonych portów przynależących do określonych grup multicastowych lub odmówić tylko określonym portom przynależącym do określonych grup multicastowych. Ta funkcja filtrowania dostępna jest po utworzeniu profilu i następnym powiązaniu go z odpowiednimi portami przynależącymi.

### 7.4.3 Topologia sieci

Jak pokazano na poniższym schemacie topologii sieci, host B jest podłączony do portu 1/0/1, host C do portu 1/0/2, a host D do portu 1/0/3. Każdy z nich należy do VLAN 10.

Rys. 7-18 Topologia sieci dla filtrowania pakietów multicastu



W poniższych podrozdziałach opisano dwa sposoby przeprowadzenia procedury konfiguracji: przez GUI oraz przez CLI.

#### 7.4.4 Przez GUI

- 1) Utwórz VLAN 10. Dodaj porty 1/0/1-3 do tej sieci jako porty nietagowane i port 1/0/4 jako port tagowany. Ustaw PVID tych czterech portów jako 10. Szczegółowe informacje znajdują się w części *Konfiguracja 802.1Q VLAN*.
- 2) Wybierz z menu **L2 FEATURES > Multicast > IGMP Snooping > Global Config**, aby wyświetlić poniższą stronę. W sekcji **Global Config** włącz globalnie IGMP Snooping.

Rys. 7-19 Włączanie globalne IGMP Snooping

### Global Config

---

IGMP Snooping:  Enable

IGMP Version:  v1  v2  v3

Unknown Multicast Groups:  Forward  Discard

Header Validation:  Enable

Apply

---

### IGMP VLAN Config

| VLAN ID  | IGMP Snooping Status | Fast Leave | Report Suppression | IGMP Snooping Querier | Dynamic Router Ports | Static Router Ports | Forbidden Router Ports | Operation                                                                         |
|----------|----------------------|------------|--------------------|-----------------------|----------------------|---------------------|------------------------|-----------------------------------------------------------------------------------|
| 1        | Disabled             | Disabled   | Disabled           | Disabled              |                      |                     |                        | <a href="#">✎</a> <a href="#">🔍</a>                                               |
| 10       | Disabled             | Disabled   | Disabled           | Disabled              |                      |                     |                        | <span style="border: 1px solid #00a651; padding: 2px;">✎</span> <a href="#">🔍</a> |
| Total: 2 |                      |            |                    |                       |                      |                     |                        |                                                                                   |

- 3) W sekcji **IGMP VLAN Config** kliknij [✎](#) przy VLAN 10, aby wyświetlić poniższą stronę. Włącz IGMP Snooping dla VLAN 10.

Rys. 7-20 Włączanie IGMP Snooping dla VLAN 10

### Configure IGMP Snooping for VLAN

VLAN ID: 10

IGMP Snooping Status:  Enable

Fast Leave:  Enable

Report Suppression:  Enable

Member Port Aging Time:  seconds (60-600)

Router Port Aging Time:  seconds (60-600)

IGMP Snooping Querier:  Enable

Static Router Ports

- 4) Wybierz z menu **L2 FEATURES > Multicast > IGMP Snooping > Port Config**, aby wyświetlić poniższą stronę.

Rys. 7-21 Włączanie IGMP Snooping na porcie

Port Config

UNIT1 LAGS

| <input type="checkbox"/>            | Port   | IGMP Snooping | Fast Leave | LAG  |
|-------------------------------------|--------|---------------|------------|------|
| <input checked="" type="checkbox"/> | 1/0/1  | Enabled       | Disabled   | ---  |
| <input checked="" type="checkbox"/> | 1/0/2  | Enabled       | Disabled   | ---  |
| <input checked="" type="checkbox"/> | 1/0/3  | Enabled       | Disabled   | ---  |
| <input checked="" type="checkbox"/> | 1/0/4  | Enabled       | Disabled   | ---  |
| <input type="checkbox"/>            | 1/0/5  | Enabled       | Disabled   | ---  |
| <input type="checkbox"/>            | 1/0/6  | Enabled       | Disabled   | ---  |
| <input type="checkbox"/>            | 1/0/7  | Enabled       | Disabled   | LAG1 |
| <input type="checkbox"/>            | 1/0/8  | Enabled       | Disabled   | LAG1 |
| <input type="checkbox"/>            | 1/0/9  | Enabled       | Disabled   | ---  |
| <input type="checkbox"/>            | 1/0/10 | Enabled       | Disabled   | ---  |

Total: 10 4 entries selected. Cancel Apply

- 5) Wybierz z menu **L2 FEATURES > Multicast > Multicast Filtering > IPv4 Profile** i kliknij **+ Add**, aby wyświetlić poniższą stronę. Utwórz Profile 1, ustaw tryb jako **Permit**, powiąż profil z portami 1/0/2-3 i ustaw adres IP filtrowania pakietów mutlicastu jako 225.0.0.1. Następnie kliknij **Back**, aby wrócić do strony **IPv4 Profile Table**.

Rys. 7-22 Konfiguracja profilu filtrowania dla hosta C i hosta D

General Config

Profile ID:  (1-999)

Mode:  Permit  Deny

IP-Range

+ Add - Delete

| <input type="checkbox"/> | Index | Start IP Address | End IP Address | Operation |
|--------------------------|-------|------------------|----------------|-----------|
| <input type="checkbox"/> | 1     | 225.0.0.1        | 225.0.0.1      |           |

Total: 1

Bind Ports

UNIT1                      LAGS

Selected    Unselected    Not Available

- 6) Kliknij ponownie Add , aby wyświetlić poniższą stronę. Utwórz Profile 2, ustawa tryb jako **Deny**, powiąż profil z portem 1/0/1 i ustaw adres IP filtrowania pakietów multicastu jako 225.0.0.2.

Rys. 7-23 Konfiguracja profilu filtrowania dla hosta B

General Config

Profile ID:  (1-999)

Mode:  Permit  Deny

IP-Range

+ Add - Delete

| <input type="checkbox"/> | Index | Start IP Address | End IP Address | Operation |
|--------------------------|-------|------------------|----------------|-----------|
| <input type="checkbox"/> | 1     | 225.0.0.2        | 225.0.0.2      |           |

Total: 1

Bind Ports

UNIT1                      LAGS

Selected   
 Unselected   
 Not Available

7) Kliknij **Save**, aby zapisać ustawienia.

## 7.4.5 Przez CLI

1) Utwórz VLAN 10.

```
Switch#configure
```

```
Switch(config)#vlan 10
```

```
Switch(config-vlan)#name vlan10
```

```
Switch(config-vlan)#exit
```

2) Dodaj porty 1/0/1-3 do VLAN 10 i ustaw typ łącza jako untagged. Dodaj port 1/0/4 do VLAN 10 i ustaw typ łącza jako tagged.

```
Switch(config)#interface range fastEthernet 1/0/1-3
```

```
Switch(config-if-range)#switchport general allowed vlan 10 untagged
```

```
Switch(config-if-range)#exit
```

```
Switch(config)#interface fastEthernet 1/0/4
```

```
Switch(config-if)#switchport general allowed vlan 10 tagged
```

```
Switch(config-if)#exit
```

- 3) Ustaw PVID portów 1/0/1-4 jako 10.

```
Switch(config)#interface range fastEthernet 1/0/1-4
```

```
Switch(config-if-range)#switchport pvid 10
```

```
Switch(config-if-range)#exit
```

- 4) Włącz globalnie IGMP Snooping.

```
Switch(config)#ip igmp snooping
```

- 5) Włącz IGMP Snooping w sieci VLAN 10.

```
Switch(config)#ip igmp snooping vlan-config 10
```

- 6) Włącz IGMP Snooping na portach 1/0/1-4.

```
Switch(config)#interface range fastEthernet 1/0/1-4
```

```
Switch(config-if-range)#ip igmp snooping
```

```
Switch(config-if-range)#exit
```

- 7) Utwórz Profile 1, ustaw tryb jako permit i dodaj zakres adresów IP, których zarówno adres początkowy, jak i adres końcowy będzie mieć wartość 225.0.0.1.

```
Switch(config)#ip igmp profile 1
```

```
Switch(config-igmp-profile)#permit
```

```
Switch(config-igmp-profile)#range 225.0.0.1 225.0.0.1
```

```
Switch(config-igmp-profile)#exit
```

- 8) Powiąż Profile 1 z portem 1/0/2 i portem 1/10/3.

```
Switch(config)#interface range fastEthernet 1/0/2-3
```

```
Switch(config-if-range)#ip igmp filter 1
```

```
Switch(config-if-range)#exit
```

- 9) Utwórz Profile 2, ustaw tryb jako deny i dodaj zakres adresów IP, których zarówno adres początkowy, jak i adres końcowy będzie mieć wartość 225.0.0.2.

```
Switch(config)#ip igmp profile 2
```

```
Switch(config-igmp-profile)#deny
```

```
Switch(config-igmp-profile)#range 225.0.0.2 225.0.0.2
```

```
Switch(config-igmp-profile)#exit
```

- 10) Powiąż Profile 2 z portem 1/0/1.

```
Switch(config)#interface fastEthernet 1/0/1
```

```
Switch(config-if)#ip igmp filter 2
```

```
Switch(config-if)#exit
```

11) Zapisz ustawienia.

```
Switch(config)#end
```

```
Switch#copy running-config startup-config
```

### Sprawdzanie konfiguracji

Wyświetlanie globalnych ustawień IGMP Snooping:

```
Switch(config)#show ip igmp snooping
```

```
IGMP Snooping :Enable
```

```
IGMP Version :V3
```

```
...
```

```
Enable Port:Gi1/0/1-4
```

```
Enable VLAN:10
```

Wyświetlanie wszystkich powiązań profili:

```
Switch(config)#show ip igmp profile
```

```
IGMP Profile 1
```

```
 permit
```

```
 range 225.0.0.1 225.0.0.1
```

```
 Binding Port(s)
```

```
 Gi1/0/2-3
```

```
IGMP Profile 2
```

```
 deny
```

```
 range 225.0.0.2 225.0.0.2
```

```
 Binding Port(s)
```

```
 Gi1/0/1
```



# Część 13

## Konfiguracja Spanning Tree

### ROZDZIAŁY

1. Spanning Tree
2. Konfiguracja STP/RSTP
3. Konfiguracja MSTP
4. Konfiguracja zabezpieczeń STP
5. Przykład konfiguracji MSTP

# 1 Spanning Tree

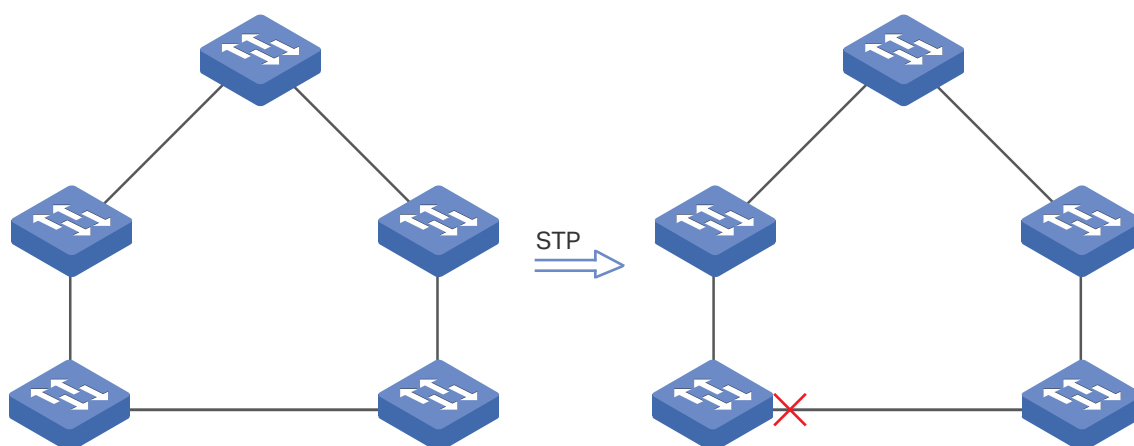
## 1.1 Informacje ogólne

### STP

STP (Spanning Tree Protocol) to protokół warstwy 2, który zapobiega powstawaniu pętli w sieci. Jak pokazano na Rys. 1-1, STP pomaga:

- w blokowaniu określonych portów przełączników w celu stworzenia topologii sieci wykluczającej powstawanie pętli;
- w wykrywaniu zmian w topologii sieci i automatycznym tworzeniu nowej topologii, wykluczającej powstawanie pętli.

Rys. 1-1 Funkcja STP



### RSTP

RSTP (Rapid Spanning Tree Protocol) oferuje te same funkcjonalności co STP. Zapewnia jednak znacznie szybszą konwergencję spanning tree.

### MSTP

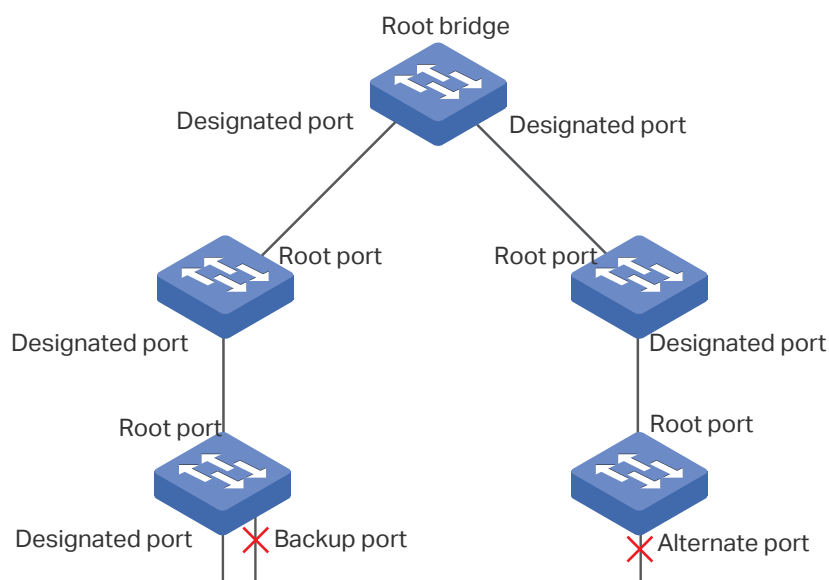
MSTP (Multiple Spanning Tree Protocol) także zapewnia szybką konwergencję spanning tree (drzewa rozpinającego), tak samo jako RSTP. MST umożliwia jednak także mapowanie VLAN-ów do innych drzew rozpinających (instancje MST), a ruch w różnych VLAN-ach jest przesyłany odpowiednio wzdłuż ich ścieżek, co zapewnia równowagę obciążenia pasma.

## 1.2 Podstawowe pojęcia

### 1.2.1 Podstawowe pojęcia STP/RSTP

W tym rozdziale omówimy podstawowe pojęcia związane z STP/RSTP, bazując na poniższej topologii sieci.

Rys. 1-2 Topologia STP/RSTP



#### Root Bridge

Root bridge (korzeń) to główny przełącznik drzewa rozpinającego. Wybierany jest na podstawie najniższego bridge ID. Każde drzewo rozpinające ma tylko jeden root bridge.

#### Bridge ID

Bridge ID to identyfikator, na podstawie którego wybierany jest root bridge. Składa się z 2-bajtowego priorytetu i 6-bajtowego adresu MAC. Priorytet może być skonfigurowany na przełączniku ręcznie. Przełącznik o najniższym priorytecie obejmuje rolę root bridge. Jeśli priorytety przełączników są takie same, o wyborze na root bridge decyduje najniższy adres MAC.

#### Role portów

- Root Port

Root port (port główny) wybierany jest na przełączniku, który nie jest urządzeniem root bridge, ale który może zapewnić do niego najkrótszą ścieżkę. Każdy z takich przełączników ma tylko jeden root port.

- Designated Port

Designated port (port desygnowany) wybierany jest w każdym segmencie sieci LAN na podstawie najkrótszej ścieżki z danego LAN-u do urządzenia root bridge.

- Alternate Port

Jeśli port nie zostanie wybrany na designated port, ponieważ odbiera lepsze ramki BPDU wysyłane z innego przełącznika, staje się alternate port (portem alternatywnym).

W przypadku RSTP/MSTP alternate port stanowi port zapasowy dla root port. Jest on zablokowany, gdy root port działa prawidłowo, Natomiast gdy root port ulegnie awarii, alternate port stanie się nowym root port.

W przypadku STP alternate port jest zawsze zablokowany.

- Backup Port

Jeśli port nie zostanie wybrany na designated port, ponieważ odbiera lepsze ramki BPDU wysyłane z przełącznika, do którego należy, staje się backup port (portem zapasowym).

W przypadku RSTP/MSTP backup port jest portem zapasowym designated port. Jest on zablokowany, gdy designated port działa prawidłowo. Natomiast gdy root port ulegnie awarii, backup port stanie się nowym designated port.

W przypadku STP backup port jest zawsze zablokowany.

- Disable Port

Odłączony port z włączoną funkcją spanning tree.

## Stany portów

Zasadniczo w STP uwzględnia się następujące stany portów: Blocking, Listening, Learning, Forwarding i Disabled.

- Blocking (stan blokowania)

W tym stanie port odbiera i wysyła ramki BPDU. Inne pakiety są odrzucane.

- Listening (stan nasłuchiwania)

W tym stanie port odbiera i wysyła ramki BPDU. Inne pakiety są odrzucane.

- Learning (uczenie się adresów MAC)

W tym stanie port odbiera i wysyła ramki BPDU. Odbiera także pakiety innych użytkowników w celu aktualizacji ich tablicy adresów MAC, ale nie przesyła ich dalej.

- Forwarding (stan przekazywania)

W tym stanie port odbiera i wysyła ramki BPDU. Odbiera także pakiety innych użytkowników w celu aktualizacji ich tablicy adresów MAC i przesyła je dalej.

- Disabled (stan wyłączenia)

W tym stanie port nie jest aktywnym elementem drzewa rozpinającego i odrzuca wszystkie pakiety, które otrzymuje.

W RSTP/MSTP uwzględnia się następujące stany portów: Discarding, Learning i Forwarding. Stan Discarding to kombinacja stanu Blocking STP, Stany Listening i Disabled oraz Learning i Forwarding odpowiadają dokładnie wyszczególnionym dla STP stanom Learning i Forwarding.

W przypadku przełączników TP-Link uwzględnia się następujące stany portów: Blocking, Learning, Forwarding i Disconnected.

- Blocking

W tym stanie port odbiera i wysyła ramki BPDU. Inne pakiety są odrzucane.

- Learning

W tym stanie port odbiera i wysyła ramki BPDU. Odbiera także pakiety innych użytkowników w celu aktualizacji ich tablicy adresów MAC, ale nie przesyła ich dalej.

- Forwarding

W tym stanie port odbiera i wysyła ramki BPDU. Odbiera także pakiety innych użytkowników w celu aktualizacji ich tablicy adresów MAC i przesyła je dalej.

- Disconnected

W tym stanie port ma włączoną funkcję spanning tree, ale nie jest podłączony do żadnego urządzenia.

## Path Cost

Path cost (koszt ścieżki) oznacza prędkość łącza danego portu. Im niższa jest ta wartość, tym wyższą port ma prędkość.

Path cost może być skonfigurowany ręcznie na każdym z portów. Jeśli tak się nie stanie, wartość ta zostanie automatycznie obliczona zgodnie z wartościami domyślnymi:

Tabela 1-1 Domyślne wartości kosztu ścieżki

| Prędkość łącza | Wartość path cost |
|----------------|-------------------|
| 10Mb/s         | 2,000,000         |
| 100Mb/s        | 200,000           |
| 1Gb/s          | 20,000            |
| 10Gb/s         | 2,000             |

## Root Path Cost

Root path cost (koszt ścieżki głównej) to ogólny koszt ścieżek prowadzących od urządzenia root bridge do innych przełączników. Gdy urządzenie root bridge wysyła ramkę BPDU, wartością root path cost jest 0. Gdy przełącznik odbiera tę ramkę BPDU, root path cost wzrasta proporcjonalnie do path cost portu odbierającego. Następnie tworzy się nowa ramka BPDU z nowym kosztem ścieżki, która zostaje przekazana przełącznikowi odbierającemu. Wartość ogólnego kosztu ścieżki głównej wzrasta wraz z rozprzestrzenianiem się ramek BPDU.

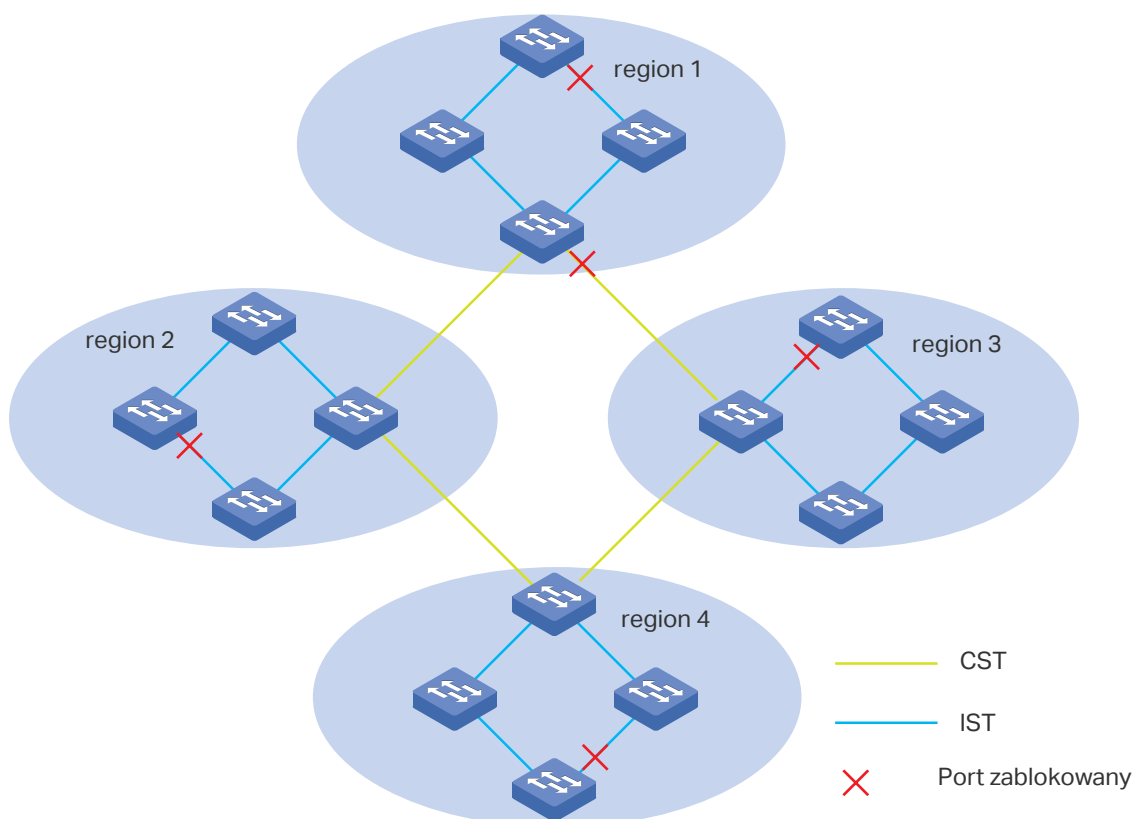
## BPDU

BPDU jest to rodzaj pakietu, który jest wykorzystywany do tworzenia i utrzymywania topologii spanning tree. Ramki BPDU (Bridge Protocol Data Unit) zawierają dużo informacji, w tym bridge ID, root path cost, priorytet portu itp. Przełączniki udostępniają te informacje, aby pomóc w ustaleniu topologii spanning tree.

### 1.2.2 Podstawowe pojęcia MSTP

Protokół MSTP, zgodny z STP and RSTP, opiera się na tych samych podstawowych elementach co STP i RSTP. W tym rozdziale omówimy pojęcia stosowane wyłącznie w przypadku MSTP, bazując na poniższej topologii sieci.

Rys. 1-3 Topologia MSTP



## MST region

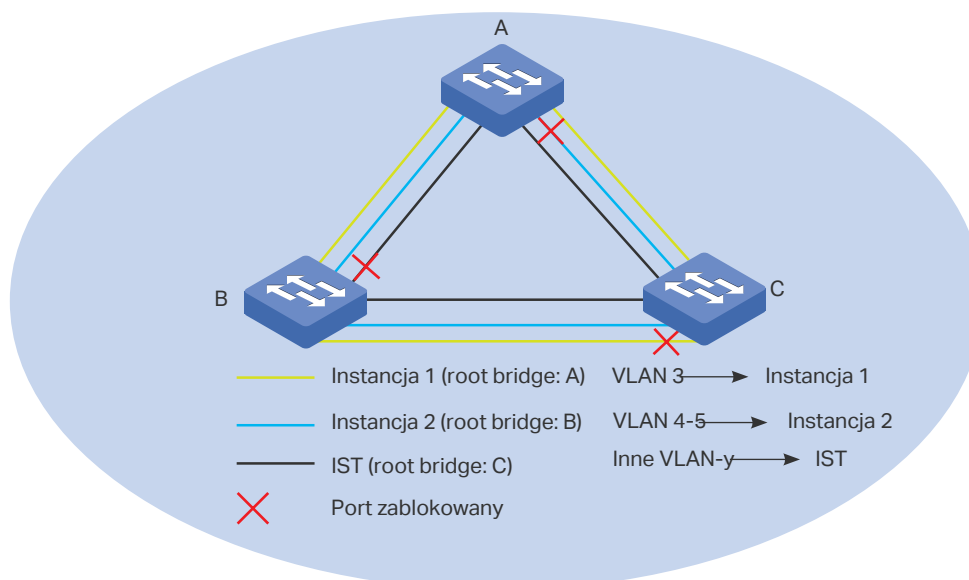
MST region (region MST) składa się z wielu połączonych ze sobą przełączników. Za przynależące do tego samego regionu uważa się przełączniki, które mają takie same cechy, w tym:

- taką samą nazwę regionu;
- taką samą poziom weryfikacji;
- takie samo mapowanie VLAN-instancja.

## MST Instance

MST instance (instancja MST) to drzewo rozpinające funkcjonujące w regionie MST. W jednym regionie MST można ustanowić wiele instancji MST i są one od siebie niezależne. Jak pokazano na Rys. 1-4, w regionie są trzy instancje, a każda z instancji ma swoje własne urządzenie root bridge.

Rys. 1-4 Region MST



## VLAN-Instance Mapping

VLAN-Instance Mapping (mapowanie VLAN-instancja) określa relację mapowania pomiędzy VLAN-ami a instancjami. Do tej samej instancji mapowanych może być wiele VLAN-ów, ale dany VLAN może być mapowany tylko do jednej instancji. Jak pokazano na Rys. 1-4, VLAN 3 mapowany jest do instancji 1, VLAN 4 i VLAN 5 mapowane są do instancji 2, a inne VLAN-y mapowane są do IST.

## IST

Internal Spanning Tree (IST) jest to specjalna instancja MST, której ID wynosi 0. Domyślnie wszystkie VLAN-y mapowane są do IST.

## CST

Common Spanning Tree (CST) to drzewo rozpinające, które łączy wszystkie regiony MST. Jak pokazano na Rys. 1-3, regiony od 1 do 4 połączone są CST.

## CIST

Common and Internal Spanning Tree (CIST) to połączenie IST i CST. CIST to drzewo rozpinające, które łączy wszystkie przełączniki w sieci.

## 1.3 STP Security

STP Security to zabezpieczenia, które zapobiegają pętlom wynikającym z nieprawidłowych ustawień lub ataków na ramki BPDU. Zabezpieczenia te uwzględniają następujące funkcje: Loop Protect, Root Protect, BPDU Protect, BPDU Filter i TC Protect.

### » Loop Protect

Funkcja Loop Protect służy do zapobiegania pętlom spowodowanym przeciążeniem łącza lub jego awarią. Zaleca się włączyć tę funkcję na portach root i alternate.

Jeśli przełącznik nie może odbierać ramek BPDU z powodu przeciążenia lub awarii łącza, root port staje się designated port, a alternate port zmienia stan na Forwarding, co prowadzi do powstawania pętli.

Jeśli funkcja Loop Protect jest włączona, port tymczasowo zmieni swój stan na Blocking, gdy przestanie otrzymywać ramki BPDU. Gdy łącze zacznie działać prawidłowo, port powróci do swojego normalnego stanu, aby zapobiegać pętlom.

### » Root Protect

Funkcja Root Protect służy do ochrony pozycji urządzenia root bridge. Zaleca się włączyć tę funkcję na portach designated urządzenia root bridge.

Zasadniczo urządzenie root bridge traci swoją pozycję, gdy otrzyma ramki BPDU o wyższym priorytecie w wyniku nieprawidłowej konfiguracji ustawień lub złośliwego ataku. W takim wypadku drzewo rozpinające zostanie odtworzone, a ruch przekazywany poprzez szybkie łącza zostanie poprowadzony przez łącza o niskiej prędkości.

Jeśli funkcja root protect jest włączona, gdy port otrzyma ramki BPDU o wyższym priorytecie, zmieni tymczasowo swój stan na Blocking. Po dwukrotnym opóźnieniu przekazywania, jeśli port nie odbierze żadnych ramek BPDU o wyższym priorytecie, powróci do swojego normalnego stanu.

### » BPDU Protect

Funkcja BPDU Protect zapobiega odbieraniu ramek BPUD przez port. Zaleca się włączyć tę funkcję na portach brzegowych.



Zwykle porty brzegowe nie odbierają ramek BPDU, ale jeśli użytkownik przeprowadzi złośliwy atak na przełącznik poprzez wysłanie ramek BPDU, system automatycznie skonfiguruje te porty jako porty inne niż brzegowe i odtworzy drzewo rozpinające.

Jeśli funkcja BPDU protect jest włączona, port brzegowy zostanie odłączony, gdy otrzyma ramki BPDU i zgłosi to zdarzenie do administratora. Tylko administrator może go w takim wypadku przywrócić do działania.

#### » BPDU Filter

Funkcja BPDU filter służy zapobieganiu BPDU flooding w sieci. Zaleca się włączyć tę funkcję na portach brzegowych.

Gdy przełącznik otrzymuje złośliwe ramki BPDU, przekazuje te ramki do innych przełączników w sieci, a drzewo rozpinające ulega ciągłemu odtworzeniu. W takim wypadku przełącznik zbyt mocno obciąża procesor lub stan protokołu ramek BPDU jest nieprawidłowy.

Jeśli funkcja BPDU filter jest włączona, port nie odbiera ani nie przekazuje ramek BPDU, ale wysyła swoje własne ramki BPDU, uniemożliwiając w ten sposób zaatakowanie przełącznika przez ramki BPDU.

#### » TC Protect

Funkcja TC Protect zapobiega ciągłemu usuwaniu wpisów adresów MAC przez przełącznik. Zaleca się włączyć tę funkcję na portach przełączników niebędących przełącznikiem głównym.

Przełącznik usuwa wpisy adresów MAC po otrzymaniu pakietów TC-BPDU (pakiety, które zgłaszają zmiany w topologii sieci). Jeśli użytkownik przeprowadzi złośliwy atak na przełącznik, wysyłając mu w krótkim czasie dużą liczbę pakietów TC-BPDU, przełącznik zajmie się usuwaniem wpisów adresów MAC, co może negatywnie wpłynąć na wydajność i stabilność sieci.

Jeśli funkcja TC protect jest włączona, gdy liczba odebranych pakietów TC-BPDU przekroczy maksymalną wartość TC threshold (progu TC), przełącznik nie będzie usuwać wpisów adresów MAC w cyklu ochrony TC.

# 2 Konfiguracja STP/RSTP

Aby przeprowadzić konfigurację STP/RSTP, wykonaj poniższe kroki:

- 1) Skonfiguruj parametry STP/RSTP na portach.
- 2) Skonfiguruj STP/RSTP globalnie.
- 3) Sprawdź ustawienia STP/RSTP.

## Wskazówki dotyczące konfiguracji

- Przed konfiguracją drzewa rozpinającego (spanning tree) trzeba koniecznie jasno zaznaczyć, jaka rola przypisana jest każdemu przełącznikowi w drzewie rozpinającym.
- Aby zapobiec migotaniu sieci (ang. flapping) spowodowanemu zmianą parametrów STP/RSTP, po skonfigurowaniu odpowiednich parametrów zaleca się globalne włączenie funkcji STP/RSTP.

## 2.1 Przez GUI

### 2.1.1 Konfiguracja parametrów STP/RSTP na portach

Wybierz z menu **L2 FEATURES > Spanning Tree > Port Config**, aby wyświetlić poniższą stronę.

Rys. 2-1 Konfiguracja parametrów STP/RSTP na portach

| Port Config                         |        |          |          |               |               |           |          |        |           |        |
|-------------------------------------|--------|----------|----------|---------------|---------------|-----------|----------|--------|-----------|--------|
| UNIT1                               |        | LAGS     |          |               |               |           |          |        |           |        |
| <input type="checkbox"/>            | Port   | Status   | Priority | Ext-Path Cost | Int-Path Cost | Edge Port | P2P Link | MCheck | Port Mode | Port I |
| <input checked="" type="checkbox"/> | 1/0/1  | Disabled | 128      | Auto          | Auto          | Disabled  | Auto     | --     | --        |        |
| <input type="checkbox"/>            | 1/0/2  | Disabled | 128      | Auto          | Auto          | Disabled  | Auto     | --     | --        |        |
| <input type="checkbox"/>            | 1/0/3  | Disabled | 128      | Auto          | Auto          | Disabled  | Auto     | --     | --        |        |
| <input type="checkbox"/>            | 1/0/4  | Disabled | 128      | Auto          | Auto          | Disabled  | Auto     | --     | --        |        |
| <input type="checkbox"/>            | 1/0/5  | Disabled | 128      | Auto          | Auto          | Disabled  | Auto     | --     | --        |        |
| <input type="checkbox"/>            | 1/0/6  | Disabled | 128      | Auto          | Auto          | Disabled  | Auto     | --     | --        |        |
| <input type="checkbox"/>            | 1/0/7  | Disabled | 128      | Auto          | Auto          | Disabled  | Auto     | --     | --        |        |
| <input type="checkbox"/>            | 1/0/8  | Disabled | 128      | Auto          | Auto          | Disabled  | Auto     | --     | --        |        |
| <input type="checkbox"/>            | 1/0/9  | Disabled | 128      | Auto          | Auto          | Disabled  | Auto     | --     | --        |        |
| <input type="checkbox"/>            | 1/0/10 | Disabled | 128      | Auto          | Auto          | Disabled  | Auto     | --     | --        |        |

Total: 10      1 entry selected.     

Wykonaj poniższe kroki, aby skonfigurować na portach parametry STP/RSTP:

1) W sekcji **Port Config** skonfiguruj parametry STP/RSTP na portach.

|               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|---------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| UNIT          | Wybierz właściwą jednostkę lub grupy LAG.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Status        | Włącz lub wyłącz funkcję drzewa rozpinającego na wybranym porcie.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Priority      | <p>Określ priorytet dla wybranego portu. Wartość powinna być całkowitą wielokrotnością liczby 16, mieszczącą się w zakresie od 0 do 240.</p> <p>Port z mniejszą wartością ma wyższy priorytet. Jeżeli ścieżka główna portu jest taka sama jak ścieżka innych portów, przełącznik porówna priorytety portów i wybierze port główny z najwyższym priorytetem.</p>                                                                                                                                                                                                                                                                                                                                                            |
| Ext-Path Cost | <p>Wpisz wartość kosztu ścieżki zewnętrznej. Wartość musi mieścić się między 0 a 2000000. Domyślnie ustawiona jest opcja Auto - port automatycznie wylicza koszt ścieżki zewnętrznej, w zależności od prędkości łącza portu.</p> <p>W przypadku STP/RSTP koszt ścieżki zewnętrznej wskazuje koszt ścieżki portu w drzewie rozpinającym. Port z najniższym kosztem ścieżki głównej zostanie wybrany na port główny przełącznika.</p> <p>W przypadku MSTP koszt ścieżki zewnętrznej wskazuje koszt ścieżki portu w CST.</p>                                                                                                                                                                                                  |
| Int-Path Cost | <p>Wpisz wartość kosztu ścieżki wewnętrznej. Domyślnie ustawiona jest opcja Auto - port automatycznie wylicza koszt ścieżki wewnętrznej, w zależności od prędkości łącza portu. Ten parametr używany jest jedynie w MSTP, nie trzeba go konfigurować, jeżeli tryb drzewa rozpinającego to STP/RSTP.</p> <p>W przypadku MSTP koszt ścieżki wewnętrznej wykorzystywany jest do obliczania kosztu ścieżki w IST. Port z najniższym kosztem ścieżki głównej zostanie wybrany na port główny przełącznika w IST.</p>                                                                                                                                                                                                            |
| Edge Port     | <p>Wybierz Enable, aby ustawić port jako brzegowy.</p> <p>W przypadku zmiany topologii port końcowy może zmienić swój stan z blokowania do przekazywania. Dla szybkiego generowania drzewa rozpinającego zaleca się ustawienie portów połączonych z urządzeniami brzegowymi jako porty brzegowe.</p>                                                                                                                                                                                                                                                                                                                                                                                                                       |
| P2P Link      | <p>Wybierz stan łącza P2P (Point-to-Point), do którego podłączone są porty. Podczas regeneracji drzewa rozpinającego, jeżeli port łącza P2P wybrany jest jako port główny lub port desygnowany, może on zmienić swój stan na przekazywanie.</p> <p>Dostępne są trzy opcje: Auto, Open(Force) i Closed(Force). Domyślnie ustawiona jest opcja Auto.</p> <p><b>Auto:</b> Przełącznik sprawdza automatycznie, czy port podłączony jest do łącza P2P i ustawia status na Open lub Closed.</p> <p><b>Open(Force):</b> Port ustawiony jest jako podłączony do łącza P2P. Najpierw należy sprawdzić łącze.</p> <p><b>Close(Force):</b> Port ustawiony jest jako niepodłączony do łącza P2P. Najpierw należy sprawdzić łącze..</p> |

|             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|-------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| MCheck      | Wybierz, czy na porcie wykonywane będą operacje MCheck. Jeżeli port na urządzeniu RSTP-enabled/MSTP-enabled podłączony jest do urządzenia STP-enabled, port przełączy się do trybu kompatybilności z STP i będzie wysyłał pakiety w formacie STP. MCheck pozwala z powrotem przełączyć tryb portu na RSTP/MSTP po odłączeniu portu od urządzenia STP-enabled. Konfigurację MCheck przeprowadzić można tylko raz, po tym status MCheck portu zmieni się na Disabled (wył.).                                                                                                                                                                                                                                                                                                                                                       |
| Port Mode   | Wyświetla tryb drzewa rozpinającego portu.<br><br><b>STP:</b> Tryb drzewa rozpinającego to STP.<br><br><b>RSTP:</b> Tryb drzewa rozpinającego to RSTP.<br><br><b>MSTP:</b> Tryb drzewa rozpinającego to MSTP.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Port Role   | Wyświetla rolę portu w drzewie rozpinającym.<br><br><b>Root Port:</b> Port jest portem głównym w drzewie rozpinającym. Ma najniższy koszt ścieżki od mostu głównego do przełącznika i wykorzystywany jest do komunikacji z mostem głównym.<br><br><b>Designated Port:</b> Port jest portem desygnowanym w drzewie rozpinającym. Ma najniższy koszt ścieżki od mostu głównego do segmentu sieci fizycznej i wykorzystywany jest do przekazywania danych do odpowiednich segmentów sieci.<br><br><b>Alternate Port:</b> Port jest portem alternatywnym w drzewie rozpinającym. Jest to port zapasowy portu głównego lub master portu.<br><br><b>Backup Port:</b> Port jest portem zapasowym w drzewie rozpinającym. Jest to port zapasowy portu desygnowanego.<br><br><b>Disabled:</b> Port nie jest częścią drzewa rozpinającego. |
| Port Status | Wyświetla stan portu.<br><br><b>Forwarding:</b> Port odbiera i wysyła ramki BPDU oraz przekazuje dane użytkownika.<br><br><b>Learning:</b> Port odbiera i wysyła ramki BPDU. Odbiera również ruch użytkownika, ale nie przekazuje go.<br><br><b>Blocking:</b> Port jedynie odbiera i wysyła ramki BPDU.<br><br><b>Disconnected:</b> Port ma włączoną funkcję drzewa rozpinającego, ale nie jest połączony z żadnym urządzeniem.                                                                                                                                                                                                                                                                                                                                                                                                  |
| LAG         | Wyświetla grupę LAG, do której należy port.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |

2) Kliknij **Apply**.

## 2.1.2 Konfiguracja globalna STP/RSTP

Wybierz z menu **L2 FEATURES > Spanning Tree > STP Config > STP Config**, aby wyświetlić poniższą stronę.

Rys. 2-2 Konfiguracja globalna STP/RSTP

**Global Config**

---

Spanning Tree:  Enable

Mode: STP ▼

Apply

---

**Parameters Config**

CIST Priority: 32768 (0-61440, in increments of 4096)

Hello Time: 2 seconds (1-10)

Max Age: 20 seconds (6-40)

Forward Delay: 15 seconds (4-30)

Tx Hold Count: 5 pps (1-20)

Max Hops: 20 hop (1-40)

Apply

Wykonaj poniższe kroki, aby skonfigurować globalnie STP/RSTP:

1) W sekcji **Parameters Config** skonfiguruj parametry globalne STP/RSTP i kliknij **Apply**.

|                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>CIST Priority</b> | <p>Wyznacz priorytet CIST dla przełącznika. Priorytet CIST jest parametrem wykorzystywanym do ustawienia mostu głównego w drzewie rozpinającym. Przełącznik o niższej wartości ma wyższy priorytet.</p> <p>W przypadku STP/RSTP, priorytet CIST jest priorytetem przełącznika w drzewie rozpinającym. Przełącznik o najwyższym priorytecie wybrany zostanie mostem głównym.</p> <p>W przypadku MSTP, priorytet CISP jest priorytetem przełącznika w CIST. Przełącznik z najwyższym priorytetem wybrany zostanie mostem głównym w CIST.</p> |
| <b>Hello Time</b>    | <p>Wyznacz odstęp czasu wysyłania ramek BPDU. Wartość domyślna to 2. Most główny wysyła konfiguracyjne ramki BPDU w odstępie czasu powitania (Hello Time). Pracuje z wiekiem maksymalnym (MAX Age), aby przetestować błędy łącza i utrzymać drzewo rozpinające.</p>                                                                                                                                                                                                                                                                        |
| <b>Max Age</b>       | <p>Wyznacz maks. czas, przez który przełącznik może czekać bez odbierania BPDU przed próbą odtworzenia nowego drzewa rozpinającego. Wartość domyślna to 2.</p>                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Forward Delay</b> | <p>Wyznacz odstęp czasu między zmianą stanu portu od słuchania do uczenia się. Wartość domyślna to 15. Funkcja wykorzystywana jest do zapobiegania wytwarzania przez sieć tymczasowych pętli w trakcie odtwarzania drzewa rozpinającego. Odstęp czasu przejścia portu od stanu uczenia się do stanu przekazywania to również Forward Delay.</p>                                                                                                                                                                                            |
| <b>Tx Hold Count</b> | <p>Wyznacz maksymalną liczbę ramek BPDU wysyłanych w jedną sekundę. Wartość domyślna to 5</p>                                                                                                                                                                                                                                                                                                                                                                                                                                              |

|          |                                                                                                                                                                                                                                                                                                                     |
|----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Max Hops | Wyznacz maksymalną liczbę BPDU wysyłanych w obszar MST. Wartość domyślna to 20. Przełącznik odbiera BPDU, zmniejsza liczbę przeskoków generuje ramki BPDU o nowej wartości. Kiedy wartość przeskoku wyniesie zero, przełącznik odrzuci BPDU. Wartość ta może kontrolować skalę drzewa rozpinającego w obszarze MST. |
|----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

*Note:* Maks. liczba przeskoków to parametr konfigurowany w MSTP. Nie musisz go konfigurować, jeżeli tryb drzewa rozpinającego to STP/RSTP.

### Uwaga:

Aby zapobiec częstemu migotaniu sieci (ang. flapping), upewnij się, że Hello Time, Forward Delay i Max Age są zgodne z poniższymi wzorami:

- $2 * (\text{Hello Time} + 1) \leq \text{Max Age}$
- $2 * (\text{Forward Delay} - 1) \geq \text{Max Age}$

2) W sekcji **Global Config** włącz funkcję drzewa rozpinającego, wybierz tryb STP jako STP/RSTP i kliknij **Apply**.

|               |                                                                                                                                                                                                                                                                                      |
|---------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Spanning Tree | Zaznacz pole, aby włączyć funkcję drzewa rozpinającego globalnie.                                                                                                                                                                                                                    |
| Mode          | Ustaw tryb drzewa rozpinającego na STP/RSTP na przełączniku. Domyślnie ustawiony jest tryb STP.<br><br><b>STP:</b> Ustaw tryb drzewa rozpinającego na STP.<br><br><b>RSTP:</b> Ustaw tryb drzewa rozpinającego na RSTP.<br><br><b>MSTP:</b> Ustaw tryb drzewa rozpinającego na MSTP. |

## 2.1.3 Sprawdzanie konfiguracji STP/RSTP

Po zakończeniu całego procesu konfiguracji, sprawdź dane STP/RSTP przełącznika.

Wybierz z menu **L2 FEATURES > Spanning Tree > STP Config > STP Summary**, aby wyświetlić poniższą stronę.

Rys. 2-3 Sprawdzenie konfiguracji STP/RSTP

### STP Summary

---

|                       |                           |
|-----------------------|---------------------------|
| Spanning Tree:        | Enable                    |
| Spanning Tree Mode:   | STP                       |
| Local Bridge:         | 32768---00-0a-eb-13-a2-02 |
| Root Bridge:          | 32768---00-0a-eb-13-a2-02 |
| External Path Cost:   | 0                         |
| Regional Root Bridge: | ---                       |
| Internal Path Cost:   | ---                       |
| Designated Bridge:    | 32768---00-0a-eb-13-a2-02 |
| Root Port:            | ---                       |
| Latest TC Time:       | 2006-01-01 08:00:45       |
| TC Count:             | 0                         |

### MSTP Instance Summary

---

|                       |                               |
|-----------------------|-------------------------------|
| Instance ID:          | <input type="text" value=""/> |
| Instance Status:      | Disable                       |
| Local Bridge:         | ---                           |
| Regional Root Bridge: | ---                           |
| Internal Path Cost:   | ---                           |
| Designated Bridge:    | ---                           |
| Root Port:            | ---                           |
| Latest TC Time:       | ---                           |
| TC Count:             | ---                           |

Sekcja **STP Summary** przedstawia podsumowanie informacji dotyczących drzewa rozpinającego :

|                             |                                                                                              |
|-----------------------------|----------------------------------------------------------------------------------------------|
| <b>Spanning Tree</b>        | Informuje o stanie funkcji drzewa rozpinającego.                                             |
| <b>Spanning Tree Mode</b>   | Informuje o trybie drzewa rozpinającego.                                                     |
| <b>Local Bridge</b>         | Informuje o bridge ID mostu lokalnego. Mostem lokalnym jest wykorzystywany przełącznik.      |
| <b>Root Bridge</b>          | Informuje o bridge ID mostu głównego.                                                        |
| <b>External Path Cost</b>   | Informuje o koszcie ścieżki głównej z przełącznika do mostu głównego.                        |
| <b>Regional Root Bridge</b> | To most główny IST. Nie wyświetla się, jeżeli wybrany tryb drzewa rozpinającego to STP/RSTP. |

|                    |                                                                                                                                                                    |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Internal Path Cost | Koszt ścieżki wewnętrznej to koszt ścieżki głównej od przełącznika do mostu głównego IST. Nie wyświetla się, jeżeli wybrany tryb drzewa rozpinającego to STP/RSTP. |
| Designated Bridge  | Informuje o bridge ID mostu desygnowanego. Most desygnowany to przełącznik z portami desygnowanymi.                                                                |
| Root Port          | Informuje o porcie głównym wykorzystywanego przełącznika.                                                                                                          |
| Latest TC Time     | Informuje o ostatnim czasie zmiany topologii.                                                                                                                      |
| TC Count           | Informuje o tym, ile razy zmieniła się topologia.                                                                                                                  |

## 2.2 Przez CLI

### 2.2.1 Konfiguracja parametrów STP/RSTP na portach

Wykonaj poniższe kroki, aby skonfigurować parametry STP/RSTP na portach:

|        |                                                                                                                                                                                                                                                                                                                                                                      |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Krok 1 | <b>configure</b><br>Uruchom tryb konfiguracji globalnej.                                                                                                                                                                                                                                                                                                             |
| Krok 2 | <b>interface {fastEthernet <i>port</i>   range fastEthernet <i>port-list</i>   gigabitEthernet <i>port</i>   range gigabitEthernet <i>port-list</i>   ten-gigabitEthernet <i>port</i>   range ten-gigabitEthernet <i>port-list</i>   port-channel <i>port-channel-id</i>   range port-channel <i>port-channel-list</i>}</b><br>Uruchom tryb konfiguracji interfejsu. |
| Krok 3 | <b>spanning-tree</b><br>Włącz funkcję drzewa rozpinającego dla wybranych portów.                                                                                                                                                                                                                                                                                     |



- 
- Krok 4 **spanning-tree common-config [ port-priority *pri* ] [ ext-cost *ext-cost* ] [ portfast { enable | disable } ] [ point-to-point { auto | open | close } ]**
- Skonfiguruj parametry STP/RSTP na wybranym porcie.
- pri*: Wyznacz Priorytet dla wybranego portu. Wartość powinna być całkowitą wielokrotnością liczby 16 i mieścić się w zakresie od 0 do 240. Wartość domyślna to 128. Porty z mniejszymi wartościami ma ją wyższy priorytet. Jeżeli ścieżka główna portu jest taka sama jak ścieżka innych portów, przełącznik porówna priorytety portów i wybierze port główny z najwyższym priorytetem.
- ext-cost*: Wyznacz wartość kosztu ścieżki zewnętrznej. Wartość powinna mieścić się w zakresie od 0 do 2000000. Domyślnie ustawiona jest opcja Auto - port automatycznie wylicza koszt ścieżki zewnętrznej, w zależności od prędkości łącza portu.
- W przypadku STP/RSTP koszt ścieżki zewnętrznej wskazuje koszt ścieżki portu w drzewie rozpinającym. Port z najniższym kosztem ścieżki głównej zostanie wybrany na port główny przełącznika.
- W przypadku MSTP koszt ścieżki zewnętrznej wskazuje koszt ścieżki portu w CST.
- portfast { enable | disable }**: Wybierz Enable (Włącz), aby ustawić port jako końcowy. Funkcja jest domyślnie wyłączona. W przypadku zmiany topologii port końcowy może zmienić swój stan z blokowania do przekazywania. Dla szybkiego generowania drzewa rozpinającego zaleca się ustawienie portów połączonych z urządzeniami końcowymi jako porty końcowe.
- point-to-point { auto | open | close }**: Wybierz stan łącza P2P (Point-to-Point), do którego podłączone są porty. Podczas regeneracji drzewa rozpinającego, jeżeli port łącza P2P wybrany jest jako port główny lub port desygnowany, może on zmienić swój stan na przekazywanie. Opcja **Auto** oznacza, że przełącznik sprawdza automatycznie, czy port podłączony jest do łącza P2P i ustawia status na Open lub Closed. **Open wskazuje na to, że** port ustawiony jest jako podłączony do łącza P2P; **Close** - port ustawiony jest jako niepodłączony do łącza P2P.
- 
- Krok 5 **spanning-tree mcheck**
- (Opcjonalnie) Przeprowadź MCheck na porcie.
- Jeżeli port na urządzeniu RSTP-enabled/MSTP-enabled podłączony jest do urządzenia STP-enabled, port przełączy się do trybu kompatybilności z STP i będzie wysyłał pakiety w formacie STP. MCheck pozwala z powrotem przełączyć tryb portu na RSTP/MSTP po odłączeniu portu od urządzenia STP-enabled. Konfigurację MCheck przeprowadzić można tylko raz, po tym status MCheck portu zmieni się na Disabled (wył.).
- 
- Krok 6 **show spanning-tree interface [ fastEthernet *port* | gigabitEthernet *port* | ten-gigabitEthernet *port* | port-channel *lagid* ] [ edge | ext-cost | int-cost | mode | p2p | priority | role | state | status ]**
- (Opcjonalnie) Sprawdź dane wszystkich portów lub wybranego portu.
- port*: Określ numer portu.
- lagid*: Określ ID grupy LAG.
- ext-cost | int-cost | mode | p2p | priority | role | state | status: Pokaż określone informacje.
- 
- Krok 7 **end**
- Powróć do trybu privileged EXEC.
- 
- Krok 8 **copy running-config startup-config**
- Zapisz ustawienia w pliku konfiguracyjnym.
-

Poniższy przykład prezentuje włączanie funkcji drzewa rozpinającego na porcie 1/0/3 i konfigurację priorytetu portu na 32 :

```
Switch#configure
```

```
Switch(config)#interface gigabitEthernet 1/0/3
```

```
Switch(config-if)#spanning-tree
```

```
Switch(config-if)#spanning-tree common-config port-priority 32
```

```
Switch(config-if)#show spanning-tree interface gigabitEthernet 1/0/3
```

| Interface | State  | Prio  | Ext-Cost | Int-Cost | Edge | P2p      | Mode  |
|-----------|--------|-------|----------|----------|------|----------|-------|
| -----     | -----  | ----  | -----    | -----    | ---- | -----    | ----- |
| Gi1/0/3   | Enable | 32    | Auto     | Auto     | No   | No(auto) | N/A   |
| Role      | Status | LAG   |          |          |      |          |       |
| -----     | -----  | ----- |          |          |      |          |       |
| N/A       | LnkDwn | N/A   |          |          |      |          |       |

```
Switch(config-if)#end
```

```
Switch#copy running-config startup-config
```

## 2.2.2 Konfiguracja parametrów globalnych STP/RSTP

Aby skonfigurować na przełączniku parametry globalne STP/RSTP, wykonaj poniższe kroki:

Krok 1     **configure**

Uruchom tryb konfiguracji globalnej.

Krok 2     **spanning-tree priority pri**

Skonfiguruj priorytet przełącznika.

*pri*: Określ priorytet przełącznika. Wartość musi mieścić się w zakresie od 0 do 61440 i powinna być podzielna przez 4096. Priorytet jest parametrem wykorzystywanym do określenia mostu głównego drzewa rozpinającego. Przełącznik z niższą wartością ma wyższy priorytet.

W przypadku STP/RSTP wartość jest priorytetem przełącznika w drzewie rozpinającym. Przełącznik z najwyższym priorytetem zostanie wybrany na most główny.

W przypadku MSTP wartość jest priorytetem przełącznika w CIST. Przełącznik z wyższym priorytetem zostanie wybrany na most główny w CIST.

---

Krok 3 **spanning-tree timer** [[ **forward-time** *forward-time*] [**hello-time** *hello-time*] [**max-age** *max-age*]]

(Opcjonalnie) Skonfiguruj Forward Delay, Hello Time i Max Age.

*forward-time*: Wyznacz odstęp czasu między zmianą stanu portu od słuchania do uczenia się. Wartość powinna wynosić od 4 do 30 s. Wartość domyślna to 15. Funkcja wykorzystywana jest do zapobiegania wytwarzania przez sieć tymczasowych pętli w trakcie odtwarzania drzewa rozpinającego. Odstęp czasu przejścia portu od stanu uczenia się do stanu przekazywania to również Forward Delay.

*hello-time*: Wyznacz wartość Hello Time, czyli odstęp czasu pomiędzy wysyłaniem ramek BPDU. Wartość powinna mieścić się w zakresie między 1 a 10 s. Wartość domyślna to 2. Most główny wysyła konfiguracyjne ramki BPDU w odstępie czasu powitania (Hello Time). Pracuje z wiekiem maksymalnym (MAX Age), aby przetestować błędy łącza i utrzymać drzewo rozpinające.

*max-age*: Wyznacz maks. czas, przez który przełącznik może czekać bez odbierania BPDU przed próbą odtworzenia nowego drzewa rozpinającego. Wartość powinna wynosić od 6 do 40 s. Wartość domyślna to 20.

---

Krok 4 **spanning-tree hold-count** *value*

Określ maksymalną liczbę ramek BPDU wysyłanych na sekundę.

*value*: Określ maksymalną liczbę pakietów BPDU wysyłanych na sekundę. Wartość powinna wynosić od 1 do 20 p/s. Wartość domyślna to 5.

---

Krok 5 **show spanning-tree bridge**

(Opcjonalnie) Sprawdź parametry globalne STP/RSTP przełącznika.

---

Krok 6 **end**

Powróć do trybu privileged EXEC.

---

Krok 7 **copy running-config startup-config**

Zapisz ustawienia w pliku konfiguracyjnym.

---

 **Uwaga:**

Aby zapobiec częstemu migotaniu sieci (ang. flapping), upewnij się, że Hello Time, Forward Delay i Max Age są zgodne z poniższymi wzorami:

- $2 * (\text{Hello Time} + 1) \leq \text{Max Age}$
- $2 * (\text{Forward Delay} - 1) \geq \text{Max Age}$

---

Poniższy przykład prezentuje konfigurację priorytetu przełącznika na 36864 i Forward Delay na 12 sekund:

```
Switch#configure
```

```
Switch(config)#spanning-tree priority 36864
```

```
Switch(config)#spanning-tree timer forward-time 12
```

```
Switch(config)#show spanning-tree bridge
```

| State  | Mode  | Priority | Hello-Time | Fwd-Time | Max-Age | Hold-Count | Max-Hops |
|--------|-------|----------|------------|----------|---------|------------|----------|
| -----  | ----- | -----    | -----      | -----    | -----   | -----      | -----    |
| Enable | Rstp  | 36864    | 2          | 12       | 20      | 5          | 20       |

```
Switch(config)#end
```

```
Switch#copy running-config startup-config
```

### 2.2.3 Włączanie STP/RSTP globalnie

Aby ustawić tryb drzewa rozpinającego jako STP/RSTP i włączyć funkcję Spanning Tree globalnie, wykonaj poniższe kroki:

|        |                                                                                                                                                                                                 |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Krok 1 | <b>configure</b><br>Uruchom tryb konfiguracji globalnej.                                                                                                                                        |
| Krok 2 | <b>spanning-tree mode { stp   rstp }</b><br>Ustaw tryb drzewa rozpinającego na STP/RSTP.<br><br>stp: Ustaw tryb drzewa rozpinającego na STP.<br>rstp: Ustaw tryb drzewa rozpinającego na RSTP . |
| Krok 3 | <b>spanning-tree</b><br>Włącz funkcję drzewa rozpinającego globalnie.                                                                                                                           |
| Krok 4 | <b>show spanning-tree active</b><br>(Opcjonalnie) Sprawdź dane aktywne STP/RSTP.                                                                                                                |
| Krok 5 | <b>end</b><br>Powróć do trybu privileged EXEC.                                                                                                                                                  |
| Krok 6 | <b>copy running-config startup-config</b><br>Zapisz ustawienia w pliku konfiguracyjnym.                                                                                                         |

Poniższy przykład prezentuje włączanie funkcji drzewa rozpinającego, konfigurację trybu na RSTP i sprawdzanie ustawień:

```
Switch#configure
```

```
Switch(config)#spanning-tree mode rstp
```

```
Switch(config)#spanning-tree
```

**Switch(config)#show spanning-tree active**

Spanning tree is enabled

Spanning-tree's mode: RSTP (802.1w Rapid Spanning Tree Protocol)

Latest topology change time: 2006-01-02 10:04:02

Root Bridge

Priority : 32768

Address : 00-0a-eb-13-12-ba

Local bridge is the root bridge

Designated Bridge

Priority : 32768

Address : 00-0a-eb-13-12-ba

Local Bridge

Priority : 32768

Address : 00-0a-eb-13-12-ba

| Interface | State  | Prio | Ext-Cost | Int-Cost | Edge | P2p       | Mode  |
|-----------|--------|------|----------|----------|------|-----------|-------|
| -----     | -----  | ---- | -----    | -----    | ---- | -----     | ----- |
| Gi1/0/16  | Enable | 128  | 200000   | 200000   | No   | Yes(auto) | Rstp  |
| Gi1/0/18  | Enable | 128  | 200000   | 200000   | No   | Yes(auto) | Rstp  |
| Gi1/0/20  | Enable | 128  | 200000   | 200000   | No   | Yes(auto) | Rstp  |

| Role  | Status | LAG   |
|-------|--------|-------|
| ----- | -----  | ----- |
| Desg  | Fwd    | N/A   |
| Desg  | Fwd    | N/A   |
| Desg  | Fwd    | N/A   |

**Switch(config)#end**

**Switch#copy running-config startup-config**

# 3 Konfiguracja MSTP

Aby przeprowadzić konfigurację MSTP, wykonaj poniższe kroki:

- 1) Skonfiguruj parametry na portach w CIST.
- 2) Skonfiguruj region MSTP.
- 3) Skonfiguruj MSTP globalnie.
- 4) Sprawdź ustawienia MSTP.

## Wskazówki dotyczące konfiguracji

- Przed konfiguracją drzewa rozpinającego (spanning tree) trzeba koniecznie jasno zaznaczyć, jaka rola przypisana jest każdemu przełącznikowi w drzewie rozpinającym.
- Aby zapobiec migotaniu sieci (ang. flapping) spowodowanemu zmianą parametrów MSTP, po skonfigurowaniu odpowiednich parametrów zaleca się globalne włączenie funkcji MSTP.

## 3.1 Przez GUI

### 3.1.1 Konfiguracja parametrów na portach w CIST

Wybierz z menu **L2 FEATURES > Spanning Tree > Port Config**, aby wyświetlić poniższą stronę.

Rys. 3-1 Konfiguracja parametrów na portach

| Port Config                         |        |          |          |               |               |           |          |        |           |        |
|-------------------------------------|--------|----------|----------|---------------|---------------|-----------|----------|--------|-----------|--------|
| UNIT1                               |        | LAGS     |          |               |               |           |          |        |           |        |
| <input type="checkbox"/>            | Port   | Status   | Priority | Ext-Path Cost | Int-Path Cost | Edge Port | P2P Link | MCheck | Port Mode | Port f |
| <input checked="" type="checkbox"/> | 1/0/1  | Disabled | 128      | Auto          | Auto          | Disabled  | Auto     | --     | --        | --     |
| <input type="checkbox"/>            | 1/0/2  | Disabled | 128      | Auto          | Auto          | Disabled  | Auto     | --     | --        | --     |
| <input type="checkbox"/>            | 1/0/3  | Disabled | 128      | Auto          | Auto          | Disabled  | Auto     | --     | --        | --     |
| <input type="checkbox"/>            | 1/0/4  | Disabled | 128      | Auto          | Auto          | Disabled  | Auto     | --     | --        | --     |
| <input type="checkbox"/>            | 1/0/5  | Disabled | 128      | Auto          | Auto          | Disabled  | Auto     | --     | --        | --     |
| <input type="checkbox"/>            | 1/0/6  | Disabled | 128      | Auto          | Auto          | Disabled  | Auto     | --     | --        | --     |
| <input type="checkbox"/>            | 1/0/7  | Disabled | 128      | Auto          | Auto          | Disabled  | Auto     | --     | --        | --     |
| <input type="checkbox"/>            | 1/0/8  | Disabled | 128      | Auto          | Auto          | Disabled  | Auto     | --     | --        | --     |
| <input type="checkbox"/>            | 1/0/9  | Disabled | 128      | Auto          | Auto          | Disabled  | Auto     | --     | --        | --     |
| <input type="checkbox"/>            | 1/0/10 | Disabled | 128      | Auto          | Auto          | Disabled  | Auto     | --     | --        | --     |

Total: 10      1 entry selected.      Cancel Apply

Aby skonfigurować parametry na portach w CIST, wykonaj poniższe kroki:

1) W sekcji **Port Config** skonfiguruj parametry na portach.

|               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|---------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| UNIT          | Wybierz właściwą jednostkę lub grupy LAG.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Status        | Włącz lub wyłącz funkcję drzewa rozpinającego na wybranym porcie.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Priority      | <p>Określ priorytet dla wybranego portu. Wartość powinna być całkowitą wielokrotnością liczby 16, mieszczącą się w zakresie od 0 do 240.</p> <p>Port z mniejszą wartością ma wyższy priorytet. Jeżeli ścieżka główna portu jest taka sama jak ścieżka innych portów, przełącznik porówna priorytety portów i wybierze port główny z najwyższym priorytetem.</p>                                                                                                                                                                                              |
| Ext-Path Cost | <p>Wpisz wartość kosztu ścieżki zewnętrznej. Domyślnie ustawiona jest opcja Auto - port automatycznie wylicza koszt ścieżki zewnętrznej, w zależności od prędkości łącza portu.</p> <p>W przypadku STP/RSTP koszt ścieżki zewnętrznej wskazuje koszt ścieżki portu w drzewie rozpinającym. Port z najniższym kosztem ścieżki głównej zostanie wybrany na port główny przełącznika.</p> <p>W przypadku MSTP koszt ścieżki zewnętrznej wskazuje koszt ścieżki portu w CST.</p>                                                                                 |
| Int-Path Cost | <p>Wpisz wartość kosztu ścieżki wewnętrznej. Wartość musi mieścić się między 0 a 2000000. Domyślnie ustawiona jest opcja Auto - port automatycznie wylicza koszt ścieżki wewnętrznej, w zależności od prędkości łącza portu. Ten parametr używany jest jedynie w MSTP, nie trzeba go konfigurować, jeżeli tryb drzewa rozpinającego to STP/RSTP.</p> <p>W przypadku MSTP koszt ścieżki wewnętrznej wykorzystywany jest do obliczania kosztu ścieżki w IST. Port z najniższym kosztem ścieżki głównej zostanie wybrany na port główny przełącznika w IST.</p> |
| Edge Port     | <p>Wybierz Enable, aby ustawić port jako brzegowy.</p> <p>W przypadku zmiany topologii port brzegowy może zmienić swój stan z blokowania do przekazywania. Dla szybkiego generowania drzewa rozpinającego zaleca się ustawienie portów połączonych z urządzeniami końcowymi jako porty brzegowe.</p>                                                                                                                                                                                                                                                         |

---

|           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|-----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| P2P Link  | <p>Wybierz stan łącza P2P (Point-to-Point), do którego podłączone są porty. Podczas regeneracji drzewa rozpinającego, jeżeli port łącza P2P wybrany jest jako port główny lub port desygnowany, może on zmienić swój stan na przekazywanie.</p> <p>Dostępne są trzy opcje: Auto, Open(Force) i Closed(Force). Domyślnie ustawiona jest opcja Auto.</p> <p><b>Auto:</b> Przełącznik sprawdza automatycznie, czy port podłączony jest do łącza P2P i ustawia status na Open lub Closed.</p> <p><b>Open(Force):</b> Port ustawiony jest jako podłączony do łącza P2P. Najpierw należy sprawdzić łącze.</p> <p><b>Close(Force):</b> Port ustawiony jest jako niepodłączony do łącza P2P. Najpierw należy sprawdzić łącze.</p>                                                                                                            |
| MCheck    | <p>Wybierz, czy na porcie wykonywane będą operacje MCheck. Jeżeli port na urządzeniu RSTP-enabled/MSTP-enabled podłączony jest do urządzenia STP-enabled, port przełączy się do trybu kompatybilności z STP i będzie wysyłał pakiety w formacie STP. MCheck pozwala z powrotem przełączyć tryb portu na RSTP/MSTP po odłączeniu portu od urządzenia STP-enable. Konfigurację MCheck przeprowadzić można tylko raz, po tym status MCheck portu zmieni się na Disabled (wył.).</p>                                                                                                                                                                                                                                                                                                                                                     |
| Port Mode | <p>Wyświetla tryb drzewa rozpinającego portu.</p> <p><b>STP:</b> Tryb drzewa rozpinającego to STP.</p> <p><b>RSTP:</b> Tryb drzewa rozpinającego to RSTP.</p> <p><b>MSTP:</b> Tryb drzewa rozpinającego to MSTP.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Port Role | <p>Wyświetla rolę portu w drzewie rozpinającym.</p> <p><b>Root Port:</b> Port jest portem głównym w drzewie rozpinającym. Ma najniższy koszt ścieżki od mostu głównego do przełącznika i wykorzystywany jest do komunikacji z mostem głównym.</p> <p><b>Designated Port:</b> Port jest portem desygnowanym w drzewie rozpinającym. Ma najniższy koszt ścieżki od mostu głównego do segmentu sieci fizycznej i wykorzystywany jest do przekazywania danych do odpowiednich segmentów sieci.</p> <p><b>Alternate Port:</b> Port jest portem zastępczym w drzewie rozpinającym. Jest to port zapasowy portu głównego lub master portu.</p> <p><b>Backup Port:</b> Port jest portem zapasowym w drzewie rozpinającym. Jest to port zapasowy portu desygnowanego.</p> <p><b>Disabled:</b> Port nie jest częścią drzewa rozpinającego.</p> |

---



|             |                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Port Status | Wyświetla stan portu.<br><br><b>Forwarding:</b> Port odbiera i wysyła ramki BPDU oraz przekazuje dane użytkownika.<br><br><b>Learning:</b> Port odbiera i wysyła ramki BPDU. Odbiera również ruch użytkownika, ale nie przekazuje go.<br><br><b>Blocking:</b> Port jedynie odbiera i wysyła ramki BPDU.<br><br><b>Disconnected:</b> Port ma włączoną funkcję drzewa rozpinającego, ale nie jest połączony z żadnym urządzeniem. |
| LAG         | Wyświetla grupę LAG, do której należy port.                                                                                                                                                                                                                                                                                                                                                                                     |

2) Kliknij **Apply**.

### 3.1.2 Konfiguracja regionu MSTP

Skonfiguruj nazwę regionu, poziom weryfikacji i mapowanie VLAN do instancji przełącznika. Przełączniki z tą samą nazwą regionu, jednakowym poziomem weryfikacji i mapowaniem VLAN do instancji należą do tego samego regionu.

Dodatkowo należy skonfigurować priorytet przełącznika oraz priorytet i koszt ścieżki portów w wybranej instancji.

- **Konfiguracja nazwy regionu i poziomu weryfikacji**

Wybierz z menu **L2 FEATURES > Spanning Tree > MSTP Instance > Region Config**, aby wyświetlić poniższą stronę.

Rys. 3-2 Konfiguracja regionu

Aby utworzyć region MST, wykonaj poniższe kroki.

1) 1) W sekcji **Region Config** ustaw nazwę i poziom weryfikacji, aby określić region MSTP.

|             |                                                                                                       |
|-------------|-------------------------------------------------------------------------------------------------------|
| Region Name | Skonfiguruj nazwę regionu MST, używając maks. 32 znaków. Domyślnie nazwą jest adres MAC przełącznika. |
| Revision    | Wprowadź poziom weryfikacji. Wartość domyślna to 0.                                                   |

2) Kliknij **Apply**.

- Konfiguracja mapowania VLAN do instancji i priorytetu przełącznika

Wybierz z menu **L2 FEATURES > Spanning Tree > MSTP Instance > Instance Config**, aby wyświetlić poniższą stronę.

Rys. 3-3 Konfiguracja mapowania VLAN do instancji

| Instance Config          |             |          |         |           |
|--------------------------|-------------|----------|---------|-----------|
| <input type="checkbox"/> | Instance ID | Priority | VLAN ID | Operation |
| <input type="checkbox"/> | CIST        | 36864    | 1-4094, |           |
| Total: 1                 |             |          |         |           |

Aby mapować VLAN do odpowiedniej instancji i skonfigurować priorytet przełącznika w wybranej instancji, wykonaj poniższe kroki.

- 1) W sekcji **Instance Config** kliknij **Add** i wpisz ID instancji, priorytet i odpowiedni VLAN ID.

Rys. 3-4 Konfiguracja instancji

Instance Config

Instance ID:  (1-8)

Priority:  (0-61440, in increments of 4096)

VLAN ID:  Add  Delete

(1-4094, format:1,3,4-7,11-30)

|             |                                                                                                                                                                                                                                                                                                                                                                                                 |
|-------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Instance ID | Wprowadź odpowiedni ID instancji.                                                                                                                                                                                                                                                                                                                                                               |
| Priority    | Określ priorytet przełącznika w odpowiedniej instancji. Wartość powinna być całkowitą wielokrotnością liczby 4096 i powinna mieścić się w zakresie od 0 do 61440. Priorytet wykorzystywany jest do określania mostu głównego instancji. Przełączniki z niższą wartością mają wyższy priorytet. Przełącznik z najwyższym priorytetem zostanie wybrany na most główny w odpowiadającej instancji. |
| VLAN ID     | Wpisz VLAN ID, aby mapować VLAN do wybranej instancji lub rozwiązać mapowanie VLAN do instancji.                                                                                                                                                                                                                                                                                                |

- 2) Kliknij **Create**.

- Konfiguracja parametrów na portach w instancji

Wybierz z menu **L2 FEATURES > Spanning Tree > MSTP Instance > Instance Port Config**, aby wyświetlić poniższą stronę.

Rys. 3-5 Konfiguracja parametrów portów w instancji

Instance Port Config

---

Instance ID:

UNIT1

LAGS

|                                     | Port   | Priority | Path Cost | Port Role | Port Status | LAG |
|-------------------------------------|--------|----------|-----------|-----------|-------------|-----|
| <input checked="" type="checkbox"/> | 1/0/1  | 128      | Auto      | --        | --          | --- |
| <input type="checkbox"/>            | 1/0/2  | 128      | Auto      | --        | --          | --- |
| <input type="checkbox"/>            | 1/0/3  | 128      | Auto      | --        | --          | --- |
| <input type="checkbox"/>            | 1/0/4  | 128      | Auto      | --        | --          | --- |
| <input type="checkbox"/>            | 1/0/5  | 128      | Auto      | --        | --          | --- |
| <input type="checkbox"/>            | 1/0/6  | 128      | Auto      | --        | --          | --- |
| <input type="checkbox"/>            | 1/0/7  | 128      | Auto      | --        | --          | --- |
| <input type="checkbox"/>            | 1/0/8  | 128      | Auto      | --        | --          | --- |
| <input type="checkbox"/>            | 1/0/9  | 128      | Auto      | --        | --          | --- |
| <input type="checkbox"/>            | 1/0/10 | 128      | Auto      | --        | --          | --- |

Total: 10
1 entry selected.

Cancel
Apply

Aby skonfigurować parametry portów w instancji, wykonaj poniższe kroki.

1) W sekcji **Instance Port Config** wybierz odpowiedni ID instancji.

|             |                                                         |
|-------------|---------------------------------------------------------|
| Instance ID | Wybierz numer ID instancji, którą chcesz skonfigurować. |
|-------------|---------------------------------------------------------|

2) Skonfiguruj parametry portu w wybranej instancji.

|           |                                                                                                                                                                                                                                                                                                                                                                 |
|-----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| UNIT      | Wybierz jednostkę lub grupę LAG do skonfigurowania.                                                                                                                                                                                                                                                                                                             |
| Priority  | <p>Określ priorytet dla wybranego portu. Wartość powinna być całkowitą wielokrotnością liczby 16, mieszczącą się w zakresie od 0 do 240.</p> <p>Port z mniejszą wartością ma wyższy priorytet. Jeżeli ścieżka główna portu jest taka sama jak ścieżka innych portów, przełącznik porówna priorytety portów i wybierze port główny z najwyższym priorytetem.</p> |
| Path Cost | <p>Wpisz wartość kosztu ścieżki w odpowiadającej instancji. Wartość musi mieścić się między 0 a 2000000. Domyślnie ustawiona jest opcja Auto - port automatycznie wylicza koszt ścieżki zewnętrznej, w zależności od prędkości łącza portu. Port z najniższym kosztem ścieżki głównej zostanie wybrany na port główny przełącznika.</p>                         |

---

|             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|-------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Port Role   | <p>Wyświetla rolę portu w drzewie rozpinającym.</p> <p><b>Root Port:</b> Port jest portem głównym w drzewie rozpinającym. Ma najniższy koszt ścieżki od mostu głównego do przełącznika i wykorzystywany jest do komunikacji z mostem głównym.</p> <p><b>Designated Port:</b> Port jest portem desygnowanym w drzewie rozpinającym. Ma najniższy koszt ścieżki od mostu głównego do segmentu sieci fizycznej i wykorzystywany jest do przekazywania danych do odpowiednich segmentów sieci.</p> <p><b>Alternate Port:</b> Port jest portem zastępczym w drzewie rozpinającym. Jest to port zapasowy portu głównego lub master portu.</p> <p><b>Backup Port:</b> Port jest portem zapasowym w drzewie rozpinającym. Jest to port zapasowy portu desygnowanego.</p> <p><b>Disabled:</b> Port nie jest częścią drzewa rozpinającego.</p> |
| Port Status | <p>Wyświetla stan portu.</p> <p><b>Forwarding:</b> Port odbiera i wysyła ramki BPDU oraz przekazuje dane użytkownika.</p> <p><b>Learning:</b> Port odbiera i wysyła ramki BPDU. Odbiera również ruch użytkownika, ale nie przekazuje go.</p> <p><b>Blocking:</b> Port jedynie odbiera i wysyła ramki BPDU.</p> <p><b>Disconnected:</b> Port ma włączoną funkcję drzewa rozpinającego, ale nie jest połączony z żadnym urządzeniem.</p>                                                                                                                                                                                                                                                                                                                                                                                               |
| LAG         | <p>Wyświetla grupę LAG, do której należy port.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |

---

### 3.1.3 Konfiguracja globalna MSTP

Wybierz z menu **L2 FEATURES > Spanning Tree > STP Config > STP Config**, aby wyświetlić poniższą stronę.

Rys. 3-1 Konfiguracja globalna funkcji MSTP

**Global Config**

---

Spanning Tree:  Enable

Mode: MSTP

Apply

---

**Parameters Config**

CIST Priority: 36864 (0-61440, in increments of 4096)

Hello Time: 2 seconds (1-10)

Max Age: 20 seconds (6-40)

Forward Delay: 12 seconds (4-30)

Tx Hold Count: 5 pps (1-20)

Max Hops: 20 hop (1-40)

Apply

Aby skonfigurować MSTP globalnie, wykonaj poniższe kroki.

1) W sekcji **Parameters Config** skonfiguruj parametry globalne MSTP i kliknij **Apply**.

|                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>CIST Priority</b> | <p>Wyznacz priorytet CIST dla przełącznika. Priorytet CIST jest parametrem wykorzystywanym do ustawienia mostu głównego w drzewie rozpinającym. Przełącznik o niższej wartości ma wyższy priorytet.</p> <p>W przypadku STP/RSTP, priorytet CIST jest priorytetem przełącznika w drzewie rozpinającym. Przełącznik o najwyższym priorytecie wybrany zostanie mostem głównym.</p> <p>W przypadku MSTP, priorytet CISP jest priorytetem przełącznika w CIST. Przełącznik z najwyższym priorytetem wybrany zostanie mostem głównym w CIST.</p> |
| <b>Hello Time</b>    | <p>Wyznacz odstęp czasu wysyłania ramek BPDU. Wartość domyślna to 2. Most główny wysyła konfiguracyjne ramki BPDU w odstępie czasu powitania (Hello Time). Pracuje z wiekiem maksymalnym (MAX Age), aby przetestować błędy łącza i utrzymać drzewo rozpinające.</p>                                                                                                                                                                                                                                                                        |
| <b>Max Age</b>       | <p>Wyznacz maks. czas, przez który przełącznik może czekać bez odbierania BPDU przed próbą odtworzenia nowego drzewa rozpinającego. Wartość domyślna to 20.</p>                                                                                                                                                                                                                                                                                                                                                                            |

|               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|---------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Forward Delay | Wyznacz odstęp czasu między zmianą stanu portu od słuchania do uczenia się. Wartość domyślna to 15. Funkcja wykorzystywana jest do zapobiegania wytwarzania przez sieć tymczasowych pętli w trakcie odtwarzania drzewa rozpinającego. Odstęp czasu przejścia portu od stanu uczenia się do stanu przekazywania to również Forward Delay.                                                                                                                              |
| Tx Hold Count | Wyznacz maksymalną liczbę ramek BPDU wysyłanych w jedną sekundę. Wartość domyślna to 5                                                                                                                                                                                                                                                                                                                                                                                |
| Max Hops      | Wyznacz maksymalną liczbę BPDU wysyłanych w obszar MST. Wartość domyślna to 20. Przełącznik odbiera BPDU, zmniejsza liczbę przeskoków generuje ramki BPDU o nowej wartości. Kiedy wartość przeskoku wyniesie zero, przełącznik odrzuci BPDU. Wartość ta może kontrolować skalę drzewa rozpinającego w obszarze MST.<br><br>Uwaga: Maks. liczba przeskoków to parametr konfigurowany w MSTP. Nie musisz go konfigurować, jeżeli tryb drzewa rozpinającego to STP/RSTP. |

### Uwaga:

Aby zapobiec częstemu migotaniu sieci (ang. flapping), upewnij się, że Hello Time, Forward Delay i Max Age są zgodne z poniższymi wzorami:

- $2 * (\text{Hello Time} + 1) \leq \text{Max Age}$
- $2 * (\text{Forward Delay} - 1) \geq \text{Max Age}$

2) W sekcji **Global Config** włącz funkcję Spanning-Tree, wybierz tryb STP jaki MSTP i kliknij **Apply**.

|               |                                                                                                                                                                                                                                                                                      |
|---------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Spanning-Tree | Zaznacz pole, aby włączyć funkcję drzewa rozpinającego globalnie.                                                                                                                                                                                                                    |
| Mode          | Ustaw tryb drzewa rozpinającego na STP/RSTP na przełączniku. Domyślnie ustawiony jest tryb STP.<br><br><b>STP:</b> Ustaw tryb drzewa rozpinającego na STP.<br><br><b>RSTP:</b> Ustaw tryb drzewa rozpinającego na RSTP.<br><br><b>MSTP:</b> Ustaw tryb drzewa rozpinającego na MSTP. |

### 3.1.4 Sprawdzanie konfiguracji MSTP

Wybierz z menu **Spanning Tree > STP Config > STP Summary**, aby wyświetlić następującą stronę.

Rys. 3-6 Sprawdzanie konfiguracji MSTP

**STP Summary**

---

|                       |                          |
|-----------------------|--------------------------|
| Spanning Tree:        | Enable                   |
| Spanning Tree Mode:   | MSTP                     |
| Local Bridge:         | 36864--00-0a-eb-13-a2-02 |
| Root Bridge:          | 36864--00-0a-eb-13-a2-02 |
| External Path Cost:   | 0                        |
| Regional Root Bridge: | 36864--00-0a-eb-13-a2-02 |
| Internal Path Cost:   | 0                        |
| Designated Bridge:    | 36864--00-0a-eb-13-a2-02 |
| Root Port:            | ---                      |
| Latest TC Time:       | 2006-01-01 08:00:45      |
| TC Count:             | 0                        |

**MSTP Instance Summary**

---

|                       |                               |
|-----------------------|-------------------------------|
| Instance ID:          | <input type="text" value=""/> |
| Instance Status:      | Disable                       |
| Local Bridge:         | ---                           |
| Regional Root Bridge: | ---                           |
| Internal Path Cost:   | ---                           |
| Designated Bridge:    | ---                           |
| Root Port:            | ---                           |
| Latest TC Time:       | ---                           |
| TC Count:             | ---                           |

Sekcja **STP Summary** przedstawia podsumowanie informacji dotyczących CIST:

|                           |                                                                                         |
|---------------------------|-----------------------------------------------------------------------------------------|
| <b>Spanning Tree</b>      | Informuje o stanie funkcji drzewa rozpinającego.                                        |
| <b>Spanning-Tree Mode</b> | Informuje o trybie drzewa rozpinającego.                                                |
| <b>Local Bridge</b>       | Informuje o bridge ID mostu lokalnego. Mostem lokalnym jest wykorzystywany przełącznik. |
| <b>Root Bridge</b>        | Informuje o bridge ID mostu głównego w CIST.                                            |
| <b>External Path Cost</b> | Informuje o koszcie ścieżki głównej z przełącznika do mostu głównego w CIST.            |

|                      |                                                                                                                                 |
|----------------------|---------------------------------------------------------------------------------------------------------------------------------|
| Regional Root Bridge | Informuje o bridge ID mostu głównego w IST.                                                                                     |
| Internal Path Cost   | Informuje o koszcie ścieżki wewnętrznej. Jest to koszt ścieżki głównej z wykorzystywanego przełącznika do mostu głównego w IST. |
| Designated Bridge    | Informuje o bridge ID mostu desygnowanego w CIST.                                                                               |
| Root Port            | Informuje o porcie głównym w CIST.                                                                                              |
| Latest TC Time       | Informuje o ostatnim czasie zmiany topologii.                                                                                   |
| TC Count             | Informuje o tym, ile razy zmieniła się topologia.                                                                               |

Sekcja **MSTP Instance Summary** przedstawia dane w instancjach MST:

|                      |                                                                                                                                        |
|----------------------|----------------------------------------------------------------------------------------------------------------------------------------|
| Instance ID          | Wybierz odpowiednią instancję.                                                                                                         |
| Instance Status      | Informuje o statusie wybranej instancji.                                                                                               |
| Local Bridge         | Informuje o bridge ID przełącznika lokalnego. Most lokalny to wykorzystywany przełącznik.                                              |
| Regional Root Bridge | Informuje o bridge ID mostu głównego w wybranej instancji.                                                                             |
| Internal Path Cost   | Informuje o koszcie ścieżki wewnętrznej. Jest to koszt ścieżki głównej z wykorzystywanego przełącznika to głównego mostu regionalnego. |
| Designated Bridge    | Informuje o bridge ID mostu desygnowanego w wybranej instancji.                                                                        |
| Root Port            | Informuje o porcie głównym wybranej instancji.                                                                                         |
| Latest TC Time       | Informuje o ostatnim czasie zmiany topologii.                                                                                          |
| TC Count             | Informuje o tym, ile razy zmieniła się topologia.                                                                                      |

## 3.2 Przez CLI

### 3.2.1 Konfiguracja parametrów na portach w CIST

Aby skonfigurować parametry portu w CIST, wykonaj poniższe kroki:

|        |                                                                                                                                                                                                                                                                                                                                                                      |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Krok 1 | <b>configure</b><br>Uruchom tryb konfiguracji globalnej.                                                                                                                                                                                                                                                                                                             |
| Krok 2 | <b>interface {fastEthernet <i>port</i>   range fastEthernet <i>port-list</i>   gigabitEthernet <i>port</i>   range gigabitEthernet <i>port-list</i>   ten-gigabitEthernet <i>port</i>   range ten-gigabitEthernet <i>port-list</i>   port-channel <i>port-channel-id</i>   range port-channel <i>port-channel-list</i>}</b><br>Uruchom tryb konfiguracji interfejsu. |



**Krok 3** **spanning-tree**

Włącz funkcję drzewa rozpinającego dla wybranych portów.

**Krok 4** **spanning-tree common-config [ port-priority *pri* ] [ ext-cost *ext-cost* ] [ int-cost *int-cost* ] [ portfast { enable | disable } ] [ point-to-point { auto | open | close } ]**

Skonfiguruj parametry na portach w CIST.

*pri*: Wyznacz Priorytet dla wybranego portu. Wartość powinna być całkowitą wielokrotnością liczby 16 i mieścić się w zakresie od 0 do 240. Wartość domyślna to 128. Porty z mniejszymi wartościami ma ją wyższy priorytet. Jeżeli ścieżka główna portu jest taka sama jak ścieżka innych portów, przełącznik porówna priorytety portów i wybierze port główny z najwyższym priorytetem.

*ext-cost*: Wyznacz wartość kosztu ścieżki zewnętrznej. Wartość powinna mieścić się w zakresie od 0 do 2000000. Domyślnie ustawiona jest opcja Auto - port automatycznie wylicza koszt ścieżki zewnętrznej, w zależności od prędkości łącza portu.

W przypadku STP/RSTP koszt ścieżki zewnętrznej wskazuje koszt ścieżki portu w drzewie rozpinającym. Port z najniższym kosztem ścieżki głównej zostanie wybrany na port główny przełącznika.

W przypadku MSTP koszt ścieżki zewnętrznej wskazuje koszt ścieżki portu w CST.

*int-cost*: Wyznacz wartość kosztu ścieżki wewnętrznej. Wartość powinna mieścić się w zakresie od 0 do 2000000. Domyślnie ustawiona jest opcja Auto - port automatycznie wylicza koszt ścieżki zewnętrznej, w zależności od prędkości łącza portu. Parametr ten stosuje się jedynie w MSTP.

W przypadku MSTP koszt ścieżki wewnętrznej wykorzystywany jest do wyliczania kosztu ścieżki w IST. Port z najniższym kosztem ścieżki głównej zostanie wybrany na port główny przełącznika w IST.

**portfast { enable | disable }**: Wybierz Enable (Włącz), aby ustawić port jako końcowy. Funkcja jest domyślnie wyłączona. W przypadku zmiany topologii port końcowy może zmienić swój stan z blokowania do przekazywania. Dla szybkiego generowania drzewa rozpinającego zaleca się ustawienie portów połączonych z urządzeniami końcowymi jako porty końcowe.

**point-to-point { auto | open | close }**: Wybierz stan łącza P2P (Point-to-Point), do którego podłączone są porty. Podczas regeneracji drzewa rozpinającego, jeżeli port łącza P2P wybrany jest jako port główny lub port desygnowany, może on zmienić swój stan na przekazywanie. Opcja **Auto** oznacza, że przełącznik sprawdza automatycznie, czy port podłączony jest do łącza P2P i ustawia status na Open lub Closed. **Open wskazuje na to, że** port ustawiony jest jako podłączony do łącza P2P; **Close** - Port ustawiony jest jako niepodłączony do łącza P2P.

**Krok 5** **spanning-tree mcheck**

(Opcjonalnie) Przeprowadź MCheck na porcie.

Jeżeli port na urządzeniu RSTP-enabled/MSTP-enabled podłączony jest do urządzenia STP-enabled, port przełączy się do trybu kompatybilności z STP i będzie wysyłał pakiety w formacie STP. MCheck pozwala z powrotem przełączyć tryb portu na RSTP/MSTP po odłączeniu portu od urządzenia STP-enabled. Konfigurację MCheck przeprowadzić można tylko raz, po tym status MCheck portu zmieni się na Disabled (wył.).

Krok 6 **show spanning-tree interface [ fastEthernet *port* | gigabitEthernet *port* | ten-gigabitEthernet *port* | port-channel *lagid* ] [ edge | ext-cost | int-cost | mode | p2p | priority | role | state | status ]**  
(Opcjonalnie) Sprawdź dane wszystkich portów lub wybranego portu.

*port*: Określ numer portu.

*lagid*: Określ ID grupy LAG.

ext-cost | int-cost | mode | p2p | priority | role | state | status: Pokaż określone informacje.

Krok 7 **end**  
Powróć do trybu privileged EXEC.

Krok 8 **copy running-config startup-config**  
Zapisz ustawienia w pliku konfiguracyjnym.

Poniższy przykład prezentuje włączanie funkcji Spanning Tree dla portu 1/0/3 i konfigurację priorytetu portu na 32 :

**Switch#configure**

**Switch(config)#interface gigabitEthernet 1/0/3**

**Switch(config-if)#spanning-tree**

**Switch(config-if)#spanning-tree common-config port-priority 32**

**Switch(config-if)#show spanning-tree interface gigabitEthernet 1/0/3**

MST-Instance 0 (CIST)

| Interface | State  | Prio | Ext-Cost | Int-Cost | Edge | P2p      | Mode  | Role  | Status |
|-----------|--------|------|----------|----------|------|----------|-------|-------|--------|
| -----     | -----  | ---- | -----    | -----    | ---- | -----    | ----- | ----- | -----  |
| Gi1/0/3   | Enable | 32   | Auto     | Auto     | No   | No(auto) | N/A   | N/A   | LnkDwn |

MST-Instance 5

| Interface | Prio  | Cost  | Role  | Status |
|-----------|-------|-------|-------|--------|
| -----     | ----- | ----- | ----- | -----  |
| Gi1/0/3   | 144   | 200   | N/A   | LnkDwn |

**Switch(config-if)#end**

**Switch#copy running-config startup-config**

## 3.2.2 Konfiguracja regionu MSTP

### ■ Konfiguracja regionu MST

Aby skonfigurować region MST i priorytet przełącznika w instancji, wykonaj poniższe kroki:

|        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Krok 1 | <b>configure</b><br>Uruchom tryb konfiguracji globalnej.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Krok 2 | <b>spanning-tree mst instance <i>instance-id</i> priority <i>pri</i></b><br>Skonfiguruj priorytet przełącznika w instancji.<br><br><i>instance-id</i> : <b>Określ</b> ID instancji. Wartość powinna wynosić od 1 do 8.<br><br><i>pri</i> : Określ priorytet przełącznika w odpowiadającej instancji. Wartość musi mieścić się w zakresie od 0 do 61440 i powinna być podzielna przez 4096. Priorytet jest parametrem wykorzystywanym do określenia mostu głównego instancji. Przełącznik z niższą wartością ma wyższy priorytet, a przełącznik z najwyższym priorytetem zostanie wybrany na most główny w odpowiadającej instancji. |
| Krok 3 | <b>spanning-tree mst configuration</b><br>Uruchom tryb konfiguracji MST, żeby skonfigurować mapowanie VLAN do instancji, nazwę regionu i poziom weryfikacji.                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Krok 4 | <b>name <i>name</i></b><br>Skonfiguruj nazwę regionu.<br><br><i>name</i> : Określ nazwę regionu, wykorzystywaną do identyfikacji regionu MST. Wartość musi zawierać od 1 do 32 znaków.                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Krok 5 | <b>revision <i>revision</i></b><br>Skonfiguruj poziom weryfikacji regionu.<br><br><i>revision</i> : Określ poziom weryfikacji regionu. Wartość powinna mieścić się w zakresie od 0 do 65535.                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Krok 6 | <b>instance <i>instance-id</i> vlan <i>vlan-id</i></b><br>Skonfiguruj mapowanie VLAN do instancji.<br><br><i>instance-id</i> : Określ ID instancji. Wartość powinna wynosić od 1 do 8.<br><br><i>vlan-id</i> : <b>Określ</b> VLAN mapowaną do odpowiedniej instancji.                                                                                                                                                                                                                                                                                                                                                               |
| Krok 7 | <b>show spanning-tree mst { configuration [ digest ]   instance <i>instance-id</i> [ interface [ fastEthernet <i>port</i>   gigabitEthernet <i>port</i>   port-channel <i>lagid</i>   ten-gigabitEthernet <i>port</i> ] ] }</b><br>(Opcjonalnie) Podejrzyj powiązane dane instancji MSTP.<br><br><i>digest</i> : <b>Zaznacz wyświetlanie skrótu wyliczonego przez mapę VLAN do instancji.</b><br><br><i>instance-id</i> : <b>Określ instancję</b> ID, którą chcesz wyświetlić, w zakresie od 1 do 8.<br><br><i>port</i> : Określ numer portu.<br><br><i>lagid</i> : Określ numer ID grupy LAG.                                      |

---

Krok 8     **end**  
Powróć do trybu privileged EXEC.

---

Krok 9     **copy running-config startup-config**  
Zapisz ustawienia w pliku konfiguracyjnym.

---

Poniższy przykład prezentuje tworzenie regionu MST o nazwie R1, poziomie weryfikacji 100, w którym VLAN 2-VLAN 6 są mapowane do instancji 5:

**Switch#configure**

**Switch(config)#spanning-tree mst configuration**

**Switch(config-mst)#name R1**

**Switch(config-mst)#revision 100**

**Switch(config-mst)#instance 5 vlan 2-6**

**Switch(config-mst)#show spanning-tree mst configuration**

Region-Name : R1

Revision : 100

| MST-Instance | Vlans-Mapped |
|--------------|--------------|
| -----        | -----        |
| 0            | 1,7-4094     |
| 5            | 2-6,         |
| -----        | -----        |

**Switch(config-mst)#end**

**Switch#copy running-config startup-config**

- Konfiguracja parametrów na portach w instancji

Aby skonfigurować priorytet i koszt ścieżki portów w określonej instancji, wykonaj poniższe kroki:

---

Krok 1     **configure**  
Uruchom tryb konfiguracji globalnej.

---

Krok 2     **interface {fastEthernet port | range fastEthernet port-list | gigabitEthernet port | range gigabitEthernet port-list | ten-gigabitEthernet port | range ten-gigabitEthernet port-list | port-channel port-channel-id | range port-channel port-channel-list}**  
Uruchom tryb konfiguracji interfejsu.

---

**Krok 3** `spanning-tree mst instance instance-id [[ port-priority pri ] | [ cost cost ]]`

Skonfiguruj priorytet i koszt ścieżki portów w wyznaczonej instancji.

*instance-id*: Określ ID instancji, wartość powinna wynosić od 1 do 8.

*pri*: Wartość powinna być całkowitą wielokrotnością liczby 16, mieszczącą się w zakresie od 0 do 240. Wartość domyślna to 128. Port z mniejszą wartością ma wyższy priorytet. Jeżeli ścieżka główna portu jest taka sama jak ścieżka innych portów, przełącznik porówna priorytety portów i wybierze port główny z najwyższym priorytetem.

*cost*: Wpisz wartość kosztu ścieżki w odpowiadającej instancji. Wartość musi mieścić się między 0 a 2000000. Domyślnie ustawiona jest opcja Auto - port automatycznie wylicza koszt ścieżki zewnętrznej, w zależności od prędkości łącza portu. Port z najniższym kosztem ścieżki głównej zostanie wybrany na port główny przełącznika.

**Krok 4** `show spanning-tree mst { configuration [ digest ] | instance instance-id [ interface [ fastEthernet port | gigabitEthernet port | port-channel lagid | ten-gigabitEthernet port ] ] }`

(Opcjonalnie) Podejrzyj powiązane dane instancji MSTP.

*digest*: **Zaznacz wyświetlanie skrótu wyliczonego przez mapę VLAN do instancji.**

*instance-id*: Określ ID instancji, którą chcesz wyświetlić, w zakresie od 1 do 8.

*port*: Określ numer portu.

*lagid*: Określ ID grupy LAG.

**Krok 5** `end`

Powróć do trybu privileged EXEC.

**Krok 6** `copy running-config startup-config`

Zapisz ustawienia w pliku konfiguracyjnym.

Poniższy przykład prezentuje konfigurację priorytetu na 144, kosztu ścieżki portu 1/0/3 na 200 w instancji 5:

**Switch#configure****Switch(config)#interface gigabitEthernet 1/0/3****Switch(config-if)#spanning-tree mst instance 5 port-priority 144 cost 200****Switch(config-if)#show spanning-tree interface gigabitEthernet 1/0/3**

## MST-Instance 0 (CIST)

| Interface | State  | Prio | Ext-Cost | Int-Cost | Edge | P2p      | Mode  | Role | Status | LAG  |
|-----------|--------|------|----------|----------|------|----------|-------|------|--------|------|
| -----     | -----  | ---- | -----    | -----    | ---- | -----    | ----- | ---- | -----  | ---- |
| Gi1/0/3   | Enable | 32   | Auto     | Auto     | No   | No(auto) | N/A   | N/A  | LnkDwn | N/A  |

## MST-Instance 5

| Interface | Prio  | Cost  | Role  | Status | LAG   |
|-----------|-------|-------|-------|--------|-------|
| -----     | ----- | ----- | ----- | -----  | ----- |
| Gi1/0/3   | 144   | 200   | N/A   | LnkDwn | N/A   |

```
Switch(config-if)#end
```

```
Switch#copy running-config startup-config
```

### 3.2.3 Konfiguracja globalnych parametrów MSTP

Aby skonfigurować parametry globalne MSTP przełącznika, wykonaj poniższe kroki:

---

|        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Krok 1 | <b>configure</b><br>Uruchom tryb konfiguracji globalnej.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Krok 2 | <b>spanning-tree priority <i>pri</i></b><br>Skonfiguruj priorytet przełącznika dla porównania w CIST.<br><i>pri</i> : Określ priorytet przełącznika. Wartość musi mieścić się w zakresie od 0 do 61440 i powinna być podzielna przez 4096. Priorytet jest parametrem wykorzystywanym do określenia mostu głównego drzewa rozpinającego. Przełącznik z niższą wartością ma wyższy priorytet.<br>W przypadku STP/RSTP wartość jest priorytetem przełącznika w drzewie rozpinającym. Przełącznik z najwyższym priorytetem zostanie wybrany na most główny.<br>W przypadku MSTP wartość jest priorytetem przełącznika w CIST. Przełącznik z wyższym priorytetem zostanie wybrany na most główny w CIST.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Krok 3 | <b>spanning-tree timer</b> <b>[ [ forward-time <i>forward-time</i> ] [ hello-time <i>hello-time</i> ] [ max-age <i>max-age</i> ]]</b><br>(Opcjonalnie) Skonfiguruj Forward Delay, Hello Time i Max Age.<br><i>forward-time</i> : Wyznacz odstęp czasu między zmianą stanu portu od słuchania do uczenia się. Wartość powinna wynosić od 4 do 30 s. Wartość domyślna to 15. Funkcja wykorzystywana jest do zapobiegania wytwarzania przez sieć tymczasowych pętli w trakcie odtwarzania drzewa rozpinającego. Odstęp czasu przejścia portu od stanu uczenia się do stanu przekazywania to również Forward Delay.<br><i>hello-time</i> : Wyznacz wartość Hello Time, czyli odstęp czasu pomiędzy wysyłaniem ramek BPDU. Wartość powinna mieścić się w zakresie między 1 a 10 s. Wartość domyślna to 2. Most główny wysyła konfiguracyjne ramki BPDU w odstępie czasu powitania (Hello Time). Pracuje z wiekiem maksymalnym (MAX Age), aby przetestować błędy łącza i utrzymać drzewo rozpinające.<br><i>max-age</i> : Wyznacz maks. czas, przez który przełącznik może czekać bez odbierania BPDU przed próbą odtworzenia nowego drzewa rozpinającego. Wartość powinna wynosić od 6 do 40 s. Wartość domyślna to 20. |
| Krok 4 | <b>spanning-tree hold-count <i>value</i></b><br>Określ maksymalną liczbę ramek BPDU wysyłanych na sekundę.<br><i>value</i> : Określ maksymalną liczbę pakietów BPDU wysyłanych na sekundę. Wartość powinna wynosić od 1 do 20 p/s. Wartość domyślna to 5.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |

---

**Krok 5** `spanning-tree max-hops value`

(Opcjonalnie) Wyznacz maksymalną liczbę przeskoków BPDU przesyłanych w region MST. Przełącznik odbiera BPDU, obniża liczbę przeskoków i generuje BPDU z nową wartością. Jeżeli przeskok osiągnie wartość zero, przełącznik odrzuci BPDU. Wartość ta może kontrolować skalę drzewa rozpinającego w regionie MST.

*value*: Określ maks. liczbę przeskoków pojawiających się w określonym regionie przed odrzuceniem BPDU. Wartość powinna wynosić od 1 do 40 w przeskoku, wartość domyślna to 20.

**Krok 6** `show spanning-tree bridge`

(Opcjonalnie) Sprawdź parametry globalne przełącznika.

**Krok 7** `end`

Powróć do trybu privileged EXEC.

**Krok 8** `copy running-config startup-config`

Zapisz ustawienia w pliku konfiguracyjnym.

 **Uwaga:**

Aby zapobiec częstemu migotaniu sieci (ang. flapping), upewnij się, że Hello Time, Forward Delay i Max Age są zgodne z poniższymi wzorami.

- $2 * (\text{Hello Time} + 1) \leq \text{Max Age}$
- $2 * (\text{Forward Delay} - 1) \geq \text{Max Age}$

Poniższy przykład prezentuje konfigurację priorytetu CIST na 36864, Forward Delay na 12 sekund, Hold Count na 8 i Max Hop na 25:

```
Switch#configure
```

```
Switch(config)#spanning-tree priority 36864
```

```
Switch(config-if)#spanning-tree timer forward-time 12
```

```
Switch(config-if)#spanning-tree hold-count 8
```

```
Switch(config-if)#spanning-tree max-hops 25
```

```
Switch(config-if)#show spanning-tree bridge
```

| State  | Mode  | Priority | Hello-Time | Fwd-Time | Max-Age | Hold-Count | Max-Hops |
|--------|-------|----------|------------|----------|---------|------------|----------|
| -----  | ----- | -----    | -----      | -----    | -----   | -----      | -----    |
| Enable | Mstp  | 36864    | 2          | 12       | 20      | 8          | 25       |

```
Switch(config-if)#end
```

```
Switch#copy running-config startup-config
```

### 3.2.4 Włączanie globalnie funkcji Spanning Tree

Aby skonfigurować tryb drzewa rozpinającego (spanning tree mode) na MSTP i włączyć funkcję drzewa rozpinającego globalnie, wykonaj poniższe kroki:

|        |                                                                                                                                               |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------|
| Krok 1 | <b>configure</b><br>Uruchom tryb konfiguracji globalnej.                                                                                      |
| Krok 2 | <b>spanning-tree mode mstp</b><br>Skonfiguruj tryb drzewa rozpinającego na MSTP.<br><i>mstp</i> : Określ tryb drzewa rozpinającego jako MSTP. |
| Krok 3 | <b>spanning-tree</b><br>Włącz funkcję drzewa rozpinającego globalnie.                                                                         |
| Krok 4 | <b>show spanning-tree active</b><br>(Opcjonalnie) Podejrzyj dane aktywne MSTP.                                                                |
| Krok 5 | <b>end</b><br>Powróć do trybu privileged EXEC.                                                                                                |
| Krok 6 | <b>copy running-config startup-config</b><br>Zapisz ustawienia w pliku konfiguracyjnym.                                                       |

Poniższy przykład prezentuje konfigurację trybu drzewa rozpinającego na MSTP i globalne włączanie funkcji Spanning Tree :

```
Switch#configure
```

```
Switch(config)#spanning-tree mode mstp
```

```
Switch(config)#spanning-tree
```

```
Switch(config)#show spanning-tree active
```

```
Spanning tree is enabled
```

```
Spanning-tree's mode: MSTP (802.1s Multiple Spanning Tree Protocol)
```

```
Latest topology change time: 2006-01-04 10:47:42
```

```
MST-Instance 0 (CIST)
```

```
Root Bridge
```

```
Priority : 32768
```

```
Address : 00-0a-eb-13-23-97
```

```
External Cost : 200000
```

```
Root Port : Gi/0/20
```

```
Designated Bridge
```



Priority : 32768

Address : 00-0a-eb-13-23-97

Regional Root Bridge

Priority : 36864

Address : 00-0a-eb-13-12-ba

Local bridge is the regional root bridge

Local Bridge

Priority : 36864

Address : 00-0a-eb-13-12-ba

| Interface | State  | Prio | Ext-Cost | Int-Cost | Edge | P2p       | Mode | Role | Status |
|-----------|--------|------|----------|----------|------|-----------|------|------|--------|
| Gi/0/16   | Enable | 128  | 200000   | 200000   | No   | Yes(auto) | Mstp | Altn | Blk    |
| Gi/0/20   | Enable | 128  | 200000   | 200000   | No   | Yes(auto) | Mstp | Root | Fwd    |

MST-Instance 1

Root Bridge

Priority : 32768

Address : 00-0a-eb-13-12-ba

Local bridge is the root bridge

Designated Bridge

Priority : 32768

Address : 00-0a-eb-13-12-ba

Local Bridge

Priority : 32768

Address : 00-0a-eb-13-12-ba

| Interface | Prio | Cost   | Role | Status |
|-----------|------|--------|------|--------|
| Gi/0/16   | 128  | 200000 | Altn | Blk    |
| Gi/0/20   | 128  | 200000 | Mstr | Fwd    |

**Switch(config)#end**

**Switch#copy running-config startup-config**

# 4 Konfiguracja zabezpieczeń STP

## 4.1 Przez GUI

Wybierz z menu **L2 FEATURES > Spanning Tree > STP Security**, aby wyświetlić poniższą stronę.

Rys. 4-1 Konfiguracja zabezpieczeń portów

Port Protect

UNIT1

LAGS

| <input type="checkbox"/>            | Port   | Loop Protect | Root Protect | TC Guard | BPDU Protect | BPDU Filter | BPDU Forward | LAG |
|-------------------------------------|--------|--------------|--------------|----------|--------------|-------------|--------------|-----|
| <input checked="" type="checkbox"/> | 1/0/1  | Disabled     | Disabled     | Disabled | Disabled     | Disabled    | Enabled      | --- |
| <input type="checkbox"/>            | 1/0/2  | Disabled     | Disabled     | Disabled | Disabled     | Disabled    | Enabled      | --- |
| <input type="checkbox"/>            | 1/0/3  | Disabled     | Disabled     | Disabled | Disabled     | Disabled    | Enabled      | --- |
| <input type="checkbox"/>            | 1/0/4  | Disabled     | Disabled     | Disabled | Disabled     | Disabled    | Enabled      | --- |
| <input type="checkbox"/>            | 1/0/5  | Disabled     | Disabled     | Disabled | Disabled     | Disabled    | Enabled      | --- |
| <input type="checkbox"/>            | 1/0/6  | Disabled     | Disabled     | Disabled | Disabled     | Disabled    | Enabled      | --- |
| <input type="checkbox"/>            | 1/0/7  | Disabled     | Disabled     | Disabled | Disabled     | Disabled    | Enabled      | --- |
| <input type="checkbox"/>            | 1/0/8  | Disabled     | Disabled     | Disabled | Disabled     | Disabled    | Enabled      | --- |
| <input type="checkbox"/>            | 1/0/9  | Disabled     | Disabled     | Disabled | Disabled     | Disabled    | Enabled      | --- |
| <input type="checkbox"/>            | 1/0/10 | Disabled     | Disabled     | Disabled | Disabled     | Disabled    | Enabled      | --- |

Total: 10
1 entry selected.

Cancel
Apply

Skonfiguruj funkcje ochrony portów na wybranych portach i kliknij **Apply**.

### UNIT

Wybierz jednostkę lub grupy LAG, które chcesz skonfigurować.

### Loop Protect

Włącz lub wyłącz Loop Protect. Zaleca się włączenie funkcji na portach głównych i portach zastępczych.

W przypadku przeciążenia lub usterek łącza w sieci przełącznik nie odbierze ramek BPDU z urządzeń upstream na czas. Funkcja Loop Protect służy do unikania pętli spowodowanych przeliczeniem w danej sytuacji. Przy włączonej funkcji Loop Protect port będzie czasowo przechodził w stan blokowania, po tym jak nie otrzyma ramek BPDU na czas.

---

|              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|--------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Root Protect | <p>Włącz lub wyłącz Root Protect. Zaleca się włączenie funkcji na portach desygnowanych mostu głównego.</p> <p>Przełączniki z błędnymi ustawieniami mogą produkować BPDU z wyższym priorytetem, niż BPDU mostu głównego, co będzie skutkowało ponownym przeliczeniem drzewa rozpinającego. Funkcja Root Protect pozwala zapewnić, że wybrany most główny nie straci swojej pozycji w powyższym scenariuszu. Przy włączonej funkcji port będzie czasowo przechodził w stan blokowania po otrzymaniu BPDU z wyższym priorytetem. Po dwóch opóźnieniach przekazywania, jeżeli port nie otrzyma innych BPDU z wysokim priorytetem, przejdzie w normalny stan.</p> |
| TC Guard     | <p>Włącz lub wyłącz funkcję TC Guard. Zaleca się włączenie funkcji na portach i przełącznikach, które nie są przełącznikami głównymi.</p> <p>Funkcja TC Guard służy do zapobiegania częstym zmianom tablicy adresów MAC przez przełącznik. Przy włączonej funkcji jeżeli przełącznik otrzyma TC-BPDU, nie będzie ich od razu przetwarzał. Przełącznik odczeka przez ustalony czas i przetworzy wszystkie TC-BPDU razem, po odebraniu pierwszego pakietu TC-BPDU, a następnie zresetuje czas.</p>                                                                                                                                                              |
| BPDU Protect | <p>Włącz lub wyłącz BPDU Protect. Zaleca się włączenie funkcji na portach końcowych.</p> <p>Porty końcowe w drzewie rozpinającym służą do łączenia się z urządzeniami końcowymi i, w standardowej sytuacji, nie otrzymują pakietów BPDU. Otrzymywanie BPDU przez porty końcowe może wskazywać na atak. Funkcja BPDU Protect służy do ochrony przełącznika przed takim zagrożeniem. Przy włączonej funkcji porty końcowe po otrzymaniu pakietu BPDU będą odrzucane, a sytuacja zostanie zaraportowana administratorowi. Jedynie administrator może przywrócić poprzedni stan portów.</p>                                                                       |
| BPDU Filter  | <p>Włącz lub wyłącz BPDU Filter. Zaleca się włączenie funkcji na portach końcowych.</p> <p>Przy włączonej funkcji BPDU filter port nie odbiera i nie przekazuje pakietów BPDU, ale rozsyła własne BPDU. BPDU Filter pozwala zapobiegać atakom na przełącznik (tak samo, jak funkcja BPDU Protect).</p>                                                                                                                                                                                                                                                                                                                                                        |
| BPDU Forward | <p>Opcjonalnie) Włącz funkcję BPDU Forward. Funkcja działa jedynie przy globalnym wyłączeniu funkcji drzewa rozpinającego.</p> <p>Przy włączonej funkcji BPDU forward, mimo wyłączonej funkcji Spanning Tree, port może nadal przesyłać BPDU drzewa rozpinającego.</p>                                                                                                                                                                                                                                                                                                                                                                                        |

---

## 4.2 Przez CLI

### 4.2.1 Konfiguracja zabezpieczeń STP

Aby skonfigurować dla portów funkcje Root protect, BPDU protect i BPDU filter, wykonaj poniższe kroki:

---

|        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Krok 1 | <b>configure</b><br>Uruchom tryb konfiguracji globalnej.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Krok 2 | <b>interface {fastEthernet <i>port</i>   range fastEthernet <i>port-list</i>   gigabitEthernet <i>port</i>   range gigabitEthernet <i>port-list</i>   ten-gigabitEthernet <i>port</i>   range ten-gigabitEthernet <i>port-list</i>   port-channel <i>port-channel-id</i>   range port-channel <i>port-channel-list</i>}</b><br>Uruchom tryb konfiguracji interfejsu.                                                                                                                                                                                                                                                                                                                         |
| Krok 3 | <b>spanning-tree guard loop</b><br>(Opcjonalnie) Włącz Loop Protect. Zaleca się włączenie funkcji na portach głównych i zastępczych.<br><br>W przypadku przeciążenia lub usterek łącza w sieci przełącznik nie odbierze ramek BPDU z urządzeń upstream na czas. Funkcja Loop Protect służy do unikania pętli spowodowanych przeliczeniem w danej sytuacji. Przy włączonej funkcji Loop Protect port będzie czasowo przechodził w stan blokowania, po tym jak nie otrzyma ramek BPDU na czas.                                                                                                                                                                                                 |
| Krok 4 | <b>spanning-tree guard root</b><br>(Opcjonalnie) Włącz Root Protect. Zaleca się włączenie funkcji na portach desygnowanych mostu głównego.<br><br>Przełączniki z błędnymi ustawieniami mogą produkować BPDU z wyższym priorytetem, niż BPDU mostu głównego, co będzie skutkowało ponownym przeliczeniem drzewa rozpinającego. Funkcja Root Protect pozwala zapewnić, że wybrany most główny nie straci swojej pozycji w powyższym scenariuszu. Przy włączonej funkcji port będzie czasowo przechodził w stan blokowania po otrzymaniu BPDU z wyższym priorytetem. Po dwóch opóźnieniach przekazywania, jeżeli port nie otrzyma innych BPDU z wysokim priorytetem, przejdzie w normalny stan. |
| Krok 5 | <b>spanning-tree guard tc</b><br>(Opcjonalnie) Włącz TC Guard. Zaleca się włączenie funkcji na portach i przełącznikach, które nie są przełącznikami głównymi.<br><br>Funkcja TC Guard służy do zapobiegania częstym zmianom tablicy adresów MAC przez przełącznik. Przy włączonej funkcji jeżeli przełącznik otrzyma TC-BPDU, nie będzie ich od razu przetwarzał. Przełącznik odczeka przez ustalony czas i przetworzy wszystkie TC-BPDU razem, po odebraniu pierwszego pakietu TC-BPDU, a następnie zresetuje czas.                                                                                                                                                                        |
| Krok 6 | <b>spanning-tree bpduguard</b><br>(Opcjonalnie) Włącz BPDU Protect. Zaleca się włączenie funkcji na portach końcowych.<br><br>Porty końcowe w drzewie rozpinającym służą do łączenia się z urządzeniami końcowymi i, w standardowej sytuacji, nie otrzymują pakietów BPDU. Otrzymywanie BPDU przez porty końcowe może wskazywać na atak. Funkcja BPDU Protect służy do ochrony przełącznika przed takim zagrożeniem. Przy włączonej funkcji porty końcowe po otrzymaniu pakietu BPDU będą odrzucane, a sytuacja zostanie zaraportowana administratorowi. Jedyne administrator może przywrócić poprzedni stan portów.                                                                         |

---

**Krok 7** **spanning-tree bpdudfilter**

(Opcjonalnie) Włącz lub wyłącz BPDU Filter. Zaleca się włączenie funkcji na portach końcowych.

Przy włączonej funkcji BPDU filter port nie odbiera i nie przekazuje pakietów BPDU, ale rozsyła własne BPDU. BPDU Filter pozwala zapobiegać atakom na przełącznik (tak samo, jak funkcja BPDU Protect).

**Krok 8** **spanning-tree bpduflood**

(Opcjonalnie) Włącz funkcję BPDU Forward. Funkcja działa jedynie przy globalnym wyłączeniu funkcji drzewa rozpinającego. Funkcja jest domyślnie włączona.

Przy włączonej funkcji BPDU forward, mimo wyłączonej funkcji Spanning Tree, port może nadal przysyłać BPDU drzewa rozpinającego.

**Krok 9** **show spanning-tree interface-security [ fastEthernet *port* | gigabitEthernet *port* | ten-gigabitEthernet *port* | port-channel *port-channel-id* ] [ bpdudfilter | bpduguard | bpduflood | loop | root | tc ]**

(Opcjonalnie) Sprawdź dane ochrony portów.

*port*: Określ numer portu.

*lagid*: Określ ID grupy LAG.

**Krok 10** **end**

Powróć do trybu privileged EXEC.

**Krok 11** **copy running-config startup-config**

Zapisz ustawienia w pliku konfiguracyjnym.

Poniższy przykład prezentuje włączanie funkcji Loop Protect, Root Protect, BPDU Filter i BPDU Protect na porcie 1/0/3:

```
Switch#configure
```

```
Switch(config)#interface gigabitEthernet 1/0/3
```

```
Switch(config-if)#spanning-tree guard loop
```

```
Switch(config-if)#spanning-tree guard root
```

```
Switch(config-if)#spanning-tree bpdudfilter
```

```
Switch(config-if)#spanning-tree bpduguard
```

```
Switch(config-if)#show spanning-tree interface-security gigabitEthernet 1/0/3
```

```
Interface BPDU-Filter BPDU-Guard Loop-Protect Root-Protect TC-Protect BPDU-Flood
```

```

```

| Interface | BPDU-Filter | BPDU-Guard | Loop-Protect | Root-Protect | TC-Protect | BPDU-Flood |
|-----------|-------------|------------|--------------|--------------|------------|------------|
| Gi1/0/3   | Enable      | Enable     | Enable       | Enable       | Disable    | Enable     |

```
Switch(config-if)#end
```

```
Switch#copy running-config startup-config
```

# 5 Przykład konfiguracji MSTP

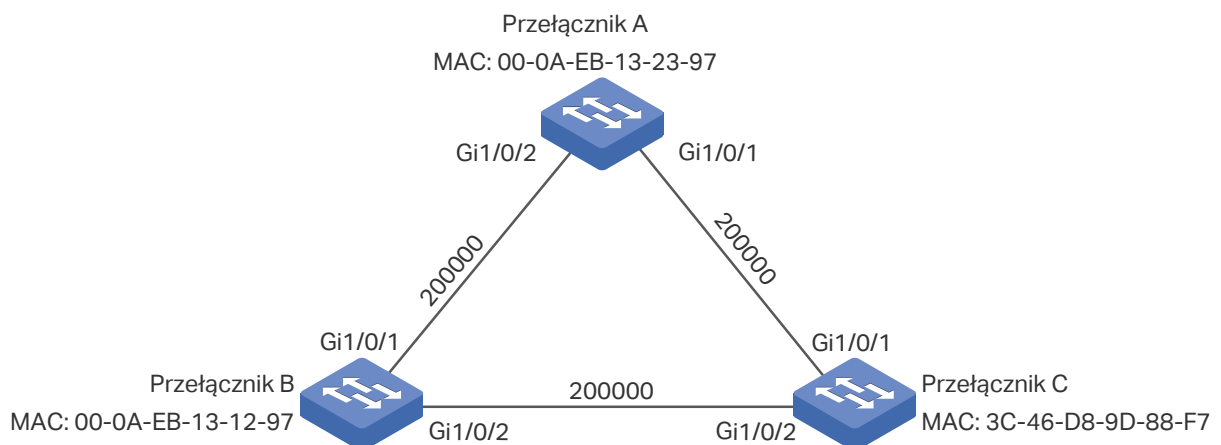
MSTP, kompatybilny wstecznie z STP i RSTP, może mapować VLAN-y do instancji w celu wdrożenia równoważenia obciążenia pasma, zapewniając tym samym większą elastyczność zarządzania siecią. W tym rozdziale omówimy przykładową konfigurację MSTP.

## 5.1 Wymagania sieciowe

Jak pokazano na Rys. 5-1, do sieci należą trzy przełączniki. W sieci tej przesyłany jest ruch VLAN 101-VLAN 106. Prędkość łącza pomiędzy tymi przełącznikami wynosi 100 Mb/s (domyślna wartość kosztu ścieżki portu to 200000).

Wymagane jest, aby ruch VLAN 101 - VLAN 103 oraz ruch VLAN 104 - VLAN 106 można było przesyłać poprzez inne ścieżki.

Rys. 5-1 Topologia sieci

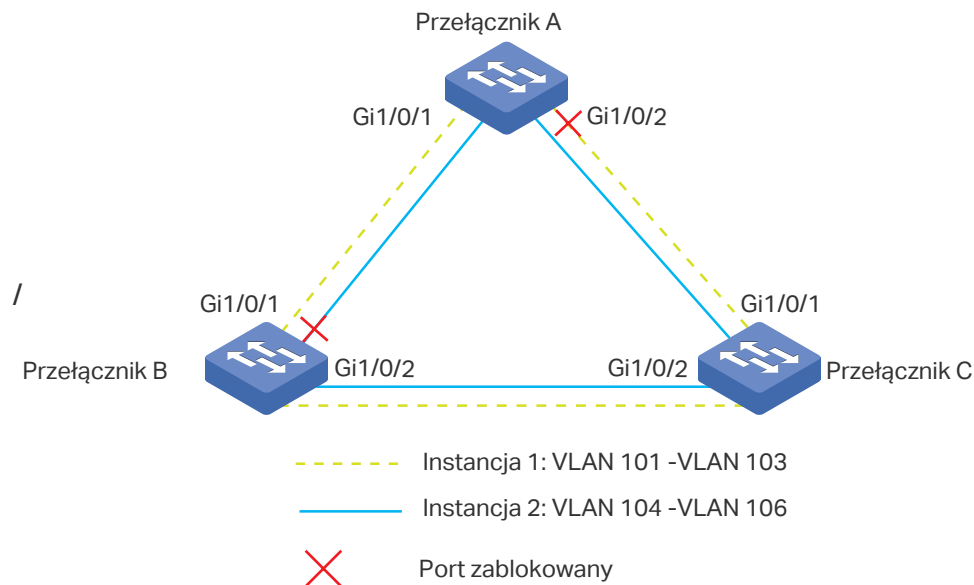


## 5.2 Schemat konfiguracji

Aby spełnić ten warunek, zaleca się skonfigurować funkcję MSTP na przełącznikach. Mapując VLAN-y do różnych instancji, umożliwia się przesyłanie ruchu przez odpowiadającą mu instancję.

Poniżej skonfigurujemy dwie instancje, co pozwoli na spełnienie warunku:

Rys. 5-2 Mapowanie VLAN do instancji



Konfiguracja wymaga podjęcia następujących działań:

- 1) Włącz funkcję Spanning Tree na portach każdego z przełączników.
- 2) Ustaw przynależność przełącznika A, przełącznika B i przełącznika C do tego samego regionu. Ustaw nazwę regionu jako 1, a poziom weryfikacji jako 100. Mapuj VLAN 101 - VLAN 103 do instancji 1, a VLAN 104 - VLAN 106 do instancji 2.
- 3) Ustaw priorytet przełącznika B jako 0, aby pełnił rolę urządzenia root bridge w instancji 1; ustaw priorytet przełącznika C jako 0, aby pełnił rolę urządzenia root bridge w instancji 2.
- 4) Skonfiguruj koszt ścieżki, aby zablokować określone porty. Dla instancji 1 skonfiguruj wartość kosztu ścieżki portu 1/0/1 przełącznika A tak, aby była wyższa niż domyślna wartość kosztu ścieżki (200000). Dla instancji 2 skonfiguruj wartość kosztu ścieżki portu 1/0/2 przełącznika B tak, aby była wyższa niż domyślna wartość kosztu ścieżki (200000).
- 5) Włącz funkcję MSTP na wszystkich przełącznikach.

## 5.3 Przez GUI

### ■ Konfiguracja dla przełącznika A

- 1) Wybierz z menu **L2 FEATURES > Spanning Tree > STP Config > Port Config**, aby wyświetlić poniższą stronę. Włącz funkcję spanning tree na porcie 1/0/1 i 1/0/2. Inne parametry pozostaną zgodne z ustawieniami domyślnymi. Kliknij **Apply**.

Rys. 5-3 Włączanie funkcji Spanning Tree na portach

Port Config

UNIT1 LAGS

| <input type="checkbox"/>            | Port   | Status   | Priority | Ext-Path Cost | Int-Path Cost | Edge Port | P2P Link | MCheck | Port Mode | Port I |
|-------------------------------------|--------|----------|----------|---------------|---------------|-----------|----------|--------|-----------|--------|
| <input checked="" type="checkbox"/> | 1/0/1  | Enabled  | 128      | Auto          | Auto          | Disabled  | Auto     | --     | --        | --     |
| <input checked="" type="checkbox"/> | 1/0/2  | Enabled  | 128      | Auto          | Auto          | Disabled  | Auto     | --     | --        | --     |
| <input type="checkbox"/>            | 1/0/3  | Disabled | 128      | Auto          | Auto          | Disabled  | Auto     | --     | --        | --     |
| <input type="checkbox"/>            | 1/0/4  | Disabled | 128      | Auto          | Auto          | Disabled  | Auto     | --     | --        | --     |
| <input type="checkbox"/>            | 1/0/5  | Disabled | 128      | Auto          | Auto          | Disabled  | Auto     | --     | --        | --     |
| <input type="checkbox"/>            | 1/0/6  | Disabled | 128      | Auto          | Auto          | Disabled  | Auto     | --     | --        | --     |
| <input type="checkbox"/>            | 1/0/7  | Disabled | 128      | Auto          | Auto          | Disabled  | Auto     | --     | --        | --     |
| <input type="checkbox"/>            | 1/0/8  | Disabled | 128      | Auto          | Auto          | Disabled  | Auto     | --     | --        | --     |
| <input type="checkbox"/>            | 1/0/9  | Disabled | 128      | Auto          | Auto          | Disabled  | Auto     | --     | --        | --     |
| <input type="checkbox"/>            | 1/0/10 | Disabled | 128      | Auto          | Auto          | Disabled  | Auto     | --     | --        | --     |

Total: 10 2 entries selected. Cancel Apply

- 2) Wybierz z menu **L2 FEATURES > Spanning Tree > MSTP Instance > Region Config**, aby wyświetlić poniższą stronę. Ustaw nazwę regionu jako 1, a poziom weryfikacji jako 100. Kliknij **Apply**.

Rys. 5-4 Konfiguracja regionu MST

Region Config

Region Name:

Revision:  (0-65535)

Apply

- 3) Wybierz z menu **L2 FEATURES > Spanning Tree > MSTP Instance > Instance Config**. Kliknij Add, mapuj VLAN101-VLAN103 do instancji 1 i ustaw priorytet jako 32768; mapuj VLAN104-VLAN106 do instancji 2 i ustaw priorytet jako 32768. Kliknij **Create**.

Rys. 5-5 Konfiguracja mapowania VLAN do instancji

Instance Config

Instance ID:  (1-8)

Priority:  (0-61440, in increments of 4096)

VLAN ID:  Add  Delete

(1-4094, format:1,3,4-7,11-30)

Cancel Create

- 4) Wybierz z menu **L2 FEATURES > Spanning Tree > MSTP Instance > Instance Port Config**, aby wyświetlić poniższą stronę. Ustaw koszt ścieżki portu 1/0/1 w instancji 1 jako 400000. Kliknij **Apply**.



Rys. 5-6 Konfiguracja kosztu ścieżki portu 1/0/1 w instancji 1

Instance Port Config

Instance ID:

| UNIT1                               | LAGS | Port   | Priority | Path Cost | Port Role | Port Status | LAG |
|-------------------------------------|------|--------|----------|-----------|-----------|-------------|-----|
| <input checked="" type="checkbox"/> |      | 1/0/1  | 128      | 400000    | --        | --          | --  |
| <input type="checkbox"/>            |      | 1/0/2  | 128      | Auto      | --        | --          | --  |
| <input type="checkbox"/>            |      | 1/0/3  | 128      | Auto      | --        | --          | --  |
| <input type="checkbox"/>            |      | 1/0/4  | 128      | Auto      | --        | --          | --  |
| <input type="checkbox"/>            |      | 1/0/5  | 128      | Auto      | --        | --          | --  |
| <input type="checkbox"/>            |      | 1/0/6  | 128      | Auto      | --        | --          | --  |
| <input type="checkbox"/>            |      | 1/0/7  | 128      | Auto      | --        | --          | --  |
| <input type="checkbox"/>            |      | 1/0/8  | 128      | Auto      | --        | --          | --  |
| <input type="checkbox"/>            |      | 1/0/9  | 128      | Auto      | --        | --          | --  |
| <input type="checkbox"/>            |      | 1/0/10 | 128      | Auto      | --        | --          | --  |

Total: 10 1 entry selected.

- 5) Wybierz z menu **L2 FEATURES > Spanning Tree > STP Config > STP Config**, aby wyświetlić poniższą stronę. Włącz globalnie funkcję MSTP. Pozostałe parametry globalne pozostaną zgodne z ustawieniami domyślnymi. **Kliknij Apply**.

Rys. 5-7 Konfiguracja globalnych parametrów MSTP przełącznika

Global Config

Spanning Tree:  Enable

Mode:

Parameters Config

CIST Priority:  (0-61440, in increments of 4096)


Hello Time:  seconds (1-10)

Max Age:  seconds (6-40)

Forward Delay:  seconds (4-30)

Tx Hold Count:  pps (1-20)

Max Hops:  (1-40)

- 6) Kliknij  **Save**, aby zapisać ustawienia.

#### ■ Konfiguracja dla przełącznika B

- 1) Wybierz z menu **L2 FEATURES > Spanning Tree > STP Config > Port Config**, aby wyświetlić poniższą stronę. Włącz funkcję spanning tree na porcie 1/0/1 i 1/0/2. Inne parametry pozostaną zgodne z ustawieniami domyślnymi. Kliknij **Apply**.

Rys. 5-8 Włączanie funkcji Spanning Tree na portach

Port Config

| UNIT1                               | LAGS | Port   | Status   | Priority | Ext-Path Cost | Int-Path Cost | Edge Port | P2P Link | MCheck | Port Mode | Port I |
|-------------------------------------|------|--------|----------|----------|---------------|---------------|-----------|----------|--------|-----------|--------|
|                                     |      |        | Enable ▾ |          |               |               |           |          |        |           |        |
| <input checked="" type="checkbox"/> |      | 1/0/1  | Enabled  | 128      | Auto          | Auto          | Disabled  | Auto     | --     | --        |        |
| <input checked="" type="checkbox"/> |      | 1/0/2  | Enabled  | 128      | Auto          | Auto          | Disabled  | Auto     | --     | --        |        |
| <input type="checkbox"/>            |      | 1/0/3  | Disabled | 128      | Auto          | Auto          | Disabled  | Auto     | --     | --        |        |
| <input type="checkbox"/>            |      | 1/0/4  | Disabled | 128      | Auto          | Auto          | Disabled  | Auto     | --     | --        |        |
| <input type="checkbox"/>            |      | 1/0/5  | Disabled | 128      | Auto          | Auto          | Disabled  | Auto     | --     | --        |        |
| <input type="checkbox"/>            |      | 1/0/6  | Disabled | 128      | Auto          | Auto          | Disabled  | Auto     | --     | --        |        |
| <input type="checkbox"/>            |      | 1/0/7  | Disabled | 128      | Auto          | Auto          | Disabled  | Auto     | --     | --        |        |
| <input type="checkbox"/>            |      | 1/0/8  | Disabled | 128      | Auto          | Auto          | Disabled  | Auto     | --     | --        |        |
| <input type="checkbox"/>            |      | 1/0/9  | Disabled | 128      | Auto          | Auto          | Disabled  | Auto     | --     | --        |        |
| <input type="checkbox"/>            |      | 1/0/10 | Disabled | 128      | Auto          | Auto          | Disabled  | Auto     | --     | --        |        |

Total: 10      2 entries selected.      Cancel      Apply

- 2) Wybierz z menu **L2 FEATURES > Spanning Tree > MSTP Instance > Region Config**, aby wyświetlić poniższą stronę. Ustaw nazwę regionu jako 1, a poziom weryfikacji jako 100. Kliknij **Apply**.

Rys. 5-9 Konfiguracja regionu

Region Config

Region Name:

Revision:  (0-65535)

Apply

- 3) Wybierz z menu **L2 FEATURES > Spanning Tree > MSTP Instance > Instance Config**. Kliknij Add, mapuj VLAN101-VLAN103 do instancji 1 i ustaw priorytet jako 0; mapuj VLAN104-VLAN106 do instancji 2 i ustaw priorytet jako 32768. Kliknij **Create**.

Rys. 5-10 Konfiguracja mapowania VLAN do instancji

Instance Config

Instance ID:  (1-8)

Priority:  (0-61440, in increments of 4096)

VLAN ID:  Add  Delete

(1-4094, format:1,3,4-7,11-30)

Cancel      Create

- 4) Wybierz z menu **L2 FEATURES > Spanning Tree > MSTP Instance > Instance Port Config**, aby wyświetlić poniższą stronę. Ustaw koszt ścieżki portu 1/0/2 w instancji 2 jako 400000. Kliknij **Apply**.

Rys. 5-11 Konfiguracja kosztu ścieżki portu 1/0/2 w instancji 2

Instance Port Config

Instance ID:

| UNIT1                               | LAGS | Port   | Priority | Path Cost | Port Role | Port Status | LAG |
|-------------------------------------|------|--------|----------|-----------|-----------|-------------|-----|
| <input type="checkbox"/>            |      | 1/0/1  | 128      | Auto      | --        | --          | --- |
| <input checked="" type="checkbox"/> |      | 1/0/2  | 128      | Auto      | --        | --          | --- |
| <input type="checkbox"/>            |      | 1/0/3  | 128      | Auto      | --        | --          | --- |
| <input type="checkbox"/>            |      | 1/0/4  | 128      | Auto      | --        | --          | --- |
| <input type="checkbox"/>            |      | 1/0/5  | 128      | Auto      | --        | --          | --- |
| <input type="checkbox"/>            |      | 1/0/6  | 128      | Auto      | --        | --          | --- |
| <input type="checkbox"/>            |      | 1/0/7  | 128      | Auto      | --        | --          | --- |
| <input type="checkbox"/>            |      | 1/0/8  | 128      | Auto      | --        | --          | --- |
| <input type="checkbox"/>            |      | 1/0/9  | 128      | Auto      | --        | --          | --- |
| <input type="checkbox"/>            |      | 1/0/10 | 128      | Auto      | --        | --          | --- |

Total: 10 1 entry selected.

- 5) Wybierz z menu **L2 FEATURES > Spanning Tree > STP Config > STP Config**, aby wyświetlić poniższą stronę. Włącz globalnie funkcję MSTP. Pozostałe parametry globalne pozostaną zgodne z ustawieniami domyślnymi. **Kliknij Apply**.

Rys. 5-12 Konfiguracja globalna MSTP

Global Config

Spanning Tree:  Enable

Mode:

Parameters Config

CIST Priority:  (0-61440, in increments of 4096)

Hello Time:  seconds (1-10)

Max Age:  seconds (6-40)

Forward Delay:  seconds (4-30)

Tx Hold Count:  pps (1-20)

Max Hops:  (1-40)

- 6) Kliknij  **Save**, aby zapisać ustawienia.

■ Konfiguracja dla przełącznika C

- 1) Wybierz z menu **L2 FEATURES > Spanning Tree > STP Config > Port Config**, aby wyświetlić poniższą stronę. Włącz funkcję spanning tree na porcie 1/0/1 i 1/0/2. Inne parametry pozostaną zgodne z ustawieniami domyślnymi. Kliknij **Apply**.

Rys. 5-13 Włączanie funkcji Spanning Tree na portach

Port Config

UNIT1 LAGS

| <input type="checkbox"/>            | Port   | Status   | Priority | Ext-Path Cost | Int-Path Cost | Edge Port | P2P Link | MCheck | Port Mode | Port I |
|-------------------------------------|--------|----------|----------|---------------|---------------|-----------|----------|--------|-----------|--------|
| <input checked="" type="checkbox"/> | 1/0/1  | Enabled  | 128      | Auto          | Auto          | Disabled  | Auto     | --     | --        |        |
| <input checked="" type="checkbox"/> | 1/0/2  | Enabled  | 128      | Auto          | Auto          | Disabled  | Auto     | --     | --        |        |
| <input type="checkbox"/>            | 1/0/3  | Disabled | 128      | Auto          | Auto          | Disabled  | Auto     | --     | --        |        |
| <input type="checkbox"/>            | 1/0/4  | Disabled | 128      | Auto          | Auto          | Disabled  | Auto     | --     | --        |        |
| <input type="checkbox"/>            | 1/0/5  | Disabled | 128      | Auto          | Auto          | Disabled  | Auto     | --     | --        |        |
| <input type="checkbox"/>            | 1/0/6  | Disabled | 128      | Auto          | Auto          | Disabled  | Auto     | --     | --        |        |
| <input type="checkbox"/>            | 1/0/7  | Disabled | 128      | Auto          | Auto          | Disabled  | Auto     | --     | --        |        |
| <input type="checkbox"/>            | 1/0/8  | Disabled | 128      | Auto          | Auto          | Disabled  | Auto     | --     | --        |        |
| <input type="checkbox"/>            | 1/0/9  | Disabled | 128      | Auto          | Auto          | Disabled  | Auto     | --     | --        |        |
| <input type="checkbox"/>            | 1/0/10 | Disabled | 128      | Auto          | Auto          | Disabled  | Auto     | --     | --        |        |

Total: 10 2 entries selected. Cancel Apply

- 2) Wybierz z menu **Spanning Tree > MSTP Instance > Region Config**, aby wyświetlić poniższą stronę. Ustaw nazwę regionu jako 1, a poziom weryfikacji jako 100. Kliknij **Apply**.

Rys. 5-14 Konfiguracja regionu

Region Config

Region Name:

Revision:  (0-65535)

Apply

- 3) Wybierz z menu **L2 FEATURES > Spanning Tree > MSTP Instance > Instance Config**. Kliknij Add, mapuj VLAN101-VLAN103 do instancji 1 i ustaw priorytet jako 32768; mapuj VLAN104-VLAN106 do instancji 2 i ustaw priorytet jako 0. Kliknij **Create**.

Rys. 5-15 Konfiguracja mapowania VLAN do instancji

Instance Config

Instance ID:  (1-8)

Priority:  (0-61440, in increments of 4096)

VLAN ID:  Add  Delete

(1-4094, format:1,3,4-7,11-30)

Cancel Create

- 4) Wybierz z menu **L2 FEATURES > Spanning Tree > STP Instance > STP Config**, aby wyświetlić poniższą stronę. Włącz globalnie funkcję MSTP. Pozostałe parametry globalne pozostaną zgodne z ustawieniami domyślnymi. Kliknij **Apply**.

Rys. 5-16 Konfiguracja globalna MSTP

Global Config

---

Spanning Tree:  Enable

Mode: MSTP ▼

Apply

---

Parameters Config

CIST Priority:  (0-61440, in increments of 4096)

Hello Time:  seconds (1-10)


Max Age:  seconds (6-40)

Forward Delay:  seconds (4-30)

Tx Hold Count:  pps (1-20)

Max Hops:  (1-40)

Apply

- 5) Kliknij  **Save**, aby zapisać ustawienia.

## 5.4 Przez CLI

### ■ Konfiguracja dla przełącznika A

- 1) Włącz funkcję spanning tree na porcie 1/0/1 i 1/0/2, a następnie ustaw path cost portu 1/0/1 w instancji 1 jako 400000.

```
Switch#configure
```

```
Switch(config)#interface gigabitEthernet 1/0/1
```

```
Switch(config-if)#spanning-tree
```

```
Switch(config-if)#spanning-tree mst instance 1 cost 400000
```

```
Switch(config-if)#exit
```

```
Switch(config)#interface gigabitEthernet 1/0/2
```

```
Switch(config-if)#spanning-tree
```

```
Switch(config-if)#exit
```

- 2) Ustaw region name jako 1, revision number jako 100; mapowanie VLAN101-VLAN103 do instancji 1; mapowanie VLAN104-VLAN106 do instancji 2:

```
Switch(config)#spanning-tree mst configuration
```

```
Switch(config-mst)#name 1
```

```
Switch(config-mst)#revision 100
```

```
Switch(config-mst)#instance 1 vlan 101-103
```

```
Switch(config-mst)#instance 2 vlan 104-106
```

```
Switch(config-mst)#exit
```

- 3) Ustaw tryb spanning tree jako MSTP, a następnie włącz globalnie funkcję spanning tree.

```
Switch(config)#spanning-tree mode mstp
```

```
Switch(config)#spanning-tree
```

```
Switch(config)#end
```

```
Switch#copy running-config startup-config
```

#### ■ Konfiguracja dla przełącznika B

- 1) Włącz funkcję spanning tree na porcie 1/0/1 i 1/0/2, a następnie ustaw path cost portu 1/0/2 w instancji 2 jako 400000.

```
Switch#configure
```

```
Switch(config)#interface gigabitEthernet 1/0/2
```

```
Switch(config-if)#spanning-tree
```

```
Switch(config-if)#spanning-tree mst instance 2 cost 400000
```

```
Switch(config-if)#exit
```

```
Switch(config)#interface gigabitEthernet 1/0/1
```

```
Switch(config-if)#spanning-tree
```

```
Switch(config-if)#exit
```

- 2) Ustaw region name jako 1, revision number jako 100; mapowanie VLAN101-VLAN103 do instancji 1; mapowanie VLAN104-VLAN106 do instancji 2; ustaw priority przełącznika B w instancji 1 jako 0, aby mógł on pełnić rolę root bridge w instancji 1:

```
Switch(config)#spanning-tree mst configuration
```

```
Switch(config-mst)#name 1
```

```
Switch(config-mst)#revision 100
```

```
Switch(config-mst)#instance 1 vlan 101-103
```

```
Switch(config-mst)#instance 2 vlan 104-106
```

```
Switch(config-mst)#exit
```

```
Switch(config)#spanning-tree mst instance 1 priority 0
```

- 3) Ustaw tryb spanning tree jako MSTP, a następnie włącz globalnie funkcję spanning tree.

```
Switch(config)#spanning-tree mode mstp
```

```
Switch(config)#spanning-tree
```

```
Switch(config)#end
```

```
Switch#copy running-config startup-config
```

- Konfiguracja dla przełącznika C

- 1) Włącz funkcję spanning tree na porcie 1/0/1 i 1/0/2.

```
Switch#configure
```

```
Switch(config)#interface range gigabitEthernet 1/0/1-2
```

```
Switch(config-if-range)#spanning-tree
```

```
Switch(config-if-range)#exit
```

- 2) Ustaw region name jako 1, revision number jako 100; mapowanie VLAN101-VLAN103 do instancji 1; mapowanie VLAN104-VLAN106 do instancji 2; ustaw priority przełącznika C w instancji 2 jako 0, aby mógł on pełnić rolę root bridge w instancji 2:

```
Switch(config)#spanning-tree mst configuration
```

```
Switch(config-mst)#name 1
```

```
Switch(config-mst)#revision 100
```

```
Switch(config-mst)#instance 1 vlan 101-103
```

```
Switch(config-mst)#instance 2 vlan 104-106
```

```
Switch(config-mst)#exit
```

```
Switch(config)#spanning-tree mst instance 2 priority 0
```

- 3) Ustaw tryb spanning tree jako MSTP, a następnie włącz globalnie funkcję spanning tree.

```
Switch(config)#spanning-tree mode mstp
```

```
Switch(config)#spanning-tree
```

```
Switch(config)#end
```

```
Switch#copy running-config startup-config
```

## Sprawdzanie konfiguracji

- Przełącznik A

Sprawdzanie konfiguracji przełącznika A w instancji 1:

```
Switch(config)#show spanning-tree mst instance 1
```

```
MST-Instance 1
```

```
Root Bridge
```

```
Priority :0
```

Address : 00-0a-eb-13-12-ba

Internal Cost : 400000

Root Port : 1

Designated Bridge

Priority : 0

Address : 00-0a-eb-13-12-ba

Local Bridge

Priority : 32768

Address : 00-0a-eb-13-23-97

| Interface | Prio | Cost   | Role  | Status | LAG  |
|-----------|------|--------|-------|--------|------|
| -----     | ---- | -----  | ----- | -----  | ---- |
| Gi1/0/1   | 128  | 400000 | Root  | Fwd    | N/A  |
| Gi1/0/2   | 128  | 200000 | Altn  | Blk    | N/A  |

Sprawdzanie konfiguracji przełącznika A w instancji 2:

Switch(config)#show spanning-tree mst instance 2

MST-Instance 2

Root Bridge

Priority : 0

Address : 3c-46-d8-9d-88-f7

Internal Cost : 200000

Root Port : 2

Designated Bridge

Priority : 0

Address : 3c-46-d8-9d-88-f7

Local Bridge

Priority : 32768

Address : 00-0a-eb-13-23-97



| Interface | Prio | Cost   | Role  | Status | LAG  |
|-----------|------|--------|-------|--------|------|
| -----     | ---- | -----  | ----- | -----  | ---- |
| Gi1/0/1   | 128  | 200000 | Desg  | Fwd    | N/A  |
| Gi1/0/2   | 128  | 200000 | Root  | Fwd    | N/A  |

- **Przełącznik B**

Sprawdzanie konfiguracji przełącznika B w instancji 1:

```
Switch(config)#show spanning-tree mst instance 1
```

```
MST-Instance 1
```

```
Root Bridge
```

```
Priority :0
```

```
Address :00-0a-eb-13-12-ba
```

```
Local bridge is the root bridge
```

```
Designated Bridge
```

```
Priority :0
```

```
Address :00-0a-eb-13-12-ba
```

```
Local Bridge
```

```
Priority :0
```

```
Address :00-0a-eb-13-12-ba
```

| Interface | Prio | Cost   | Role  | Status |
|-----------|------|--------|-------|--------|
| -----     | ---- | -----  | ----- | -----  |
| Gi1/0/1   | 128  | 200000 | Desg  | Fwd    |
| Gi1/0/2   | 128  | 200000 | Desg  | Fwd    |

Sprawdzanie konfiguracji przełącznika B w instancji 2:

```
Switch(config)#show spanning-tree mst instance 2
```

```
MST-Instance 2
```

```
Root Bridge
```

```
Priority :0
```

```
Address :3c-46-d8-9d-88-f7
```

```
Internal Cost : 400000
```

```

Root Port : 2
Designated Bridge
Priority : 0
Address : 3c-46-d8-9d-88-f7
Local Bridge
Priority : 32768
Address : 00-0a-eb-13-12-ba
Interface Prio Cost Role Status
----- ---- -
Gi1/0/1 128 200000 Altn Blk
Gi1/0/2 128 200000 Root Fwd

```

- **Przełącznik C**

Sprawdzanie konfiguracji przełącznika C w instancji 1:

```
Switch(config)#show spanning-tree mst instance 1
```

```
MST-Instance 1
```

```
Root Bridge
```

```
Priority : 0
```

```
Address : 00-0a-eb-13-12-ba
```

```
Internal Cost : 200000
```

```
Root Port : 2
```

```
Designated Bridge
```

```
Priority : 0
```

```
Address : 00-0a-eb-13-12-ba
```

```
Local Bridge
```

```
Priority : 32768
```

```
Address : 3c-46-d8-9d-88-f7
```

```

Interface Prio Cost Role Status
----- ---- -
Gi1/0/1 128 200000 Desg Fwd
Gi1/0/2 128 200000 Root Fwd

```

Sprawdzanie konfiguracji przełącznika C w instancji 2:

```
Switch(config)#show spanning-tree mst instance 2
```

```
MST-Instance 2
```

```
Root Bridge
```

```
Priority :0
```

```
Address : 3c-46-d8-9d-88-f7
```

```
Local bridge is the root bridge
```

```
Designated Bridge
```

```
Priority :0
```

```
Address : 3c-46-d8-9d-88-f7
```

```
Local Bridge
```

```
Priority :0
```

```
Address : 3c-46-d8-9d-88-f7
```

| Interface | Prio  | Cost   | Role  | Status |
|-----------|-------|--------|-------|--------|
| -----     | ----- | -----  | ----- | -----  |
| Gi1/0/1   | 128   | 200000 | Desg  | Fwd    |
| Gi1/0/2   | 128   | 200000 | Desg  | Fwd    |

# Część 14

## Konfiguracja LLDP

### ROZDZIAŁY

1. LLDP
2. Konfiguracja LLDP
3. Konfiguracja LLDP-MED
4. Przeglądanie ustawień LLDP
5. Przeglądanie ustawień LLDP-MED
6. Przykład konfiguracji

# 1 LLDP

## 1.1 Informacje ogólne

LLDP (Link Layer Discovery Protocol) to protokół wykrywania urządzeń sąsiadujących, który umożliwia urządzeniom sieciowym na przekazywanie informacji o sobie innym urządzeniom w sieci. Protokół ten opiera się na standardzie IEEE 802.1ab i działa w warstwie 2 (warstwa łącza danych), co pozwala na współpracę urządzeń sieciowych różnych producentów.

Po włączeniu funkcji LLDP przełącznik może pozyskiwać informacje o urządzeniach sąsiadujących, a administratorzy sieci mogą korzystać z NMS (Network Management System) do zbierania informacji, które umożliwiają im zorientowanie się jak wygląda topologia sieci, sprawdzanie połączeń sieciowych i rozwiązywanie problemów z siecią.

LLDP-MED (LLDP for Media Endpoint Discovery) jest rozszerzeniem protokołu LLDP i służy do wymiany informacji pomiędzy urządzeniami sieciowymi a urządzeniami końcowymi. Z funkcji tej korzysta się razem z Auto VoIP (Voice over Internet Protocol), co pozwala urządzeniu VoIP na dostęp do sieci. Urządzenia VoIP mogą korzystać z LLDP-MED do przeprowadzania automatycznej konfiguracji w celu uproszczenia tego procesu.

## 1.2 Obsługiwane funkcje

Przełącznik obsługuje protokoły LLDP i LLDP-MED.

Protokół LLDP umożliwia urządzeniom lokalnym kapsułkowanie swoich adresów zarządzania, ID i innych informacji do jednostki danych LLDP (LLDPDU) i okresowe rozgłaszanie tej LLDPDU urządzeniom sąsiadującym. Urządzenia te przechowują otrzymane LLDPDU w standardowych bazach danych MIB (Management Information Base), co umożliwia dostęp do tych informacji poprzez NMS (Network Management System) za pomocą protokołu zarządzania, takiego jak SNMP (Simple Network Management Protocol).

LLDP-MED umożliwia urządzeniom sieciowym przesyłanie swoich informacji, w tym m. in. o Auto VoIP, czy też o pojemności PoE (Power over Ethernet), do urządzeń końcowych (np. telefonów IP) w celu automatycznej konfiguracji. Urządzenia końcowe odbierają informacje o Auto VoIP, kończą proces automatycznej konfiguracji i przesyłają ruch głosowy z żądaną konfiguracją, co może zapewnić preferencyjne traktowanie tego ruchu głosowego.

# 2 Konfiguracja LLDP

Aby skonfigurować funkcję LLDP, wykonaj poniższe kroki:

- 1) Skonfiguruj funkcję LLDP globalnie.
- 2) Skonfiguruj funkcję LLDP dla portu.

## 2.1 Przez GUI

### 2.1.1 Globalna konfiguracja LLDP

Wybierz z menu **L2 FEATURES > LLDP > LLDP Config > Global Config**, aby wyświetlić poniższą stronę.

Rys. 2-1 Konfiguracja globalna

| Global Config            |                                 |                   |
|--------------------------|---------------------------------|-------------------|
| LLDP:                    | <input type="checkbox"/>        | Enable            |
| LLDP Forwarding:         | <input type="checkbox"/>        | Enable            |
| <a href="#">Apply</a>    |                                 |                   |
| Parameter Config         |                                 |                   |
| Transmit Interval:       | <input type="text" value="30"/> | seconds (5-32768) |
| Hold Multiplier:         | <input type="text" value="4"/>  | (2-10)            |
| Transmit Delay:          | <input type="text" value="2"/>  | seconds (1-8192)  |
| Reinitialization Delay:  | <input type="text" value="2"/>  | seconds (1-10)    |
| Notification Interval:   | <input type="text" value="5"/>  | seconds (5-3600)  |
| Fast Start Repeat Count: | <input type="text" value="3"/>  | (1-10)            |
| <a href="#">Apply</a>    |                                 |                   |

Wykonaj poniższe kroki, aby skonfigurować globalnie funkcję LLDP.

- 1) W sekcji **Global Config** włącz LLDP. Możesz także włączyć przekierowywanie komunikatów LLDP przez przełącznik, gdy funkcja LLDP jest wyłączona. Kliknij **Apply**.

|                 |                                                                                                           |
|-----------------|-----------------------------------------------------------------------------------------------------------|
| LLDP            | Włącz globalnie funkcję LLDP.                                                                             |
| LLDP Forwarding | (Opcjonalnie) Włącz przekierowywanie komunikatów LLDP przez przełącznik, gdy funkcja LLDP jest wyłączona. |

- 2) W sekcji **Parameter Config** skonfiguruj parametry LLDP. Kliknij **Apply**.

|                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|-------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Transmit Interval       | Podaj interwał kolejnych pakietów LLDP, które są cyklicznie wysyłane z urządzenia lokalnego do urządzeń sąsiadujących. Wartością domyślną jest 30 sekund.                                                                                                                                                                                                                                                                                                   |
| Hold Multiplier         | Ten parametr jest mnożnikiem interwału transmisji, który określa rzeczywistą wartość TTL (Time To Live) użytą w pakiecie LLDP. TTL to czas, przez który urządzenie sąsiadujące powinno przechowywać odebrany pakiet LLDP przed jego odrzuceniem. Wartością domyślną jest 4.<br><br>TTL= Hold Multiplier * Transmit Interval.                                                                                                                                |
| Transmit Delay          | Określ czas opóźnienia, po którym stan portów zmieni się na „Disable”, aż do momentu ponownej próby inicjalizacji. Wartością domyślną są 2 sekundy.                                                                                                                                                                                                                                                                                                         |
| Reinitialization Delay  | Określ czas opóźnienia, po którym stan portów zmieni się na „Disable”, aż do momentu ponownej próby inicjalizacji. Wartością domyślną są 2 sekundy.                                                                                                                                                                                                                                                                                                         |
| Notification Interval   | Podaj interwał w sekundach pomiędzy kolejnymi komunikatami Trap, które są cyklicznie wysyłane z urządzenia lokalnego do NMS. Wartością domyślną jest 5.                                                                                                                                                                                                                                                                                                     |
| Fast Start Repeat Count | Określ liczbę pakietów LLDP, którą port lokalny ma wysłać po jego zmianie stanu administracyjnego z Disable (lub Rx_Only) na Tx&RX (lub Tx_Only). Wartością domyślną jest 3.<br><br>W tym przypadku urządzenie lokalne skróci Transmit Interval pakietów LLDP do 1 sekundy, aby mogły być szybko wykrywane przez urządzenia sąsiadujące. Po wysłaniu określonej liczby pakietów LLDP, Transmit Interval zostanie przywrócony do podanej wcześniej wartości. |

## 2.1.2 Konfiguracja LLDP dla portów

Wybierz z menu **L2 FEATURES > LLDP > LLDP Config > Port Config**, aby wyświetlić poniższą stronę.

Rys. 2-2 Konfiguracja portów

Port Config

| UNIT1                               |        |              |                   |                    |                                     |                                     |                                     |                                     |                                     |                                     |                                     |                                     |                                     |                                     |                                     |                                     |        |       |
|-------------------------------------|--------|--------------|-------------------|--------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|--------|-------|
| <input type="checkbox"/>            | Port   | Admin Status | Notification Mode | Management Address | Included TLVs                       |                                     |                                     |                                     |                                     |                                     |                                     |                                     |                                     |                                     |                                     |                                     |        |       |
| <input checked="" type="checkbox"/> | 1/0/1  | Tx & Rx      | Disabled          |                    | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |        |       |
| <input type="checkbox"/>            | 1/0/2  | Tx & Rx      | Disabled          |                    | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            |        |       |
| <input type="checkbox"/>            | 1/0/3  | Tx & Rx      | Disabled          |                    | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            |        |       |
| <input type="checkbox"/>            | 1/0/4  | Tx & Rx      | Disabled          |                    | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            |        |       |
| <input type="checkbox"/>            | 1/0/5  | Tx & Rx      | Disabled          |                    | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            |        |       |
| <input type="checkbox"/>            | 1/0/6  | Tx & Rx      | Disabled          |                    | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            |        |       |
| <input type="checkbox"/>            | 1/0/7  | Tx & Rx      | Disabled          |                    | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            |        |       |
| <input type="checkbox"/>            | 1/0/8  | Tx & Rx      | Disabled          |                    | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            |        |       |
| <input type="checkbox"/>            | 1/0/9  | Tx & Rx      | Disabled          |                    | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            |        |       |
| <input type="checkbox"/>            | 1/0/10 | Tx & Rx      | Disabled          |                    | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            |        |       |
| Total: 10                           |        |              |                   |                    | 1 entry selected.                   |                                     |                                     |                                     |                                     |                                     |                                     |                                     |                                     |                                     |                                     |                                     | Cancel | Apply |

Wykonaj poniższe kroki, aby skonfigurować funkcję LLDP dla interfejsu.

- 1) Wybierz jeden lub kilka portów do konfiguracji.
- 2) Skonfiguruj Admin Status i Notification Mode dla portu.

**Admin Status** Ustaw stan dla portu, aby określić jego działania względem pakietów LLDP.

Tx&Rx: Port wysyła i odbiera pakiety LLDP.

Rx\_Only: Port tylko odbiera pakiety LLDP.

Tx\_Only: Port tylko wysyła pakiety LLDP.

Disable: Port nie wysyła i nie odbiera pakietów LLDP.

**Notification Mode** (Opcjonalnie) Zezwól przełącznikowi na przesyłanie komunikatów trap do NMS, gdy informacje o urządzeniach sąsiadujących, połączonych z tym portem, ulegają zmianie.

**Management Address** Podaj adres IP zarządzania portu, o którym urządzenie sąsiadujące ma być poinformowane. Wartość 0.0.0.0 oznacza, że port poda urządzeniu sąsiadującemu swój domyślny adres zarządzania.

- 3) Wybierz kodowania TLV (Type-length-value) zawarte w pakietach LLDP, zgodnie ze swoimi oczekiwaniami.



|               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|---------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Included TLVs | <p>Skonfiguruj kodowania TLV, zawarte w wychodzących pakietach LLDP.</p> <p>Przełącznik obsługuje następujące kodowania TLV:</p> <p>PD: Służy do rozgłaszania opisu portu zdefiniowanego przez stację LAN IEEE 802.</p> <p>SC: Służy do rozgłaszania obsługiwanych funkcji i informacji czy te funkcje są włączone.</p> <p>SD: Służy do rozgłaszania opisu systemu, zawierającego pełną nazwę i identyfikator wersji sprzętowej, system operacyjny oprogramowania i oprogramowanie sieciowe.</p> <p>SN: Służy do rozgłaszania nazwy systemowej.</p> <p>SA: Służy do rozgłaszania adresu zarządzania urządzeniem lokalnym, aby urządzenie mogło być zarządzane przez SNMP.</p> <p>PV: Służy do rozgłaszania ID VLAN-u 802.1Q portu.</p> <p>VP: Służy do rozgłaszania ID protokołu VLAN-u portu.</p> <p>VA: Służy do rozgłaszania nazwy VLAN-u, do którego przynależy port.</p> <p>LA: Służy do rozgłaszania informacji, czy łącze jest zdolne agregacji, czy łącze jest aktualnie w trakcie procesu agregacji, a także o identyfikatorze portu, gdy podlega agregacji.</p> <p>PS: Służy do rozgłaszania atrybutów portu, w tym możliwości dupleksu i przepływności wysyłającego węzła LAN IEEE 802.3, który jest podłączony do nośnika fizycznego, aktualnych ustawień dupleksu i przepływności wysyłającego węzła LAN IEEE 802.3 oraz informacji, czy te ustawienia są wynikiem autonegociacji podczas inicjacji łącza, czy ręcznej czynności zastępowania.</p> <p>FS: Służy do rozgłaszania maksymalnego rozmiaru ramki zaimplementowanego adresu MAC i fizycznej warstwy ochronnej (PHY).</p> <p>PW: Służy do rozgłaszania możliwości obsługi PoE na porcie.</p> |
|---------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

4) Kliknij **Apply**.

## 2.2 Przez CLI

### 2.2.1 Konfiguracja globalna

Włącz funkcję LLDP na przełączniku i skonfiguruj parametry LLDP.

|        |                                                                     |
|--------|---------------------------------------------------------------------|
| Krok 1 | <p><b>configure</b></p> <p>Uruchom tryb konfiguracji globalnej.</p> |
| Krok 2 | <p><b>lldp</b></p> <p>Włącz funkcję LLDP na przełączniku.</p>       |

|        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Krok 3 | <p><b>lldp forward_message</b></p> <p>(Opcjonalnie) Zezwól przełącznikowi na przesyłanie komunikatów LLDP, gdy funkcja LLDP jest wyłączona.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Krok 4 | <p><b>lldp hold-multiplier multiplier</b></p> <p>(Opcjonalnie) Podaj czas, przez który urządzenie sąsiadujące powinno przechowywać odebrany pakiet LLDP przed jego odrzuceniem. Ten parametr jest mnożnikiem interwału transmisji, który określa rzeczywistą wartość TTL (Time To Live) użytą w pakiecie LLDP.</p> <p>TTL= Hold Multiplier * Transmit Interval.</p> <p><i>multiplier</i>: Podaj hold-multiplier. Prawidłowe wartości wahają się od 2 do 10, a wartością domyślną jest 4.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Krok 5 | <p><b>lldp timer { tx-interval tx-interval   tx-delay tx-delay   reinit-delay reinit-delay   notify-interval notify-interval   fast-count fast-count }</b></p> <p>(Opcjonalnie) Skonfiguruj czasy przesyłania pakietów LLDP.</p> <p><i>tx-interval</i>: Podaj interwał kolejnych pakietów LLDP, które są cyklicznie wysyłane z urządzenia lokalnego do urządzeń sąsiadujących.</p> <p><i>tx-delay</i>: Podaj czas oczekiwania przed wysłaniem kolejnego pakietu LLDP do urządzeń sąsiadujących. Wartością domyślną są 2 sekundy.</p> <p><i>reinit-delay</i>: Podaj czas oczekiwania przed wysłaniem kolejnego pakietu LLDP do urządzeń sąsiadujących. Wartością domyślną są 2 sekundy.</p> <p><i>notify-interval</i>: Podaj interwał w sekundach pomiędzy kolejnymi komunikatami Trap, które są cyklicznie wysyłane z urządzenia lokalnego do NMS. Wartością domyślną jest 5.</p> <p><i>fast-count</i>: Podaj liczbę pakietów przesyłanych przez port lokalny, gdy jego stan administracyjny ulega zmianie. Wartością domyślną jest 3.</p> |
| Krok 6 | <p><b>show lldp</b></p> <p>Przejrzyj informacje LLDP.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Krok 7 | <p><b>end</b></p> <p>Powróć do trybu privileged EXEC.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Krok 8 | <p><b>copy running-config startup-config</b></p> <p>Zapisz ustawienia w pliku konfiguracyjnym.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |

Poniższy schemat przedstawia przykładowy sposób konfiguracji następujących parametrów: lldp timer=4, tx-interval=30 sekund, tx-delay=2 sekund, reinit-delay=3 sekund, notify-ilnterval=5 sekund, fast-count=3.

**Switch#configure**

**Switch(config)#lldp**

**Switch(config)#lldp hold-multiplier 4**

**Switch(config)#lldp timer tx-interval 30**

```

Switch(config)#lldp timer tx-delay 2
Switch(config)#lldp timer reinit-delay 3
Switch(config)#lldp timer notify-interval 5
Switch(config)#lldp timer fast-count 3
Switch(config)#show lldp
LLDP Status: Enabled
LLDP Forward Message: Disabled
Tx Interval: 30 seconds
TTL Multiplier: 4
Tx Delay: 2 seconds
Initialization Delay: 2 seconds
Trap Notification Interval: 5 seconds
Fast-packet Count: 3
LLDP-MED Fast Start Repeat Count: 4
Switch(config)#end
Switch#copy running-config startup-config

```

## 2.2.2 Konfiguracja portów

Wybierz porty i skonfiguruj ich Admin Status, Notification Mode i TLVs zawarte w pakietach LLDP.

|        |                                                                                                                                                                                                                                                                                   |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Krok 1 | <b>configure</b><br>Uruchom tryb konfiguracji globalnej.                                                                                                                                                                                                                          |
| Krok 2 | <b>interface {fastEthernet <i>port</i>   range fastEthernet <i>port-list</i>   gigabitEthernet <i>port</i>   range gigabitEthernet <i>port-list</i>   ten-gigabitEthernet <i>port</i>   range ten-gigabitEthernet <i>port-list</i> }</b><br>Uruchom tryb konfiguracji interfejsu. |
| Krok 3 | <b>lldp receive</b><br>(Opcjonalnie) Ustaw ten tryb dla portu, aby odbierać pakiety LLDP. Opcja jest domyślnie włączona.                                                                                                                                                          |
| Krok 4 | <b>lldp transmit</b><br>(Opcjonalnie) Ustaw ten tryb dla portu, aby wysyłać pakiety LLDP. Opcja jest domyślnie włączona.                                                                                                                                                          |

|        |                                                                                                                                                                                                                                                        |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Krok 5 | <b>lldp snmp-trap</b><br>(Opcjonalnie) Włącz tryb powiadomień na porcie. Włączenie opcji spowoduje, że urządzenie lokalne będzie wysyłać komunikaty trap do NMS, gdy zmienią się informacje o urządzeniu sąsiadującym. Domyślnie opcja jest wyłączona. |
| Krok 6 | <b>lldp tlv-select</b><br>(Opcjonalnie) Skonfiguruj kodowania TLV zawarte w wychodzących pakietach LLDP. Domyślnie pakiety wychodzące LLDP zawierają wszystkie kodowania TLV.                                                                          |
| Krok 7 | <b>show lldp interface { fastEthernet <i>port</i>   gigabitEthernet <i>port</i>   ten-gigabitEthernet <i>port</i> }</b><br>Przejrzyj konfigurację LLDP portu.                                                                                          |
| Krok 8 | <b>end</b><br>Powróć do trybu privileged EXEC.                                                                                                                                                                                                         |
| Krok 9 | <b>copy running-config startup-config</b><br>Zapisz ustawienia w pliku konfiguracyjnym.                                                                                                                                                                |

Poniższy schemat przedstawia przykładowy sposób konfiguracji portu 1/0/1. Port może odbierać i wysyłać pakiety LLDP, jego tryb wysyłania komunikatów ma status enabled, a wychodzące pakiety LLDP zawierają wszystkie TLVs.

```
Switch#configure
```

```
Switch(config)#lldp
```

```
Switch(config)#interface gigabitEthernet 1/0/1
```

```
Switch(config-if)#lldp receive
```

```
Switch(config-if)#lldp transmit
```

```
Switch(config-if)#lldp snmp-trap
```

```
Switch(config-if)#lldp tlv-select all
```

```
Switch(config-if)#show lldp interface gigabitEthernet 1/0/1
```

```
LLDP interface config:
```

```
gigabitEthernet 1/0/1:
```

```
Admin Status: TxRx
```

```
SNMP Trap: Enabled
```

```
TLV Status
```

```

```

```
Port-Description Yes
```

```
System-Capability Yes
```

---

|                    |     |
|--------------------|-----|
| System-Description | Yes |
| System-Name        | Yes |
| Management-Address | Yes |
| Port-VLAN-ID       | Yes |
| Protocol-VLAN-ID   | Yes |
| VLAN-Name          | Yes |
| Link-Aggregation   | Yes |
| MAC-Physic         | Yes |
| Max-Frame-Size     | Yes |
| Power              | Yes |

**Switch(config-if)#end**

**Switch#copy running-config startup-config**

# 3 Konfiguracja LLDP-MED

Aby skonfigurować funkcję LLDP-MED, wykonaj poniższe kroki:

- 1) Włącz funkcję LLDP globalnie i skonfiguruj parametry LLDP dla portów.
- 2) Skonfiguruj globalnie liczbę wysyłanych pakietów LLDP-MED.
- 3) Włącz i skonfiguruj funkcję LLDP-MED na porcie.

## Wskazówki dotyczące konfiguracji

Protokół LLDP-MED jest stosowany wraz z Auto VoIP w celu wdrożenia dostępu VoIP. Oprócz konfiguracji funkcji LLDP-MED konieczna jest także konfiguracja Auto VoIP. Szczegółowe informacje znajdziesz w części *Konfiguracja QoS*.

## 3.1 Przez GUI

### 3.1.1 Globalna konfiguracja LLDP

Włącz LLDP globalnie i skonfiguruj parametry LLDP dla portów. Szczegółowe informacje o konfiguracji LLDP znajdziesz w rozdziale *Konfiguracja LLDP*.

### 3.1.2 Globalna konfiguracja LLDP-MED

Wybierz z menu **L2 FEATURES > LLDP Config > LLDP-MED Config > Global Config**, aby wyświetlić poniższą stronę.

Rys. 3-1 Konfiguracja parametrów LLDP-MED

LLDP-MED Parameters Config

Fast Start Repeat Count:  (1-10)

Device Class: Network Connectivity

Apply

Skonfiguruj Fast Start Count i wyświetl aktualną klasę urządzenia. Kliknij **Apply**.

|                         |                                                                                                                                                                                                                                                              |
|-------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Fast Start Repeat Count | Podaj liczbę kolejnych pakietów LLDP-MED, które przełącznik wysyła, gdy odbiera pakiety LLDP-MED z sąsiadujących urządzeń końcowych. Wartością domyślną jest 4.                                                                                              |
|                         | Gdy przełącznik po raz pierwszy otrzyma pakiety LLDP-MED od sąsiadujących urządzeń końcowych, prześle określoną liczbę pakietów LLDP-MED z informacjami o LLDP-MED. Po tym wydarzeniu, transmit interval zostanie przywrócony do podanej wcześniej wartości. |

|              |                                                                                                                                      |
|--------------|--------------------------------------------------------------------------------------------------------------------------------------|
| Device Class | Aktualna klasa urządzenia.                                                                                                           |
|              | LLDP-MED definiuje dwie klasy urządzeń: Network Connectivity Device i Endpoint Device. Przełącznik jest Network Connectivity device. |

### 3.1.3 Konfiguracja LLDP-MED dla portów

Wybierz z menu **L2 FEATURES > LLDP > LLDP-MED Config > Port Config**, aby wyświetlić poniższą stronę.

Rys. 3-2 Konfiguracja portów LLDP-MED

| Port Config                         |        |                 |                        |
|-------------------------------------|--------|-----------------|------------------------|
| UNIT1                               |        |                 |                        |
| <input type="checkbox"/>            | Port   | LLDP-MED Status | Included TLVs          |
| <input checked="" type="checkbox"/> | 1/0/1  | Disabled        | <a href="#">Detail</a> |
| <input type="checkbox"/>            | 1/0/2  | Disabled        | <a href="#">Detail</a> |
| <input type="checkbox"/>            | 1/0/3  | Disabled        | <a href="#">Detail</a> |
| <input type="checkbox"/>            | 1/0/4  | Disabled        | <a href="#">Detail</a> |
| <input type="checkbox"/>            | 1/0/5  | Disabled        | <a href="#">Detail</a> |
| <input type="checkbox"/>            | 1/0/6  | Disabled        | <a href="#">Detail</a> |
| <input type="checkbox"/>            | 1/0/7  | Disabled        | <a href="#">Detail</a> |
| <input type="checkbox"/>            | 1/0/8  | Disabled        | <a href="#">Detail</a> |
| <input type="checkbox"/>            | 1/0/9  | Disabled        | <a href="#">Detail</a> |
| <input type="checkbox"/>            | 1/0/10 | Disabled        | <a href="#">Detail</a> |

Total: 10      1 entry selected.      [Cancel](#) [Apply](#)

Wykonaj poniższe kroki, aby włączyć LLDP-MED:

- 1) Wybierz porty i włącz dla nich LLDP-MED. Kliknij **Apply**.
- 2) Kliknij **Detail**, aby wyświetlić poniższą stronę. Skonfiguruj kodowania TLV zawarte w wychodzących pakietach LLDP. Jeżeli zaznaczysz **Location Identification**, musisz ustawić Emergency Number lub wybrać Civic Address, aby skonfigurować szczegółowe informacje. Kliknij **Apply**.

Rys. 3-3 Konfiguracja portów LLDP-MED - informacje szczegółowe

**Included TLVs Detail(Port:1/0/1)**

---

**Included TLVs**

All

Network Policy     Location Identification     Extended Power-Via-MDI     Inventory

---

**Location Identification Parameters**

Emergency Number     Civic Address (Parameters in total should not exceed 230 characters in length)

What:

Country Code:

Language:

Province/State:

City/Township:

County/Parish/District:

Street:

House Number:

Name:

Postal/Zip Code:

Room Number:

|                                |                                                                                                                                                                                                                                                                                 |
|--------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Network Policy</b>          | Służy do rozgłaszania konfiguracji VLAN-u i powiązanych atrybutów warstwy 2 i warstwy 3 portu do urządzeń końcowych.                                                                                                                                                            |
| <b>Location Identification</b> | <p>Służy do przypisywania urządzeniom końcowym informacji o identyfikatorze lokalizacji.</p> <p>Jeżeli opcja jest zaznaczona, możesz skonfigurować numer alarmowy i szczegółowe informacje o urządzeniu końcowym w części Location Identification Parameters.</p>               |
| <b>Extended Power-Via-MDI</b>  | Służy do rozgłaszania szczegółowych informacji o PoE, w tym o priorytetyzacji dostarczanej energii i o stanie zasilania pomiędzy urządzeniami końcowymi LLDP-MED a urządzeniami Network Connectivity.                                                                           |
| <b>Inventory</b>               | Służy do rozgłaszania informacji o inwentarzu. Zestaw TLV zawiera siedem podstawowych kodowań TLV inwentarzu zarządzania, tj. wersję sprzętową TLV, wersję firmware'u TLV, wersję oprogramowania TLV, numer seryjny TLV, nazwę producenta TLV, nazwę modelu TLV i Asset ID TLV. |
| <b>Emergency Number</b>        | Skonfiguruj numer awaryjny, aby móc zadzwonić do CAMA lub PSAP. Numer powinien składać się z 10-25 znaków.                                                                                                                                                                      |



|                      |                                                                                                       |
|----------------------|-------------------------------------------------------------------------------------------------------|
| <b>Civic Address</b> | Skonfiguruj adres urządzenia audio w formacie adresu zdefiniowanym przez IETF.                        |
|                      | What: Określ rolę urządzenia lokalnego, serwera DHCP, przełącznika lub urządzenia końcowego LLDP-MED. |
|                      | Country Code: Podaj kod kraju zgodny z ISO 3166, np. CN, US.                                          |
|                      | Language, Province/State etc.: Uzupełnij pozostałe informacje.                                        |

## 3.2 Przez CLI

### 3.2.1 Konfiguracja globalna

|        |                                                                                                                                                                                                                                                                                                                                                   |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Krok 1 | <b>configure</b><br>Uruchom tryb konfiguracji globalnej.                                                                                                                                                                                                                                                                                          |
| Krok 2 | <b>lldp</b><br>Włącz funkcję LLDP na przełączniku.                                                                                                                                                                                                                                                                                                |
| Krok 3 | <b>lldp med-fast-count count</b><br>(Opcjonalnie) Podaj liczbę kolejnych ramek LLDP-MED, które urządzenie lokalne wysyła, gdy mechanizm fast start jest aktywowany. Urządzenie lokalne wysyła określoną liczbę pakietów LLDP z informacjami LLDP-MED.<br><br><i>count</i> : Prawidłowe wartości wahają się od 1 do 10. Wartością domyślną jest 4. |
| Krok 4 | <b>show lldp</b><br>Przejrzyj informacje o LLDP.                                                                                                                                                                                                                                                                                                  |
| Krok 5 | <b>end</b><br>Powróć do trybu privileged EXEC.                                                                                                                                                                                                                                                                                                    |
| Krok 6 | <b>copy running-config startup-config</b><br>Zapisz ustawienia w pliku konfiguracyjnym.                                                                                                                                                                                                                                                           |

Poniższy schemat przedstawia przykładowy sposób ustawiania LLDP-MED fast count jako 4:

```
Switch#configure
```

```
Switch(config)#lldp
```

```
Switch(config)#lldp med-fast-count 4
```

```
Switch(config)#show lldp
```

```
LLDP Status: Enabled
```

```
Tx Interval: 30 seconds
```

|                                   |           |
|-----------------------------------|-----------|
| TTL Multiplier:                   | 4         |
| Tx Delay:                         | 2 seconds |
| Initialization Delay:             | 2 seconds |
| Trap Notification Interval:       | 5 seconds |
| Fast-packet Count:                | 3         |
| LLDP-MED Fast Start Repeat Count: | 4         |

**Switch(config)#end**

**Switch#copy running-config startup-config**

### 3.2.2 Konfiguracja portów

Zaznacz porty, włącz LLDP-MED i wybierz kodowania TLV (Type-length-value) zawarte w wychodzących pakietach LLDP, zgodnie ze swoimi oczekiwaniami.

|        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Krok 1 | <b>configure</b><br>Uruchom tryb konfiguracji globalnej.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Krok 2 | <b>interface {fastEthernet <i>port</i>   range fastEthernet <i>port-list</i>   gigabitEthernet <i>port</i>   range gigabitEthernet <i>port-list</i>   ten-gigabitEthernet <i>port</i>   range ten-gigabitEthernet <i>port-list</i> }</b><br>Uruchom tryb konfiguracji interfejsu.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Krok 3 | <b>lldp med-status</b><br>(Opcjonalnie) Włącz LLDP-MED na porcie. Domyślnie funkcja jest wyłączona.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Krok 4 | <b>lldp med-tlv-select { [ inventory-management ] [ location ] [ network-policy ] [ power-management ] [ all ] }</b><br>(Opcjonalnie) Skonfiguruj kodowania TLV, zawarte w wychodzących pakietach LLDP. Domyślnie wychodzące pakiety LLDP zawierają wszystkie kodowania TLV.<br><br>Jeżeli zaznaczysz LLDP-MED Location TLV, skonfiguruj poniższe parametry:<br><b>lldp med-location { emergency-number <i>identifier</i>   civic-address [ language <i>language</i>   province-state <i>province-state</i>   lci-county-name <i>county</i>   lci-city <i>city</i>   street <i>street</i>   house-number <i>house-number</i>   name <i>name</i>   postal-zipcode <i>postal-zipcode</i>   room-number <i>room-number</i>   post-office-box <i>post-office-box</i>   additional <i>additional</i>   country-code <i>country-code</i>   what { dhcp-server   endpoint   switch } ] }</b><br><br>Skonfiguruj lokalizację kodowania TLV LLDP-MED zawartą w pakietach wychodzących LLDP. Służy ona do przypisywania informacji o identyfikatorze lokalizacji do urządzeń końcowych.<br><br><i>identifier</i> : Skonfiguruj numer awaryjny, aby móc zadzwonić do CAMA lub PSAP. Numer powinien składać się z 10-25 znaków.<br><br><i>language, province-state, county.etc.</i> : Skonfiguruj adres w formacie adresu zdefiniowanym przez IETF. |

|        |                                                                                                                                                               |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Krok 5 | <b>show lldp interface { fastEthernet <i>port</i>   gigabitEthernet <i>port</i>   ten-gigabitEthernet <i>port</i> }</b><br>Przejrzyj konfigurację LLDP portu. |
| Krok 6 | <b>end</b><br>Powróć do trybu uprzywilejowanego (privileged EXEC mode).                                                                                       |
| Krok 7 | <b>copy running-config startup-config</b><br>Zapisz ustawienia w pliku konfiguracyjnym.                                                                       |

Poniższy schemat przedstawia przykładowy sposób włączania LLDP-MED na porcie 1/0/1 i konfiguracji kodowań TLV LLDP-MED zawartych w wychodzących pakietach LLDP.

**Switch(config)#lldp**

**Switch(config)#lldp med-fast-count 4**

**Switch(config)#interface gigabitEthernet 1/0/1**

**Switch(config-if)#lldp med-status**

**Switch(config-if)#lldp med-tlv-select all**

**Switch(config-if)#show lldp interface gigabitEthernet 1/0/1**

LLDP interface config:

gigabitEthernet 1/0/1:

Admin Status: TxRx

SNMP Trap: Enabled

TLV Status

--- -----

Port-Description                    Yes

System-Capability                 Yes

System-Description                Yes

System-Name                        Yes

Management-Address Yes

Port-VLAN-ID Yes

Protocol-VLAN-ID Yes

VLAN-Name Yes

Link-Aggregation Yes

MAC-Physic Yes

```
Max-Frame-Size Yes
Power Yes
LLDP-MED Status: Enabled
```

```
TLV Status
```

```
--- -----
```

```
Network Policy Yes
Location Identification Yes
Extended Power Via MDI Yes
Inventory Management Yes
```

```
Switch(config)#end
```

```
Switch#copy running-config startup-config
```

# 4 Przeglądanie ustawień LLDP

Ten rozdział przedstawia możliwe sposoby przeglądania ustawień LLDP na urządzeniu lokalnym.

## 4.1 Przez GUI

### 4.1.1 Przeglądanie informacji urządzenia o LLDP

- Przeglądanie informacji lokalnych

Wybierz z menu **L2 FEATURES > LLDP > LLDP Config > Local Info**, aby wyświetlić poniższą stronę.


Rys. 4-1 Informacje lokalne


Auto Refresh


Auto Refresh:  Enable Apply


Local Info

UNIT1



 Selected

 Unselected

 Not Available

| Port 1/0/8                     |                                                             |
|--------------------------------|-------------------------------------------------------------|
| Local Interface:               | 1/0/8                                                       |
| Chassic ID Subtype:            | MAC address                                                 |
| Chassic ID:                    | 00-0D-EB-13-A2-98                                           |
| Port ID Subtype:               | Interface name                                              |
| Port ID:                       | GigabitEthernet1/0/8                                        |
| TTL:                           | 120                                                         |
| Port Description:              | GigabitEthernet1/0/8 Interface                              |
| System Name:                   | T2500G-10TS                                                 |
| System Description:            | JetStream 8-Port Gigabit L2 Managed Switch with 2 SFP Slots |
| System Capabilities Supported: | Bridge                                                      |
| System Capabilities Enabled:   | Bridge                                                      |
| Management Address Type:       | IPv4                                                        |
| Management Address:            | 192.168.0.25                                                |

Wykonaj poniższe kroki, aby uzyskać dostęp do informacji lokalnych:

- 1) W sekcji **Auto Refresh** włącz funkcję automatycznego odświeżania i ustaw częstotliwość odświeżania (Refresh Rate), zgodnie z oczekiwaniami. Kliknij **Apply**.
- 2) W sekcji **Local Info** wybierz port i wyświetl informacje o powiązonym z nim urządzeniu lokalnym.

|                                   |                                                                                                                            |
|-----------------------------------|----------------------------------------------------------------------------------------------------------------------------|
| Local Interface                   | ID portu lokalnego.                                                                                                        |
| Chassis ID Subtype                | Typ ID obudowy.                                                                                                            |
| Chassis ID                        | Wartość ID obudowy.                                                                                                        |
| Port ID Subtype                   | Typ ID portu.                                                                                                              |
| Port ID                           | Wartość ID portu.                                                                                                          |
| TTL                               | Podaj czas w sekundach, przez który urządzenie sąsiadujące powinno przechowywać odebraną informację przed jej odrzuceniem. |
| Port Description                  | Opis portu lokalnego.                                                                                                      |
| System Name                       | Nazwa systemowa urządzenia lokalnego.                                                                                      |
| System Description                | Opis systemowy urządzenia lokalnego.                                                                                       |
| System Capabilities Supported     | Obsługiwane możliwości systemu lokalnego.                                                                                  |
| System Capabilities Enabled       | Podstawowe funkcje urządzenia lokalnego.                                                                                   |
| Management Address Type           | Typ adresu IP zarządzania urządzenia lokalnego.                                                                            |
| Management Address                | Adres IP zarządzania urządzenia lokalnego.                                                                                 |
| Management Address Interface Type | Typ numerowania interfejsu, który jest stosowany do ustalania ID interfejsu.                                               |
| Management Address Interface ID   | ID interfejsu, który służy identyfikowaniu określonego interfejsu, powiązanego z adresem MAC urządzenia lokalnego.         |
| Management Address OID            | OID (Object Identifier) urządzenia lokalnego. Wartość równa 0 oznacza, że nie ma OID.                                      |
| Port VLAN ID(PVID)                | PVID portu lokalnego.                                                                                                      |
| Port And Protocol VLAN ID(PPVID)  | PPVID portu lokalnego.                                                                                                     |

---

|                                |                                                                              |
|--------------------------------|------------------------------------------------------------------------------|
| Port And Protocol Supported    | Informacja, czy urządzenie lokalne obsługuje funkcję portu i protokołu VLAN. |
| Port And Protocol VLAN Enabled | Stan funkcji portu i protokołu VLAN.                                         |
| VLAN Name of VLAN 1            | Nazwa VLAN 1 dla urządzenia lokalnego.                                       |
| Protocol Identify              | Protokół zalecany przez urządzenie lokalne.                                  |
| Auto-negotiation Supported     | Informacja, czy urządzenie lokalne obsługuje auto negocjację.                |
| Auto-Negotiation Enable        | Stan auto negocjacji urządzenia lokalnego.                                   |
| OperMau                        | Pole OperMau (opcjonalne Mau) TLV, skonfigurowane przez urządzenie lokalne.  |
| Link Aggregation Supported     | Informacja, czy urządzenie lokalne obsługuje agregację łączy.                |
| Link Aggregation Enabled       | Stan agregacji łączy urządzenia lokalnego.                                   |
| Aggregation Port ID            | ID portu agregacji urządzenia lokalnego.                                     |
| Power Port Class               | Klasa portu zasilającego urządzenia lokalnego.                               |
| PSE Power Supported            | Informacja, czy urządzenie lokalne obsługuje zasilanie PSE.                  |
| PSE Power Enabled              | Stan zasilania PSE urządzenia lokalnego.                                     |
| PSE Pairs Control Ability      | Informacja, czy można kontrolować pary PSE dla urządzenia lokalnego.         |
| Maximum Frame Size             | Maksymalny rozmiar ramki obsługiwany przez urządzenie lokalne.               |

---

- Przeglądanie informacji o urządzeniach sąsiadujących

Wybierz z menu **L2 FEATURES > LLDP > LLDP Config > Neighbor Info**, aby wyświetlić poniższą stronę.

Rys. 4-2 Informacje o urządzeniach sąsiadujących

Auto Refresh

Auto Refresh:  Enable Apply

---

Neighbor Info

UNIT1

| Port 1/0/1                |            |                    |               |             |
|---------------------------|------------|--------------------|---------------|-------------|
| System Name               | Chassic ID | System Description | Neighbor Port | Information |
| No entries in this table. |            |                    |               |             |

Wykonaj poniższe kroki, aby wyświetlić informacje o urządzeniach sąsiadujących:

- W sekcji **Auto Refresh** włącz funkcję automatycznego odświeżania i ustaw częstotliwość odświeżania (Refresh Rate), zgodnie oczekiwaniami. Kliknij **Apply**.
- W sekcji **Nieghbor Info** wybierz port i wyświetl informacje o powiązonym z nim urządzeniu sąsiadującym.

|                    |                                                                              |
|--------------------|------------------------------------------------------------------------------|
| System Name        | Nazwa systemowa urządzenia sąsiadującego.                                    |
| Chassis ID         | ID obudowy urządzenia sąsiadującego.                                         |
| System Description | Opis systemowy urządzenia sąsiadującego.                                     |
| Neighbor Port      | ID portu urządzenia sąsiadującego, które jest podłączone do portu lokalnego. |
| Information        | Kliknij, aby wyświetlić informacje szczegółowe o urządzeniu sąsiadującym.    |



## 4.1.2 Przeglądanie statystyk LLDP

Wybierz z menu **L2 FEATURES > LLDP > LLDP Config > Statistics Info**, aby wyświetlić poniższą stronę.

Rys. 4-3 Statystyki

**Auto Refresh**

Auto Refresh:  Enable Apply

---

**Global Statistics**

| Last Update        | Total Inserts | Total Deletes | Total Drops | Total Age-outs |
|--------------------|---------------|---------------|-------------|----------------|
| 2 days 18h:25m:00s | 1             | 0             | 0           | 0              |

---

**Neighbor Statistics**

UNIT1
Refresh ↻ Clear 🗑️

| Port      | Transmit Total | Receive Total | Discards | Errors | Age-outs | Discarded TLVs | Unknown TLVs |
|-----------|----------------|---------------|----------|--------|----------|----------------|--------------|
| 1/0/1     | 0              | 0             | 0        | 0      | 0        | 0              | 0            |
| 1/0/2     | 0              | 0             | 0        | 0      | 0        | 0              | 0            |
| 1/0/3     | 0              | 0             | 0        | 0      | 0        | 0              | 0            |
| 1/0/4     | 0              | 0             | 0        | 0      | 0        | 0              | 0            |
| 1/0/5     | 0              | 0             | 0        | 0      | 0        | 0              | 0            |
| 1/0/6     | 0              | 0             | 0        | 0      | 0        | 0              | 0            |
| 1/0/7     | 0              | 0             | 0        | 0      | 0        | 0              | 0            |
| 1/0/8     | 0              | 0             | 0        | 0      | 0        | 0              | 0            |
| 1/0/9     | 0              | 0             | 0        | 0      | 0        | 0              | 0            |
| 1/0/10    | 3948           | 3939          | 0        | 0      | 0        | 0              | 0            |
| Total: 10 |                |               |          |        |          |                |              |

Wykonaj poniższe kroki, aby wyświetlić statystyki LLDP:

- 1) W sekcji **Auto Refresh** włącz funkcję automatycznego odświeżania i ustaw częstotliwość odświeżania (Refresh Rate) zgodnie oczekiwaniami. Kliknij **Apply**.
- 2) W sekcji **Global Statistics** wyświetl globalne statystyki urządzenia lokalnego.

|                      |                                                                                                                                                                                                            |
|----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Last Update</b>   | Czas ostatniej aktualizacji statystyk.                                                                                                                                                                     |
| <b>Total Inserts</b> | Całkowita liczba urządzeń sąsiadujących po ostatniej aktualizacji.                                                                                                                                         |
| <b>Total Deletes</b> | Liczba urządzeń sąsiadujących, usuniętych przez urządzenie lokalne. Port usuwa urządzenie sąsiadujące, gdy jest wyłączony lub wartość TTL pakietów LLDP przesyłanych do urządzenia sąsiadującego wynosi 0. |
| <b>Total Drops</b>   | Liczba urządzeń sąsiadujących, odrzuconych przez urządzenie lokalne. Każdy z portów może nauczyć się maksymalnie 80 urządzeń sąsiadujących. Każde kolejne urządzenie będzie odrzucane.                     |

---

|                |                                                                               |
|----------------|-------------------------------------------------------------------------------|
| Total Age-outs | Liczba urządzeń sąsiadujących, które straciły ważność na urządzeniu lokalnym. |
|----------------|-------------------------------------------------------------------------------|

---

3) W sekcji **Neighbors Statistics** możesz wyświetlić statystyki portu.

---

|                |                                                       |
|----------------|-------------------------------------------------------|
| Transmit Total | Całkowita liczba pakietów LLDP przesłanych na porcie. |
|----------------|-------------------------------------------------------|

---

|               |                                                      |
|---------------|------------------------------------------------------|
| Receive Total | Całkowita liczba pakietów LLDP odebranych na porcie. |
|---------------|------------------------------------------------------|

---

|          |                                                        |
|----------|--------------------------------------------------------|
| Discards | Całkowita liczba pakietów LLDP odrzuconych przez port. |
|----------|--------------------------------------------------------|

---

|        |                                                               |
|--------|---------------------------------------------------------------|
| Errors | Całkowita liczba błędnych pakietów LLDP odebranych na porcie. |
|--------|---------------------------------------------------------------|

---

|          |                                                                              |
|----------|------------------------------------------------------------------------------|
| Age-outs | Liczba podłączonych do portu urządzeń sąsiadujących, które utraciły ważność. |
|----------|------------------------------------------------------------------------------|

---

|              |                                                                                  |
|--------------|----------------------------------------------------------------------------------|
| TLV Discards | Całkowita liczba kodowań TLV odrzuconych przez port po otrzymaniu pakietów LLDP. |
|--------------|----------------------------------------------------------------------------------|

---

|              |                                                                                  |
|--------------|----------------------------------------------------------------------------------|
| TLV Unknowns | Całkowita liczba nieznanymi kodowań TLV, zawartych w otrzymanych pakietach LLDP. |
|--------------|----------------------------------------------------------------------------------|

---

## 4.2 Przez CLI

- Przeglądanie informacji lokalnych

---

```
show lldp local-information interface { fastEthernet port | gigabitEthernet port | ten-gigabitEthernet port }
```

Wyświetla szczegółowe informacje LLDP o określonym porcie lub o wszystkich portach na urządzeniu lokalnym.

---

- Przeglądanie informacji o urządzeniach sąsiadujących

---

```
show lldp neighbor-information interface { fastEthernet port | gigabitEthernet port | ten-gigabitEthernet port }
```

Wyświetla informacje o urządzeniu sąsiadującym, które jest podłączone do portu.

---

- Przeglądanie statystyk LLDP

---

```
show lldp traffic interface { fastEthernet port | gigabitEthernet port | ten-gigabitEthernet port }
```

Wyświetla statystyki wybranego portu na urządzeniu lokalnym.

---

# 5 Przeglądanie ustawień LLDP-MED

## 5.1 Przez GUI

Wybierz z menu **L2 FEATURES > LLDP > LLDP-MED Config > Local Info**, aby wyświetlić poniższą stronę.

- Przeglądanie informacji lokalnych

Rys. 5-1 Informacje lokalne o LLDP-MED

Auto Refresh

Auto Refresh:  Enable

Apply

Local Info

UNIT1

1

2

3

4

5

6

7

8

9

10

Selected

Unselected

Not Available

| Port 1/0/8                     |                      |
|--------------------------------|----------------------|
| Local Interface:               | 1/0/8                |
| Device Type:                   | Network Connectivity |
| Application Type:              | Reserved             |
| Unknown Policy Flag:           | Yes                  |
| VLAN tagged:                   | 0                    |
| Media Policy VLAN ID:          | 0                    |
| Media Policy Layer 2 Priority: | 0                    |
| Media Policy DSCP:             | 0                    |
| Location Data Format:          | Civic Address LCI    |
| What:                          | Switch               |
| Country Code:                  | CN China(Default)    |
| Hardware Revision:             | T2500G-10TS 2.0      |

Wykonaj poniższe kroki, aby wyświetlić informacje lokalne o LLDP-MED:

- 1) W sekcji **Auto Refresh** włącz funkcję automatycznego odświeżania i ustaw częstotliwość odświeżania (Refresh Rate), zgodnie oczekiwaniami. Kliknij **Apply**.
- 2) W sekcji **LLDP-MED Local Info** wybierz porty i wyświetl ustawienia LLDP-MED.

---

Local Interface      ID portu lokalnego.

---

|                               |                                                                                                                                                                                               |
|-------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Device Type                   | Typ urządzenia lokalnego, definiowanego przez LLDP-MED.LLDP-MED.                                                                                                                              |
| Application Type              | Obsługiwane zastosowania urządzenia lokalnego.                                                                                                                                                |
| Unknown Policy Flag           | Ustawienia nieznannej lokalizacji zawartej w polityce sieciowej TLV.                                                                                                                          |
| VLAN tagged                   | Typ tagu VLAN aplikacji, tagowany lub nietagowany.                                                                                                                                            |
| Media Policy VLAN ID          | ID 802.1Q VLAN portu.                                                                                                                                                                         |
| Media Policy Layer 2 Priority | Priorytet warstwy 2, stosowany dla określonego zastosowania.                                                                                                                                  |
| Media Policy DSCP             | Wartość DSCP, stosowana dla określonego zastosowania.                                                                                                                                         |
| Location Data Format          | Format danych identyfikatora lokalizacji urządzenia lokalnego.                                                                                                                                |
| What                          | Typ urządzenia lokalnego.                                                                                                                                                                     |
| Country Code                  | Kod kraju urządzenia lokalnego.                                                                                                                                                               |
| Power Type                    | Informacja, czy urządzenie lokalne jest urządzeniem PSE czy PD.                                                                                                                               |
| Power Source                  | Źródło zasilania urządzenia lokalnego.                                                                                                                                                        |
| Power Priority                | Priorytet zasilania urządzenia lokalnego to priorytet energii elektrycznej, która dostarczana jest przez urządzenia PD lub priorytet energii elektrycznej, dostarczanej przez urządzenia PSE. |
| Power Value                   | Moc wymagana od urządzenia PD lub dostarczana przez urządzenie PSE.                                                                                                                           |
| Hardware Revision             | Wersja sprzętowa urządzenia lokalnego.                                                                                                                                                        |
| Firmware Revision             | Wersja firmware'u urządzenia lokalnego.                                                                                                                                                       |
| Software Revision             | Wersja oprogramowania urządzenia lokalnego.                                                                                                                                                   |
| Serial Number                 | Numer seryjny urządzenia lokalnego.                                                                                                                                                           |
| Manufacturer Name             | Nazwa producenta urządzenia lokalnego.                                                                                                                                                        |
| Model Name                    | Model urządzenia lokalnego.                                                                                                                                                                   |
| Asset ID                      | Asset ID urządzenia lokalnego.                                                                                                                                                                |

- Przeglądanie informacji o urządzeniach sąsiadujących

Wybierz z menu **L2 FEATURES > LLDP > LLDP-MED Config > Neighbor Info**, aby wyświetlić poniższą stronę.

Rys. 5-2 Informacje LLDP-MED urządzeń sąsiadujących

**Auto Refresh**

Auto Refresh:  Enable

[Apply](#)

**Neighbor Info**

UNIT1

1

2

3

4

5

6

7

8

9

10

Selected

Unselected

Not Available

| Port 1/0/1                |                  |                      |            |             |
|---------------------------|------------------|----------------------|------------|-------------|
| Device Type               | Application Type | Location Data Format | Power Type | Information |
| No entries in this table. |                  |                      |            |             |

Wykonaj poniższe kroki, aby wyświetlić informacje LLDP-MED urządzeń sąsiadujących:

- 1) W sekcji **Auto Refresh** włącz funkcję automatycznego odświeżania i ustaw częstotliwość odświeżania (Refresh Rate), zgodnie oczekiwaniami. Kliknij **Apply**.
- 2) W sekcji **Nieghbor Info** wybierz port i wyświetl informacje o powiązonym z nim urządzeniu sąsiadującym.

|                             |                                                                                   |
|-----------------------------|-----------------------------------------------------------------------------------|
| <b>Device Type</b>          | Typ LLDP-MED urządzenia sąsiadującego.                                            |
| <b>Application Type</b>     | Typ zastosowań urządzenia sąsiadującego.                                          |
| <b>Location Data Format</b> | Typ lokalizacji urządzenia sąsiadującego.                                         |
| <b>Power Type</b>           | Typ zasilania urządzenia sąsiadującego.                                           |
| <b>Information</b>          | Kliknij, aby wyświetlić szczegółowe informacje LLDP-MED urządzenia sąsiadującego. |

## 5.2 Przez CLI

- Przeglądanie informacji lokalnych

---

```
show lldp local-information interface { fastEthernet port | gigabitEthernet port | ten-gigabitEthernet port }
```

Wyświetla szczegółowe informacje LLDP określonego portu lub wszystkich portów na urządzeniu lokalnym.

---

- Przeglądanie informacji o urządzeniach sąsiadujących

---

```
show lldp neighbor-information interface { fastEthernet port | gigabitEthernet port | ten-gigabitEthernet port }
```

Wyświetla informacje o urządzenie sąsiadującym, które jest połączone z portem.

---

- Przeglądanie statystyk LLDP

---

```
show lldp traffic interface { fastEthernet port | gigabitEthernet port | tengigabitEthernet port }
```

Wyświetla statystyki wybranych portów.

---

# 6 Przykład konfiguracji

## 6.1 Wymagania sieciowe

Administrator sieci potrzebuje wglądu w informacje o urządzeniach w sieci firmowej, aby znać stan łącza i topologię sieci, co pomoże mu w zapobieganiu problemom.

## 6.2 Topologia sieci

Topologię omówimy na przykładzie następującej sytuacji:

Port Gi1/0/1 na przełączniku A jest podłączony bezpośrednio do portu Gi1/0/2 przełącznika B. Przełącznik B jest podłączony bezpośrednio do komputera. Administrator ma wgląd w informacje o urządzeniu poprzez NMS.

Rys. 6-1 Topologia sieci LLDP



## 6.3 Schemat konfiguracji

LLDP może spełniać wymagania sieci. Włącz globalnie funkcję LLDP na przełączniku A i przełączniku B. Skonfiguruj powiązane parametry LLDP na odpowiednich portach.

Konfiguracja przełącznika A i przełącznika B:

Konfiguracja przełącznika A jest taka sama jak przełącznika B. Poniższy instruktaż omówimy na przykładzie przełącznika A. W poniższych podrozdziałach opisano dwa sposoby przeprowadzenia procedury konfiguracji: przez GUI oraz przez CLI.

## 6.4 Przez GUI

- 1) Wybierz z menu **L2 FEATURES > LLDP > LLDP Config > Global Config**, aby wyświetlić poniższą stronę. Włącz globalnie LLDP i skonfiguruj powiązane parametry. W poniższym przykładzie skorzystamy z ustawień domyślnych.

Rys. 6-2 Konfiguracja globalna LLDP

Global Config

LLDP:  Enable

LLDP Forwarding:  Enable

---

Parameter Config

Transmit Interval:  seconds (5-32768)

Hold Multiplier:  (2-10)

Transmit Delay:  seconds (1-8192)

Reinitialization Delay:  seconds (1-10)

Notification Interval:  seconds (5-3600)

Fast Start Repeat Count:  (1-10)

- 2) Wybierz z menu **L2 FEATURES > LLDP > LLDP Config > Port Config**, aby wyświetlić poniższą stronę. Ustaw stan admina portu Fa1/0/1 jako Tx&Rx, włącz tryb powiadomień i skonfiguruj wszystkie TLVs zawarte w wychodzących pakietach LLDP.

Rys. 6-3 Konfiguracja portów LLDP

Port Config

UNIT1

| <input type="checkbox"/>            | Port   | Admin Status | Notification Mode | Included TLVs                       |                                     |                                     |                                     |                                     |                                     |                                     |                                     |                                     |                                     |                                     |                                     |                                     |                                     |
|-------------------------------------|--------|--------------|-------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|
| <input checked="" type="checkbox"/> | 1/0/1  | Tx & Rx      | Enabled           | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| <input type="checkbox"/>            | 1/0/2  | Tx & Rx      | Disabled          | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            |
| <input type="checkbox"/>            | 1/0/3  | Tx & Rx      | Disabled          | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            |
| <input type="checkbox"/>            | 1/0/4  | Tx & Rx      | Disabled          | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            |
| <input type="checkbox"/>            | 1/0/5  | Tx & Rx      | Disabled          | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            |
| <input type="checkbox"/>            | 1/0/6  | Tx & Rx      | Disabled          | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            |
| <input type="checkbox"/>            | 1/0/7  | Tx & Rx      | Disabled          | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            |
| <input type="checkbox"/>            | 1/0/8  | Tx & Rx      | Disabled          | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            |
| <input type="checkbox"/>            | 1/0/9  | Tx & Rx      | Disabled          | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            |
| <input type="checkbox"/>            | 1/0/10 | Tx & Rx      | Disabled          | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            |

Total: 10 1 entry selected.

## 6.5 Przez CLI

- 1) Włącz globalnie LLDP i skonfiguruj odpowiednie parametry.

```
Switch_A#configure
```



```
Switch_A(config)#lldp
Switch_A(config)#lldp hold-multiplier 4
Switch_A(config)#lldp timer tx-interval 30
Switch_A(config)#lldp timer tx-delay 2
Switch_A(config)#lldp timer reinit-delay 3
Switch_A(config)#lldp timer notify-interval 5
Switch_A(config)#lldp timer fast-count 3
```

- 2) Ustaw Admin Status portu Fa1/0/1 jako Tx&Rx, włącz Notification Mode i skonfiguruj wszystkie TLVs zawarte w wychodzących pakietach LLDP.

```
Switch_A#configure
Switch_A(config)#interface gigabitEthernet 1/0/1
Switch_A(config-if)#lldp receive
Switch_A(config-if)#lldp transmit
Switch_A(config-if)#lldp snmp-trap
Switch_A(config-if)#lldp tlv-select all
Switch_A(config-if)#end
Switch_A#copy running-config startup-config
```

## Sprawdzanie konfiguracji

### Wyświetlanie ustawień LLDP

```
Switch_A#show lldp

LLDP Status: Enabled
LLDP Forward Message: Disabled
Tx Interval: 30 seconds
TTL Multiplier: 4
Tx Delay: 2 seconds
Initialization Delay: 2 seconds
Trap Notification Interval: 5 seconds
Fast-packet Count: 3
LLDP-MED Fast Start Repeat Count: 4
```

### Wyświetlanie ustawień LLDP na każdym z portów

```
Switch_A#show lldp interface gigabitEthernet 1/0/1
```

```
LLDP interface config:
```

```
gigabitEthernet 1/0/1:
```

```

Admin Status: TxRx
SNMP Trap: Enabled
TLV Status
--- -----
Port-Description Yes
System-Capability Yes
System-Description Yes
System-Name Yes
Management-Address Yes
Port-VLAN-ID Yes
Protocol-VLAN-ID Yes
VLAN-Name Yes
Link-Aggregation Yes
MAC-Physic Yes
Max-Frame-Size Yes
Power Yes
LLDP-MED Status: Disabled
TLV Status
--- -----
Network Policy Yes
Location Identification Yes
Extended Power Via MDI Yes
Inventory Management Yes

```

### Wyświetlanie informacji lokalnych

```
Switch_A#show lldp local-information interface gigabitEthernet 1/0/1
```

```
LLDP local Information:
```

```
gigabitEthernet 1/0/1:
```

|                                    |                                                                |
|------------------------------------|----------------------------------------------------------------|
| Chassis type:                      | MAC address                                                    |
| Chassis ID:                        | 00:0A:EB:13:A2:11                                              |
| Port ID type:                      | Interface name                                                 |
| Port ID:                           | GigabitEthernet1/0/1                                           |
| Port description:                  | GigabitEthernet1/0/1 Interface                                 |
| TTL:                               | 120                                                            |
| System name:                       | T2500G-10TS                                                    |
| System description:                | JetStream 8-Port Gigabit L2 Managed Switch<br>with 2 SFP Slots |
| System capabilities supported:     | Bridge                                                         |
| System capabilities enabled:       | Bridge                                                         |
| Management address type:           | ipv4                                                           |
| Management address:                | 192.168.0.25                                                   |
| Management address interface type: | IfIndex                                                        |
| Management address interface ID:   | 1                                                              |
| Management address OID:            | 0                                                              |
| Port VLAN ID(PVID):                | 1                                                              |
| Port and protocol VLAN ID(PPVID):  | 0                                                              |
| Port and protocol VLAN supported:  | Yes                                                            |
| Port and protocol VLAN enabled:    | No                                                             |
| VLAN name of VLAN 1:               | System-VLAN                                                    |
| Protocol identity:                 |                                                                |
| Auto-negotiation supported:        | Yes                                                            |
| Auto-negotiation enabled:          | Yes                                                            |
| OperMau:                           | speed(1000)/duplex(Full)                                       |
| Link aggregation supported:        | Yes                                                            |
| Link aggregation enabled:          | No                                                             |
| Aggregation port ID:               | 0                                                              |
| Power port class:                  | PSE                                                            |
| PSE power supported:               | Yes                                                            |

|                            |                                                                                                        |
|----------------------------|--------------------------------------------------------------------------------------------------------|
| PSE power enabled:         | No                                                                                                     |
| PSE pairs control ability: | No                                                                                                     |
| Maximum frame size:        | 1518                                                                                                   |
| LLDP-MED Capabilities:     | Capabilities<br>Network Policy<br>Location Identification<br>Extended Power via MDI - PSE<br>Inventory |
| Device Type:               | Network Connectivity                                                                                   |
| Application type:          | Reserved                                                                                               |
| Unknown policy:            | Yes                                                                                                    |
| Tagged:                    | No                                                                                                     |
| VLAN ID:                   | 0                                                                                                      |
| Layer 2 Priority:          | 0                                                                                                      |
| DSCP:                      | 0                                                                                                      |
| Location Data Format:      | Civic Address LCI                                                                                      |
| - What:                    | Switch                                                                                                 |
| - Country Code:            | CN                                                                                                     |
| Power Type:                | PSE Device                                                                                             |
| Power Source:              | Primary                                                                                                |
| Power Priority:            | Low                                                                                                    |
| Power Value:               | 30.0w                                                                                                  |
| Hardware Revision:         | T2500G-10TS 2.0                                                                                        |
| Firmware Revision:         | Reserved                                                                                               |
| Software Revision:         | 2.0.0 Build 20181022 Rel.38882(s)                                                                      |
| Serial Number:             | Reserved                                                                                               |
| Manufacturer Name:         | TP-Link                                                                                                |
| Model Name:                | T2500G-10TS 2.0                                                                                        |
| Asset ID:                  | unknown                                                                                                |

**Wyświetlanie informacji o urządzeniach sąsiadujących**

```
Switch_A#show lldp neighbor-information interface gigabitEthernet 1/0/1
```

```
LLDP Neighbor Information:
```

```
gigabitEthernet 1/0/1:
```

```
Neighbor index 1:
```

|                                    |                                                                |
|------------------------------------|----------------------------------------------------------------|
| Chassis type:                      | MAC address                                                    |
| Chassis ID:                        | 00:0A:EB:13:18:2D                                              |
| Port ID type:                      | Interface name                                                 |
| Port ID:                           | GigabitEthernet1/0/2                                           |
| Port description:                  | GigabitEthernet1/0/2 Interface                                 |
| TTL:                               | 120                                                            |
| System name:                       | T2500G-10TS                                                    |
| System description:                | JetStream 8-Port Gigabit L2 Managed<br>Switch with 2 SFP Slots |
| System capabilities supported:     | Bridge Router                                                  |
| System capabilities enabled:       | Bridge Router                                                  |
| Management address type:           | ipv4                                                           |
| Management address:                | 192.168.0.1                                                    |
| Management address interface type: | IfIndex                                                        |
| Management address interface ID:   | 1                                                              |
| Management address OID:            | 0                                                              |
| Port VLAN ID(PVID):                | 1                                                              |
| Port and protocol VLAN ID(PPVID):  | 0                                                              |
| Port and protocol VLAN supported:  | Yes                                                            |
| Port and protocol VLAN enabled:    | No                                                             |
| VLAN name of VLAN 1:               | System-VLAN                                                    |
| Protocol identity:                 |                                                                |
| Auto-negotiation supported:        | Yes                                                            |
| Auto-negotiation enabled:          | Yes                                                            |
| OperMau:                           | speed(1000)/duplex(Full)                                       |

---

|                             |      |
|-----------------------------|------|
| Link aggregation supported: | Yes  |
| Link aggregation enabled:   | No   |
| Aggregation port ID:        | 0    |
| Power port class:           | PSE  |
| PSE power supported:        | Yes  |
| PSE power enabled:          | No   |
| PSE pairs control ability:  | No   |
| Maximum frame size:         | 1518 |

# Część 15

## Konfiguracja L2PT

### ROZDZIAŁY

1. Informacje ogólne
2. Konfiguracja L2PT
3. Przykład konfiguracji

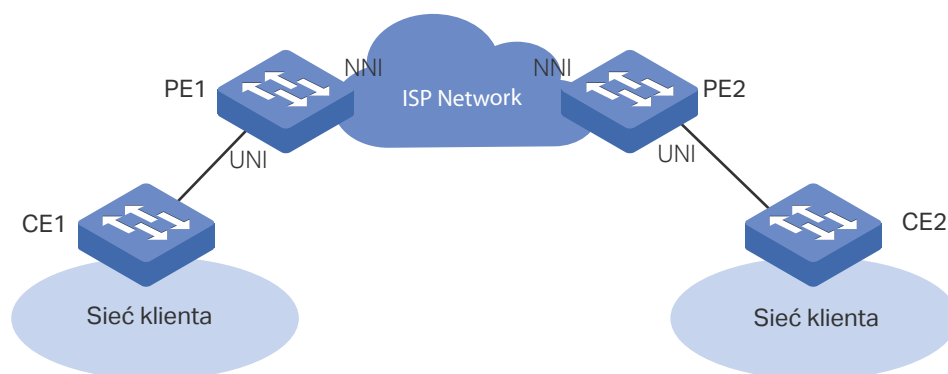
# 1 Informacje ogólne

L2PT (Layer 2 Protocol Tunneling) to funkcja dla usługodawców w celu jawnego przesyłania jednostek danych protokołu (PDU) warstwy 2 pomiędzy sieciami klientów w różnych lokalizacjach a siecią publiczną ISP. Poniżej omówiono wybraną terminologię dotyczącą tego zagadnienia:

- Edge Switch (przełącznik brzegowy): Przełącznik, który jest połączony z siecią klienta i zlokalizowany jest na granicy sieci ISP.
- UNI: User Network Interface, port skonfigurowany na przełączniku brzegowym, który jest połączony z siecią klienta.
- NNI: Network Network Interface, port skonfigurowany na przełączniku brzegowym, który jest połączony z siecią ISP.

Jak pokazano na Rys. 1-1, klient ma dwie sieci lokalne, które połączone są ze sobą poprzez sieć ISP. Gdy obydwie sieci klienta korzystają z tego samego protokołu warstwy 2, ich jednostki danych protokołu (PDUs) warstwy 2 muszą być przesyłane przez sieć ISP, aby umożliwić kalkulację protokołu warstwy 2 (na przykład kalkulację spanning tree). Zasadniczo jednostki PDU tego samego protokołu warstwy 2 korzystają z tego samego docelowego adresu MAC. Zatem gdy PDU warstwy 2 z sieci klienta dotrze do przełącznika brzegowego w sieci ISP, przełącznik nie jest w stanie stwierdzić, czy PDU pochodzi z sieci klienta, czy z sieci ISP, dlatego odrzuca PDU. W rezultacie jednostki PDU warstwy 2 nie mogą być przesyłane przez sieć ISP.

Rys. 1-1 Zastosowanie funkcji L2PT



Aby rozwiązać ten problem, sieć ISP musi jawnie przesyłać jednostki PDU warstwy 2 pomiędzy sieciami klienta. W omawianym przypadku funkcja L2PT może być skonfigurowana na przełącznikach brzegowych (PE1 i PE2), aby umożliwić tunelowanie jednostek PDU warstwy 2 przez sieć.

Poniższe punkty opisują procedurę przesyłania jednostek PDU przez sieć ISP z jednej sieci klienta do drugiej:



- 1) Po odebraniu PDU warstwy 2 od CE1 poprzez port UNI, PE1 zastępuje docelowy adres MAC PDU specjalnym adresem MAC multicast (01:00:0c:cd:cd: d0), a następnie przesyła PDU do sieci ISP poprzez port NNI.
- 2) Sieć ISP identyfikuje jednostkę PDU i przesyła ją bezpośrednio na drugi koniec.
- 3) PE2 odbiera PDU poprzez port NNI i przywraca jego pierwotny docelowy adres MAC.

Gdy funkcja L2PT skonfigurowana jest w sposób prawidłowy, przełącznik może jawnie przysyłać jednostki PDU następujących protokołów warstwy 2: STP (Spanning Tree Protocol), GVRP (GARP VLAN Registration Protocol), LACP (Link Aggregation Control Protocol), CDP (Cisco Discovery Protocol), VTP (VLAN Trunking Protocol), PAgP (Port Aggregation Protocol), UDLD (UniDirectional Link Detection) oraz PVST+(Per VLAN Spanning Tree Plus).

# 2 Konfiguracja L2PT

## 2.1 Przez GUI

Wybierz z menu **L2 FEATURES > L2PT**, aby wyświetlić poniższą stronę.

Rys. 2-1 Konfiguracja L2PT

**L2PT Config**

---

Layer 2 Protocol Tunneling:  Enable Apply

---

**Port Config**

UNIT1

LAGS

|                                     | Port   | Type | Protocol        | Threshold       | LAG |
|-------------------------------------|--------|------|-----------------|-----------------|-----|
| <input checked="" type="checkbox"/> | 1/0/1  | None | ---/---/---/--- | ---/---/---/--- | --- |
| <input type="checkbox"/>            | 1/0/2  | None | ---/---/---/--- | ---/---/---/--- | --- |
| <input type="checkbox"/>            | 1/0/3  | None | ---/---/---/--- | ---/---/---/--- | --- |
| <input type="checkbox"/>            | 1/0/4  | None | ---/---/---/--- | ---/---/---/--- | --- |
| <input type="checkbox"/>            | 1/0/5  | None | ---/---/---/--- | ---/---/---/--- | --- |
| <input type="checkbox"/>            | 1/0/6  | None | ---/---/---/--- | ---/---/---/--- | --- |
| <input type="checkbox"/>            | 1/0/7  | None | ---/---/---/--- | ---/---/---/--- | --- |
| <input type="checkbox"/>            | 1/0/8  | None | ---/---/---/--- | ---/---/---/--- | --- |
| <input type="checkbox"/>            | 1/0/9  | None | ---/---/---/--- | ---/---/---/--- | --- |
| <input type="checkbox"/>            | 1/0/10 | None | ---/---/---/--- | ---/---/---/--- | --- |

Total: 10
1 entry selected.

Cancel
Apply

Wykonaj poniższe kroki, aby skonfigurować L2PT:

- 1) W sekcji **L2PT Config** włącz globalnie L2PT i kliknij **Apply**.
- 2) W sekcji **Port Config** ustaw port podłączony do sieci klienta jako port UNI i określ żądane protokoły na porcie. Ponadto możesz także ustawić na porcie UNI próg przesyłania pakietów na sekundę.

|      |                                                                                                                                                                                                                       |
|------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Port | Numer portu.                                                                                                                                                                                                          |
| Type | Wybierz <b>UNI</b> jako typ portu dla zaznaczonego portu. Port UNI jest zwykle podłączony do sieci klienta.<br><br>Domyślnym ustawieniem jest <b>None</b> , co oznacza, że funkcja L2TP jest wyłączona na tym porcie. |

|           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Protocol  | <p>Określ typy pakietów protokołu warstwy 2, które mogą być jawnie przesyłane na wybranym porcie:</p> <p><b>STP:</b> Włącz tunelowanie protokołu dla pakietów STP.</p> <p><b>GVRP:</b> Włącz tunelowanie protokołu dla pakietów GVRP.</p> <p><b>01000CCCCCCC:</b> Włącz tunelowanie protokołu dla pakietów, których adres docelowy MAC ma wartość 01000CCCCCCC, w tym porty CDP, VTP, PAgP i UDLD.</p> <p><b>01000CCCCCD:</b> Włącz tunelowanie protokołu dla pakietów PVST+, których adres docelowy MAC ma wartość 01000CCCCCD.</p> <p><b>LACP:</b> Włącz tunelowanie protokołu dla pakietów LACP.</p> <p><b>All:</b> Wszystkie powyższe protokoły warstwy 2 mają włączone tunelowanie.</p> |
| Threshold | <p>Określ dla określonego protokołu maksymalną liczbę przesyłania na porcie pakietów na sekundę. Gdy próg ten zostanie przekroczony, port zaczyna odrzucać pakiety protokołu w warstwy 2.</p> <p>Wartość ta waha się od 1 do 1000 (pakietów na sekundę). 0 oznacza, że opcja ta jest wyłączona.</p>                                                                                                                                                                                                                                                                                                                                                                                          |
| LAG       | Grupa LAG, do której należy port.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |

- 3) W sekcji **Port Config** ustaw port podłączony do sieci ISP jako port NNI. Dla tego portu nie można skonfigurować protokołów ani ustawić progu.

|      |                                                                                                                                                                                                                         |
|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Port | Numer portu.                                                                                                                                                                                                            |
| Type | <p>Wybierz <b>NNI</b> jako typ portu dla zaznaczonego portu. Port NNI jest zwykle podłączony do sieci ISP.</p> <p>Domyślnym ustawieniem jest <b>None</b>, co oznacza, że funkcja L2TP jest wyłączona na tym porcie.</p> |
| LAG  | Grupa LAG, do której należy portu.                                                                                                                                                                                      |

- 4) Kliknij **Apply**.



#### Uwaga:

Port przynależący do LAG (Link Aggregation Group) przyjmuje konfigurację LAG, nie jest konfigurowany osobno. Konfigurację samego portu przeprowadzić można dopiero, gdy port opuści grupę LAG.

## 2.2 Przez CLI

Wykonaj poniższe kroki, aby skonfigurować funkcję L2PT.

|        |                                                                     |
|--------|---------------------------------------------------------------------|
| Krok 1 | <p><b>configure</b></p> <p>Uruchom tryb konfiguracji globalnej.</p> |
|--------|---------------------------------------------------------------------|

|        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Krok 2 | <p><b>I2protocol-tunnel</b></p> <p>Włącz globalnie funkcję L2PT.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Krok 3 | <p><b>interface { fastEthernet <i>port</i>   range fastEthernet <i>port-list</i>   gigabitEthernet <i>port</i>   range gigabitEthernet <i>port-list</i>   ten-gigabitEthernet <i>port</i>   range ten-gigabitEthernet <i>port-list</i>   port-channel <i>port-channel-id</i>   range port-channel <i>port-channel-id-list</i> }</b></p> <p>Uruchom tryb konfiguracji interfejsu.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Krok 4 | <p><b>I2protocol-tunnel type uni { 01000cccccc   01000cccccd   gvrp   stp   lacp   all } [ threshold <i>threshold</i> ]</b></p> <p>Ustaw port jako port UNI, określ typy pakietów protokołu warstwy 2, które mogą być jawnie przesyłane na tym porcie i ustaw próg dla pakietów na sekundę, akceptowanych do kapsułkowania na porcie UNI.</p> <p><b>01000cccccc:</b> Włącz tunelowanie protokołu dla pakietów, których adres docelowy MAC ma wartość 01000CCCCCC, w tym porty CDP, VTP, PAgP i UDLD.</p> <p><b>01000cccccd:</b> Włącz tunelowanie protokołu dla pakietów PVST+, których adres docelowy MAC ma wartość 01000CCCCCD.</p> <p><b>gvrp:</b> Włącz tunelowanie protokołu dla pakietów GVRP.</p> <p><b>stp:</b> Włącz tunelowanie protokołu dla pakietów STP.</p> <p><b>lacp:</b> Włącz tunelowanie protokołu dla pakietów LACP.</p> <p><b>all:</b> Wszystkie powyższe protokoły warstwy 2 mają włączone tunelowanie.</p> <p><b>threshold:</b> Określ dla określonego protokołu maksymalną liczbę przesyłania na porcie pakietów na sekundę. Gdy próg ten zostanie przekroczony, port zaczyna odrzucać pakiety protokołu w warstwy 2. Wartość ta waha się od 1 do 1000 (pakietów na sekundę). 0 oznacza, że opcja ta jest wyłączona.</p> |
| Krok 5 | <p><b>exit</b></p> <p>Wróć do trybu konfiguracji globalnej.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Krok 6 | <p><b>interface { fastEthernet <i>port</i>   range fastEthernet <i>port-list</i>   gigabitEthernet <i>port</i>   range gigabitEthernet <i>port-list</i>   ten-gigabitEthernet <i>port</i>   range ten-gigabitEthernet <i>port-list</i>   port-channel <i>port-channel-id</i>   range port-channel <i>port-channel-id-list</i> }</b></p> <p>Uruchom tryb konfiguracji interfejsu.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Krok 7 | <p><b>I2protocol-tunnel type nni</b></p> <p>Ustaw port jako port NNI.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Krok 8 | <p><b>show I2protocol-tunnel global</b></p> <p>Sprawdź globalną konfigurację L2PT.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Krok 9 | <p><b>show I2protocol-tunnel interface [ fastEthernet <i>port</i>   gigabitEthernet <i>port</i>   ten-gigabitEthernet <i>port</i>   port-channel <i>port-channel-id</i> ]</b></p> <p>Sprawdź konfigurację L2PT portu lub jego grupy LAG.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |

Krok 10      **end**  
Powróć do trybu privileged EXEC .

Krok 11      **copy running-config startup-config**  
Zapisz ustawienia w pliku konfiguracyjnym.

 **Uwaga:**

Port przynależący do LAG (Link Aggregation Group) przyjmuje konfigurację LAG, nie jest konfigurowany osobno. Konfigurację samego portu przeprowadzić można dopiero, gdy port opuści grupę LAG.

Poniższy przykład przedstawia globalne włączanie funkcji L2PT:

```
Switch#configure
Switch(config)#l2protocol-tunnel
Switch(config)#show l2protocol-tunnel global
l2protocol-tunnel State: Enable
Switch(config)#end
Switch#copy running-config startup-config
```

Poniższy przykład przedstawia sposób ustawiania portu 1/0/1 jako portu UNI dla protokołu GVRP warstwy 2 i progu jako 1000:

```
Switch#configure
Switch(config)#interface gigabitEthernet 1/0/1
Switch(config-if)#l2protocol-tunnel type uni gvrp threshold 1000
Switch(config-if)#show l2protocol-tunnel interface gigabitEthernet 1/0/1
```

| Interface | Type | Protocol         | Threshold        | LAG  |
|-----------|------|------------------|------------------|------|
| -----     | ---- | -----            | -----            | ---- |
| Gi1/0/1   | uni  | gvrp,--,--,--,-- | 1000,--,--,--,-- | N/A  |

```
Switch(config-if)#end
Switch#copy running-config startup-config
```

Poniższy przykład przedstawia sposób ustawiania portu 1/0/5 jako portu NNI.

```
Switch#configure
Switch(config)#interface gigabitEthernet 1/0/5
```

```
Switch(config-if)#l2protocol-tunnel type nni
```

```
Switch(config-if)#show l2protocol-tunnel interface gigabitEthernet 1/0/5
```

| Interface | Type | Protocol       | Threshold      | LAG  |
|-----------|------|----------------|----------------|------|
| -----     | ---- | -----          | -----          | ---- |
| Gi1/0/5   | nni  | --,--,--,--,-- | --,--,--,--,-- | N/A  |

```
Switch(config-if)#end
```

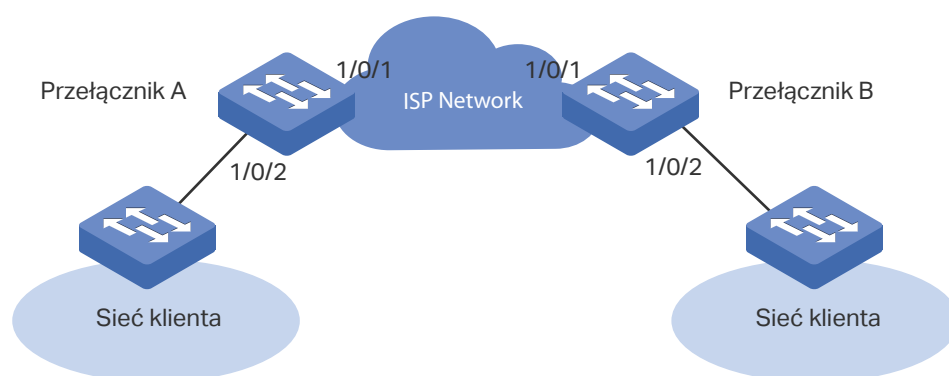
```
Switch#copy running-config startup-config
```

# 3 Przykład konfiguracji

## 3.1 Wymagania sieciowe

Jako pokazano poniżej, dwa oddziały firmy połączone są poprzez sieć ISP, a ich celem jest kalkulacja spanning tree w wyniku wzajemnej wymiany pakietów STP warstwy 2. Aby spełnić ten warunek, pakiety STP muszą być jawnie przesyłane pomiędzy sieciami klienta poprzez sieć ISP.

Rys. 3-1 Topologia sieci



## 3.2 Schemat konfiguracji

Usługodawca może skonfigurować funkcję L2PT na dwóch przełącznikach brzegowych (przełącznik A i przełącznik B). Przy włączonej funkcji L2PT pakiety STP mogą być kapsułkowane jako normalne pakiety danych i przesyłane na drugi koniec bez przetwarzania na urządzeniach w sieci ISP.

Konfiguracja wymaga wykonania następujących kroków:

- 1) Włącz globalnie funkcję L2PT.
- 2) Ustaw port 1/0/1, który jest podłączony do sieci ISP, jako port NNI.
- 3) Ustaw port 1/0/2, który jest podłączony do sieci klienta, jako port UNI dla STP. Ponadto ustaw wartość progu jako 1000, aby wprowadzić limit liczby pakietów przetwarzanych na porcie w ciągu sekundy.

W poniższych podrozdziałach opisano dwa sposoby przeprowadzenia procedury konfiguracji: przez GUI oraz przez CLI.

### 3.3 Przez GUI

Ustawienia przełącznika A i przełącznika B są takie same. Poniższy instruktaż omówimy na przykładzie przełącznika A.

- 1) Wybierz z menu **L2 FEATURES > L2PT**, aby wyświetlić poniższą stronę. Włącz globalnie funkcję L2PT i kliknij **Apply**.
- 2) Ustaw port 1/0/1 jako port NNI i kliknij **Apply**. Ustaw port 1/0/2 jako port UNI dla STP i ustaw wartość progu jako 1000. Następnie kliknij **Apply**. Rezultat jest następujący:

Rys. 3-2 Konfiguracja globalna


L2PT Config

Layer 2 Protocol Tunneling:  Enable Apply

Port Config

| UNIT1                               |        | LAGS     |           |      |
|-------------------------------------|--------|----------|-----------|------|
| Port                                | Type   | Protocol | Threshold | LAG  |
| <input type="checkbox"/>            | UNI    | STP      | 1000      | ---  |
| <input checked="" type="checkbox"/> | 1/0/1  | NNI      | ---       | ---  |
| <input checked="" type="checkbox"/> | 1/0/2  | UNI      | STP       | 1000 |
| <input type="checkbox"/>            | 1/0/3  | None     | ---       | ---  |
| <input type="checkbox"/>            | 1/0/4  | None     | ---       | ---  |
| <input type="checkbox"/>            | 1/0/5  | None     | ---       | ---  |
| <input type="checkbox"/>            | 1/0/6  | None     | ---       | ---  |
| <input type="checkbox"/>            | 1/0/7  | None     | ---       | ---  |
| <input type="checkbox"/>            | 1/0/8  | None     | ---       | ---  |
| <input type="checkbox"/>            | 1/0/9  | None     | ---       | ---  |
| <input type="checkbox"/>            | 1/0/10 | None     | ---       | ---  |

Total: 10 1 entry selected. Cancel Apply

- 3) Kliknij  **Save**, aby zapisać ustawienia.

### 3.4 Przez CLI

Ustawienia przełącznika A i przełącznika B są takie same. Poniższy instruktaż opiera się na konfiguracji przełącznika A.

```
Switch_A#configure
```

```
Switch_A(config)#l2protocol-tunnel
```

```
Switch_A(config)#interface gigabitEthernet 1/0/1
```

```
Switch_A(config-if)#l2protocol-tunnel type nni
```

```
Switch_A(config-if)#exit
```



```
Switch_A(config)#interface gigabitEthernet 1/0/2
Switch_A(config-if)#l2protocol-tunnel type uni stp 1000
Switch_A(config-if)#end
Switch_A#copy running-config startup-config
```

### Sprawdzanie konfiguracji

Sprawdzanie konfiguracji globalnej:

```
Switch_A#show l2protocol-tunnel global
```

```
l2protocol-tunnel State: Enable
```

Sprawdzanie konfiguracji na porcie 1/0/1:

```
Switch_A#show l2protocol-tunnel interface gigabitEthernet 1/0/1
```

| Interface | Type | Protocol    | Threshold   | LAG  |
|-----------|------|-------------|-------------|------|
| -----     | ---- | -----       | -----       | ---- |
| Gi1/0/1   | nni  | --,--,--,-- | --,--,--,-- | N/A  |

Sprawdzanie konfiguracji na porcie 1/0/2:

```
Switch_A#show l2protocol-tunnel interface gigabitEthernet 1/0/2
```

| Interface | Type | Protocol     | Threshold     | LAG  |
|-----------|------|--------------|---------------|------|
| -----     | ---- | -----        | -----         | ---- |
| Gi1/0/2   | uni  | stp,--,--,-- | 1000,--,--,-- | N/A  |

# Część 16

## Konfiguracja PPPoE ID Insertion

### ROZDZIAŁY

1. Informacje ogólne
2. Konfiguracja PPPoE ID Insertion

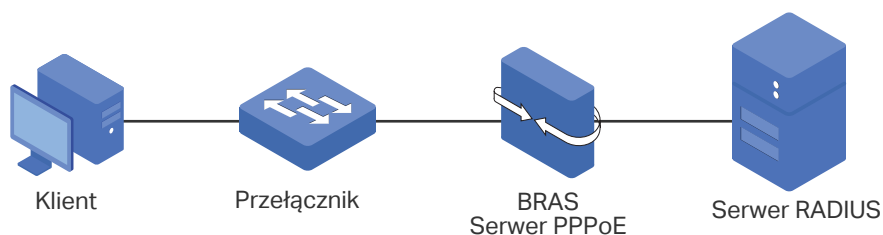
# 1 Informacje ogólne

W zwykłym trybie połączeń dial-up PPPoE, gdy użytkownicy nawiązują połączenie przez PPPoE, dostęp do sieci otrzymają tylko w przypadku, gdy ich konta zostaną uwierzytelnione na serwerze RADIUS. W rezultacie pojawia się ryzyko, że nielegalni użytkownicy przejmą konto w celu uzyskania dostępu do Internetu.

Funkcja PPPoE ID Insertion zapewnia rozwiązanie tego problemu. Włączenie tej funkcji sprawia, że przełącznik dołącza tag do pakietów PPPoE Active Discovery otrzymanych od klienta i przesyła go do BRAS (Broadband Remote Access Server). Tag rejestruje informacje o kliencie, w tym o numerze podłączonego portu oraz jego adresie MAC. BRAS używa tagu jako atrybutu NAS-Port-ID w pakiecie RADIUS i przesyła go do serwera RADIUS w celu przeprowadzenia uwierzytelnienia PPP (Point-to-Point Protocol). Jeśli informacje tagu będą różnić się od informacji konfiguracyjnych, uwierzytelnianie nie powiedzie się. W ten sposób nielegalni użytkownicy nie są w stanie przejąć kont użytkowników legalnych w celu uzyskania dostępu do Internetu.

Ponadto po otrzymaniu pakietu PPPoE Active Discovery Offer lub pakietu potwierdzającego sesję z BRAS, przełącznik usunie tag z pakietu i prześle go do klienta.

Rys. 1-1 Topologia sieci PPPoE ID-Insertion



# 2 Konfiguracja PPPoE ID Insertion

## 2.1 Przez GUI

Wybierz z menu **L2 FEATURES > PPPoE**, aby wyświetlić poniższą stronę.

Rys. 2-1 Konfiguracja PPPoE ID Insertion

PPPoE ID Insertion

---

PPPoE ID Insertion:  Enable Apply

Port Config

---

UNIT1

LAGS

| <input type="checkbox"/>            | Port   | Circuit-ID | Circuit-ID Type | UDF Value | Remote-ID | Remote-ID Value |
|-------------------------------------|--------|------------|-----------------|-----------|-----------|-----------------|
| <input checked="" type="checkbox"/> | 1/0/1  | Disabled   | IP              | ---       | Disabled  | ---             |
| <input type="checkbox"/>            | 1/0/2  | Disabled   | IP              | ---       | Disabled  | ---             |
| <input type="checkbox"/>            | 1/0/3  | Disabled   | IP              | ---       | Disabled  | ---             |
| <input type="checkbox"/>            | 1/0/4  | Disabled   | IP              | ---       | Disabled  | ---             |
| <input type="checkbox"/>            | 1/0/5  | Disabled   | IP              | ---       | Disabled  | ---             |
| <input type="checkbox"/>            | 1/0/6  | Disabled   | IP              | ---       | Disabled  | ---             |
| <input type="checkbox"/>            | 1/0/7  | Disabled   | IP              | ---       | Disabled  | ---             |
| <input type="checkbox"/>            | 1/0/8  | Disabled   | IP              | ---       | Disabled  | ---             |
| <input type="checkbox"/>            | 1/0/9  | Disabled   | IP              | ---       | Disabled  | ---             |
| <input type="checkbox"/>            | 1/0/10 | Disabled   | IP              | ---       | Disabled  | ---             |

Total: 10
1 entry selected.

Cancel
Apply

Wykonaj poniższe kroki, aby skonfigurować PPPoE ID-Insertion:

- 1) W sekcji **PPPoE ID Insertion** włącz PPPoE ID Insertion i kliknij **Apply**.
- 2) W sekcji **Port Config** wybierz co najmniej jeden port i skonfiguruj odpowiednie parametry. Następnie kliknij **Apply**.

|                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Circuit-ID      | Włącz lub wyłącz funkcję Circuit-ID Insertion. Przy włączonej opcji przełącznik będzie umieszczać Circuit ID w odebranych na danym porcie pakietach PPPoE Discovery.                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Circuit-ID Type | Wybierz typ Circuit ID. Dostępne są następujące opcje:<br><br><b>IP:</b> Circuit ID zawiera następujące trzy części: źródłowy adres MAC odebranego pakietu, adres IP przełącznika i numer portu. Ten typ jest ustawieniem domyślnym.<br><br><b>MAC:</b> Circuit ID zawiera następujące trzy części: źródłowy adres MAC pakietu, adres MAC przełącznika i numer portu.<br><br><b>UDF:</b> Circuit ID zawiera następujące trzy części: źródłowy adres MAC pakietu, ciąg znaków ustalony przez użytkownika i numer portu.<br><br><b>UDF Only:</b> Do kodowania opcji Circuit-ID stosowany będzie wyłącznie ciąg znaków ustalony przez użytkownika. |
| UDF Value       | Jeśli wybierzesz typ UDF lub UDF Only, podaj ciąg maksymalnie 40 znaków w celu kodowania opcji Circuit-ID.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Remote-ID       | Włącz lub wyłącz funkcję Remote-ID Insertion. Przy włączonej opcji przełącznik będzie umieszczać Remote ID w odebranych na danym porcie pakietach PPPoE Discovery.                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Remote-ID Value | Podaj ciąg maksymalnie 40 znaków w celu kodowania opcji Remote-ID.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |

 **Uwaga:**

Port przynależący do LAG (Link Aggregation Group) przyjmuje konfigurację LAG, nie jest konfigurowany osobno. Konfigurację samego portu przeprowadzić można dopiero, gdy port opuści grupę LAG.

## 2.2 Przez CLI

Wykonaj poniższe kroki, aby skonfigurować funkcję PPPoE ID Insertion:

|        |                                                                                                                                                                                                                                                                                    |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Krok 1 | <b>configure</b><br>Uruchom tryb konfiguracji globalnej.                                                                                                                                                                                                                           |
| Krok 2 | <b>pppoe id-insertion</b><br>Uruchom globalnie funkcję PPPoE ID Insertion.                                                                                                                                                                                                         |
| Krok 3 | <b>interface { fastEthernet <i>port</i>   range fastEthernet <i>port-list</i>   gigabitEthernet <i>port</i>   range gigabitEthernet <i>port-list</i>   ten-gigabitEthernet <i>port</i>   range ten-gigabitEthernet <i>port-list</i> }</b><br>Uruchom tryb konfiguracji interfejsu. |
| Krok 4 | <b>pppoe circuit-id</b><br>Włącz funkcję Circuit-ID Insertion, aby przełącznik umieszczał Circuit ID w odebranych na danym porcie pakietach PPPoE Discovery.                                                                                                                       |

|         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|---------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Krok 5  | <p><b>pppoe circuit-id type { mac   ip   udf [Value]   udf-only [Value] }</b></p> <p>Wybierz typ Circuit ID. Dostępne są następujące opcje:</p> <p><b>mac:</b> Do kodowania opcji Circuit-ID stosowany będzie źródłowy adres MAC pakietu, adres MAC przełącznika i numer portu.</p> <p><b>ip:</b> Circuit ID zawiera następujące trzy części: źródłowy adres MAC odebranego pakietu, adres IP przełącznika i numer portu. Ten typ jest ustawieniem domyślnym.</p> <p><b>udf [Value]:</b> Podaj ciąg maksymalnie 40 znaków. Circuit ID zawiera następujące trzy części: źródłowy adres MAC pakietu, ustalony ciąg znaków i numer portu.</p> <p><b>udf-only [Value]:</b> Podaj ciąg maksymalnie 40 znaków. Do kodowania opcji Circuit-ID stosowany będzie wyłącznie ustalony ciąg znaków</p> |
| Krok 6  | <p><b>pppoe remote-id [Value]</b></p> <p>Włącz funkcję Remote-ID Insertion i ustaw Remote ID.</p> <p><b>Value:</b> Podaj ciąg maksymalnie 40 znaków. Do kodowania opcji Remote-ID stosowany będzie źródłowy adres MAC pakietu i ustalony ciąg znaków.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Krok 7  | <p><b>show pppoe id-insertion global</b></p> <p>Sprawdź globalną konfigurację funkcji PPPoE ID Insertion.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Krok 8  | <p><b>show pppoe id-insertion interface { fastEthernet port   gigabitEthernet port   ten-gigabitEthernet port }</b></p> <p>Sprawdź konfigurację funkcji PPPoE ID Insertion na porcie.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Krok 9  | <p><b>end</b></p> <p>Powróć do trybu privileged EXEC.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Krok 10 | <p><b>copy running-config startup-config</b></p> <p>Zapisz ustawienia w pliku konfiguracyjnym.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |

Poniższy przykład przedstawia sposób globalnego włączania funkcji PPPoE ID Insertion na porcie 1/0/1 i ustawiania Circuit-ID do wartości 123 bez podawania innych informacji oraz ustawiania Remote-ID jako host1.

**Switch#configure**

**Switch(config)#pppoe id-insertion**

**Switch(config-if)#interface gigabitEthernet 1/0/1**

**Switch(config-if)#pppoe circuit-id**

**Switch(config-if)#pppoe circuit-id type udf-only 123**

**Switch(config-if)#pppoe remote-id host1**

**Switch(config-if)#show pppoe id-insertion global**

PPPoE ID Insertion State: Enabled

```
Switch(config-if)#show pppoe id-insertion interface gigabitEthernet 1/0/1
```

| Port    | Circuit-ID | C-ID Type | C-ID Value(UDF) | Remote-ID | R-ID Value |
|---------|------------|-----------|-----------------|-----------|------------|
| -----   | -----      | -----     | -----           | -----     | -----      |
| Gi1/0/1 | Enabled    | UDF-ONLY  | 123             | Enabled   | host1      |

```
Switch(config-if)#end
```

```
Switch#copy running-config startup-config
```

**Uwaga:**

Port przynależący do LAG (Link Aggregation Group) przyjmuje konfigurację LAG, nie jest konfigurowany osobno. Konfigurację samego portu przeprowadzić można dopiero, gdy port opuści grupę LAG.

# Część 17

## Konfiguracja usługi DHCP

### ROZDZIAŁY

1. DHCP
2. Konfiguracja DHCP Relay
3. Konfiguracja DHCP L2 Relay
4. Przykład dla DHCP VLAN Relay



# 1 DHCP

## 1.1 Informacje ogólne

DHCP (Dynamic Host Configuration Protocol) jest to powszechnie stosowany protokół do automatycznego przydzielania urządzeniom sieciowym adresów IP oraz innych parametrów konfiguracji sieci, co umożliwia efektywniejsze wykorzystanie adresu IP.

## 1.2 Obsługiwane funkcje

Obsługiwane przez przełącznik funkcje DHCP to DHCP Relay i DHCP L2 Relay.

### DHCP Relay

DHCP Relay służy do przetwarzania i przekazywania pakietów DHCP między różnymi podsieciami lub sieciami VLAN.

Klient DHCP wysyła pakiety żądania DHCP (DHCP Request) w celu pozyskania adresu IP. Przesyłanie pakietów broadcastowych zawsze ograniczone jest do jednego LAN, jeżeli więc serwer DHCP i klient nie należą do tego samego LAN, klient nie ma możliwości uzyskania adresu IP z serwera DHCP. Każdy LAN powinien zatem być wyposażony w serwer DHCP, co zwiększa koszty budowy sieci i stanowi utrudnienie w centralnym zarządzaniu siecią.

Funkcja DHCP Relay stanowi rozwiązanie problemu. Urządzenie z DHCP Relay pełni funkcję agenta przekazywania i przesyła pakiety DHCP między klientami DHCP i serwerami DHCP w różnych sieciach LAN. Dzięki temu klienci DHCP z różnych sieci LAN mogą dzielić jeden serwer DHCP.

Funkcja DHCP Relay obsługuje opcję 82 (Option 82) i DHCP VLAN Relay.

#### ■ Option 82

Dzięki opcji 82 przełącznik może rejestrować dane lokalizacyjne klienta DHCP. Przełącznik może dodać opcję 82 do pakietu żądania DHCP i przesłać pakiet do serwera DHCP. Serwer DHCP z obsługą opcji 82 może ustawić strategię rozdziału adresów IP i inne parametry, zapewniając bardziej elastyczny sposób rozdziału adresów.

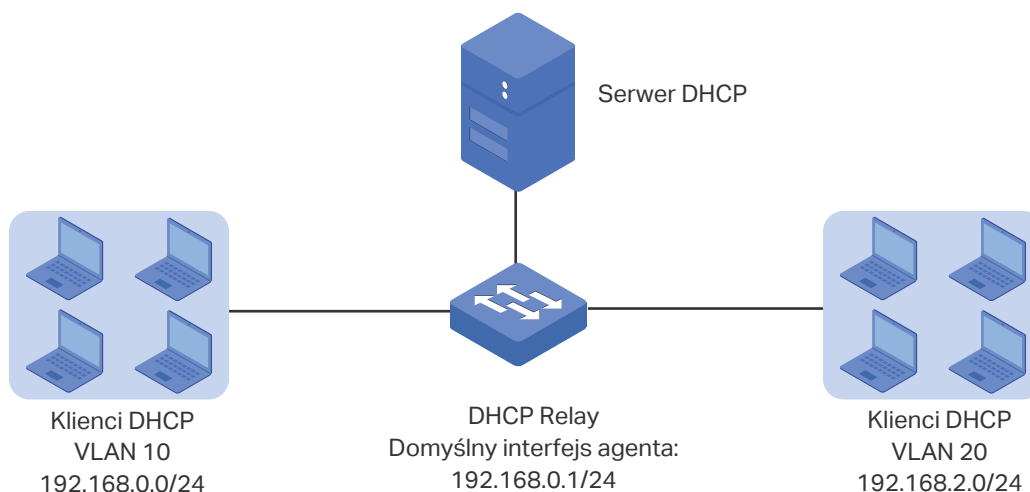
#### ■ DHCP VLAN Relay

DHCP VLAN Relay umożliwia klientom z różnych sieci VLAN pozyskiwanie adresów IP z serwera DHCP przy wykorzystaniu jednego adresu IP interfejsu agenta.

Dzięki DHCP VLAN Relay możesz ustawić VLAN interface 1 (domyślny interfejs zarządzania VLAN) jako domyślny interfejs agenta dla wszystkich sieci VLAN. Przełącznik wpisze adres IP domyślnego interfejsu agenta w pole adresu IP agenta przekazywania pakietów DHCP ze wszystkich sieci VLAN.

Jak przedstawiono na poniższym rysunku, do VLAN 10 i VLAN 20 nie przypisano żadnych adresów. Przełącznik wykorzystuje adres IP domyślnego interfejsu agenta (192.168.0.1/24) w celu zaaplikowania o adresy IP dla klientów obu sieci, VLAN 10 i VLAN 20. W rezultacie serwer DHCP przypisze adresy IP na 192.168.0.0/24 (ta sama podsieć co adres IP domyślnego interfejsu agenta) klientom obu sieci, VLAN 10 i VLAN 20.

Rys. 1-1 Zastosowanie DHCP VLAN Relay



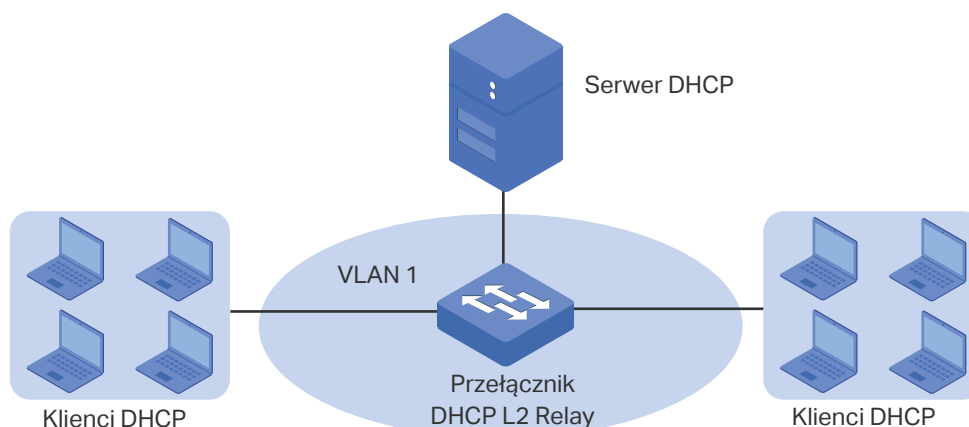
#### Uwaga:

W przełącznikach serii T1500 tylko interfejs zarządzania VLAN może być ustawiony jako domyślny interfejs agenta przekazywania.

## DHCP L2 Relay

W przeciwieństwie do DHCP relay, DHCP L2 Relay wykorzystywany jest w sytuacji, gdy serwer DHCP i klient znajdują się w jednej sieci VLAN. Dzięki DHCP L2 Relay poza standardowym przypisywaniem adresów IP klientom z serwera DHCP, przełącznik może również rejestrować dane lokalizacyjne klienta DHCP za pomocą opcji 82. Przełącznik może dodać opcję 82 do pakietu żądania DHCP i przekazać pakiet do serwera DHCP. Serwer DHCP z obsługą opcji 82 może ustawić strategię rozdziału adresów IP i inne parametry, zapewniając bardziej elastyczny sposób rozdziału adresów.

Rys. 1-2 Zastosowanie DHCP L2 Relay



# 2 Konfiguracja DHCP Relay

Aby przeprowadzić konfigurację DHCP Relay, wykonaj poniższe kroki:

- 1) Włącz DHCP Relay. W razie konieczności skonfiguruj Opcję 82.
- 2) Wyznacz serwer DHCP na interfejsie lub w sieci VLAN.

## 2.1 Przez GUI

### 2.1.1 Włączanie DHCP Relay i konfiguracja Opcji 82

Wybierz z menu **L3 FEATURES > DHCP Service > DHCP Relay > DHCP Relay Config**, aby wyświetlić poniższą stronę.

Rys. 2-1 Włączanie DHCP Relay i konfiguracja Opcji 82

**Global Config**

---

DHCP Relay:  Enable

DHCP Relay Hops:  (1-16)

DHCP Relay Time Threshold:  seconds (0-65535)

[Apply](#)

---

**Option 82 Config**

UNIT1

LAGS

| <input type="checkbox"/> | Port   | Option 82 Support | Option 82 Policy | Format | Circuit ID Customization | Circuit ID | Remote ID Customization | Remote ID | LAG |
|--------------------------|--------|-------------------|------------------|--------|--------------------------|------------|-------------------------|-----------|-----|
| <input type="checkbox"/> | 1/0/1  | Disabled          | Keep             | Normal | Disabled                 |            | Disabled                |           | --- |
| <input type="checkbox"/> | 1/0/2  | Disabled          | Keep             | Normal | Disabled                 |            | Disabled                |           | --- |
| <input type="checkbox"/> | 1/0/3  | Disabled          | Keep             | Normal | Disabled                 |            | Disabled                |           | --- |
| <input type="checkbox"/> | 1/0/4  | Disabled          | Keep             | Normal | Disabled                 |            | Disabled                |           | --- |
| <input type="checkbox"/> | 1/0/5  | Disabled          | Keep             | Normal | Disabled                 |            | Disabled                |           | --- |
| <input type="checkbox"/> | 1/0/6  | Disabled          | Keep             | Normal | Disabled                 |            | Disabled                |           | --- |
| <input type="checkbox"/> | 1/0/7  | Disabled          | Keep             | Normal | Disabled                 |            | Disabled                |           | --- |
| <input type="checkbox"/> | 1/0/8  | Disabled          | Keep             | Normal | Disabled                 |            | Disabled                |           | --- |
| <input type="checkbox"/> | 1/0/9  | Disabled          | Keep             | Normal | Disabled                 |            | Disabled                |           | --- |
| <input type="checkbox"/> | 1/0/10 | Disabled          | Keep             | Normal | Disabled                 |            | Disabled                |           | --- |

Total: 10

Wykonaj poniższe kroki, aby włączyć opcję DHCP Relay i skonfigurować Opcję 82:

- 1) W sekcji **Global Config** włącz DHCP Relay globalnie i skonfiguruj przeskok przekaźnika i próg czasu. Kliknij **Apply**.

|                           |                                                                                                                                                                                                                                                                                                                                                                                                                 |
|---------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DHCP Relay                | Włącz DHCP Relay globalnie.                                                                                                                                                                                                                                                                                                                                                                                     |
| DHCP Relay Hops           | <p>Wyznacz przeskoki DHCP relay.</p> <p>DHCP Relay Hops to maksymalna liczba przeskoków (DHCP Relay agent), w których mogą być przekazywane pakiety DHCP. Jeżeli liczba przeskoków pakietu będzie większa, niż ustawiona w tym miejscu wartość, pakiet zostanie odrzucony.</p>                                                                                                                                  |
| DHCP Relay Time Threshold | <p>Wyznacz prób czasu przekaźnika DHCP. Wartość powinna wynosić od 0 do 65535 sekund.</p> <p>Czas przekaźnika DHCP to czas, który upłynął od kiedy klient rozpoczął pozyskiwanie adresu i proces odnowy. Jeżeli czas jest dłuższy niż ustawiona w tym miejscu wartość, pakiet DHCP zostanie odrzucony przez przełącznik. Wartość 0 oznacza, że przełącznik nie będzie sprawdzać tego obszaru pakietów DHCP.</p> |

## 2) (Opcjonalnie) W sekcji **Option 82 Config** skonfiguruj opcję 82.

|                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|--------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Option 82 Support        | Zaznacz, czy chcesz włączyć opcję 82. Opcja jest domyślnie wyłączona. Opcja 82 wykorzystywana jest do zapisu lokalizacji DHCP klienta, portu Ethernet, VLAN itd. Jeżeli chcesz zapisać aktualną lokalizację klienta, możesz włączyć opcję 82 na urządzeniu przekaźnikowym, znajdującym się najbliżej niego.                                                                                                                                                                                                                       |
| Option 82 Policy         | <p>Wybierz działanie dla pola opcji 82 pakietów żądania DHCP.</p> <p><b>Keep (zachowaj):</b> Oznacza zachowanie pola opcji 82.</p> <p><b>Replace (zastąp):</b> Oznacza zastąpienie pola opcji 82 polem wyznaczonym przez przełącznik. Domyślnie Circuit ID zdefiniowany jest jako VLAN i ID portu, który odbiera pakiety DHCP Request (żądanie DHCP). Remote ID to adres MAC urządzenia DHCP Relay, które odbiera pakiety żądania DHCP.</p> <p><b>Drop (odrzuć):</b> Oznacza odrzucanie pakietów zawierających pole opcji 82.</p> |
| Format                   | <p>Wybierz format pola wartości podopcji opcji 82.</p> <p><b>Normal:</b> Oznacza zachowanie formatu TLV (ang. type-length-value, typ-długość-wartość).</p> <p><b>Private:</b> Oznacza, że format pola wartości podopcji zakłada podanie samej wartości.</p>                                                                                                                                                                                                                                                                       |
| Circuit ID Customization | Włącz lub wyłącz Customization of Option 82 (dostosowywanie opcji 82). Jeżeli funkcja jest włączona, należy skonfigurować dane opcji 82 ręcznie. Jeżeli funkcja jest wyłączona, przełącznik automatycznie skonfiguruje VLAN ID i ID portu, który odbiera pakiety DHCP jako circuit ID.                                                                                                                                                                                                                                            |
| Circuit ID               | Wprowadź zindywidualizowany circuit ID, składający się z maks. 64 znaków. Ustawienia circuit ID przełącznika i serwera DHCP powinny być ze sobą kompatybilne.                                                                                                                                                                                                                                                                                                                                                                     |
| Remote ID Customization  | Włącz lub wyłącz przełącznik w celu zdefiniowania pola Remote ID – podopcji opcji 82. Jeżeli jest włączone, możesz ręcznie skonfigurować zdalny ID. Jeżeli jest wyłączone, przełącznik automatycznie skonfiguruje adres MAC przełącznika jako zdalny ID.                                                                                                                                                                                                                                                                          |

|           |                                                                                                                                                               |
|-----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Remote ID | Wprowadź zindywidualizowany zdalny ID, składający się z maks. 64 znaków. Ustawienia zdalnego ID przełącznika i serwera DHCP powinny być ze sobą kompatybilne. |
|-----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|

3) Kliknij **Apply**.

## 2.1.2 Konfiguracja DHCP VLAN Relay

DHCP VLAN Relay wykorzystywany jest dla klientów w sieciach VLAN, ale nie posiada interfejsu warstwy trzeciej jako bramy do pozyskiwania adresów IP z serwera DHCP, który nie należy do tej samej podsieci co klienci.

Wybierz menu **L3 FEATURES > DHCP Service > DHCP Relay > DHCP VLAN Relay**, aby załadować następującą stronę.

Rys. 2-2 Wyznaczanie serwera DHCP dla sieci VLAN

Default Relay Agent Interface

---

Interface ID: VLAN ▼ 1 (1-4094)

IP Address: 192.168.0.150

Apply

---

DHCP VLAN Relay Config

+ Add - Delete

| <input type="checkbox"/>  | Index | VLAN ID | Server Address |
|---------------------------|-------|---------|----------------|
| No entries in this table. |       |         |                |
| Total: 0                  |       |         |                |

Wykonaj poniższe kroki, aby wyznaczyć serwer DHCP dla wybranej sieci VLAN:

- 1) W sekcji **Default Relay Agent Interface** ustaw VLAN zarządzający (domyślnie jest to VLAN 1) jako domyślny interfejs agenta przekazywania. Przełącznik poda jej adres IP do pola adresu IP agenta przekazywania w pakietach DHCP po zapytaniu o adresy IP z serwera DHCP. Kliknij **Apply**.

|              |                                                                                                  |
|--------------|--------------------------------------------------------------------------------------------------|
| Interface ID | Określ typ i ID interfejsu, który będzie ustawiony jako domyślny interfejs agenta przekazywania. |
|--------------|--------------------------------------------------------------------------------------------------|

Na domyślny interfejs agenta przekazywania ustawić możesz każdy z interfejsów warstwy 3. Serwer DHCP przypisze adresy IP w tej samej podsieci co interfejs agenta przekazywania do klientów, którzy wykorzystują ten interfejs agenta przekazywania do ubiegania się o adresy IP.

|            |                                    |
|------------|------------------------------------|
| IP Address | Informuje o adresie IP interfejsu. |
|------------|------------------------------------|

- 2) W sekcji **DHCP VLAN Relay Config** kliknij + Add, aby wyświetlić następującą stronę.

DHCP VLAN Relay

VLAN ID:  (1-4094)

Server Address:  (Format: 192.168.0.1)

Cancel
Create

Określ, do której sieci VLAN należą klienci i adres IP serwera DHCP. Kliknij **Create**.

|                |                                                                            |
|----------------|----------------------------------------------------------------------------|
| VLAN ID        | Określ sieć VLAN, w której klienci mogą pozyskać adresy IP z serwera DHCP. |
| Server Address | Wpisz adres IP serwera DHCP.                                               |

## 2.2 Przez CLI

### 2.2.1 Włączanie DHCP Relay

Wykonaj poniższe kroki, aby włączyć DHCP Relay i skonfigurować odpowiednie parametry:

|        |                                                                                                    |
|--------|----------------------------------------------------------------------------------------------------|
| Krok 1 | <p><b>configure</b></p> <p>Uruchom tryb konfiguracji globalnej.</p>                                |
| Krok 2 | <p><b>service dhcp relay</b></p> <p>Włącz DHCP Relay.</p>                                          |
| Krok 3 | <p><b>show ip dhcp relay</b></p> <p>Sprawdź ustawienia DHCP Relay.</p>                             |
| Krok 4 | <p><b>end</b></p> <p>Powróć do trybu privileged EXEC.</p>                                          |
| Krok 5 | <p><b>copy running-config startup-config</b></p> <p>Zapisz ustawienia w pliku konfiguracyjnym.</p> |

Poniższy przykład prezentuje włączanie DHCP Relay, konfigurację przeskoku przełącznika na 5 i konfigurację czasu przełącznika na 10 sekund :

```
Switch#configure
```

```
Switch(config)#service dhcp relay
```

```
Switch(config)#show ip dhcp relay
```

```
DHCP relay state: enabled
```

```
.....
```

```
Switch(config)#end
```

**Switch#copy running-config startup-config****2.2.2 (Opcjonalnie) Konfiguracja opcji 82**

Wykonaj poniższe kroki, aby skonfigurować opcję 82:

|        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Krok 1 | <b>configure</b><br>Uruchom tryb konfiguracji globalnej.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Krok 2 | <b>interface { fastEthernet <i>port</i>   range fastEthernet <i>port-list</i>   gigabitEthernet <i>port</i>   range gigabitEthernet <i>port-list</i>   ten-gigabitEthernet <i>port</i>   range ten-gigabitEthernet <i>port-list</i> }</b><br>Uruchom tryb konfiguracji interfejsu.                                                                                                                                                                                                                                                                                                                                    |
| Krok 3 | <b>ip dhcp relay information option</b><br>Włącz funkcję opcji 82 na porcie.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Krok 4 | <b>ip dhcp relay information strategy { keep   replace   drop }</b><br>Wybierz działanie dla pola opcji 82 pakietów żądania DHCP z hosta. Dostępne są poniższe działania.<br><br><i>keep</i> : Oznacza zachowanie pola opcji 82.<br><br><i>replace</i> : Oznacza zastąpienie pola opcji 82 polem wyznaczonym przez przełącznik. Domyślnie Circuit ID zdefiniowany jest jako VLAN i numer portu, który odbiera pakiety DHCP Request (żądanie DHCP). Remote ID to adres MAC urządzenia DHCP Snooping, które odbiera pakiety żądania DHCP.<br><br><i>drop</i> : Oznacza odrzucanie pakietów zawierających pole opcji 82. |
| Krok 5 | <b>ip dhcp relay information format { normal   private }</b><br>Wybierz format pola wartości podopcji opcji 82.<br><br><i>normal</i> : Oznacza zachowanie formatu TLV (ang. type-length-value, typ-długość-wartość).<br><br><i>private</i> : Oznacza, że format pola wartości podopcji zakłada podanie samej wartości.                                                                                                                                                                                                                                                                                                |
| Krok 6 | <b>ip dhcp relay information circuit-id <i>string</i></b><br>Skonfiguruj circuit ID. Ustawienia circuit ID przełącznika i serwera DHCP powinny być ze sobą kompatybilne.<br><br><i>string</i> : Wprowadź circuit ID, składający się z maks. 64 znaków.                                                                                                                                                                                                                                                                                                                                                                |
| Krok 7 | <b>ip dhcp relay information remote-id <i>string</i></b><br>Skonfiguruj remote ID. (zdalny ID). Ustawienia remote ID przełącznika i serwera DHCP powinny być ze sobą kompatybilne.<br><br><i>string</i> : Wprowadź remote ID, składający się z maks. 64 znaków.                                                                                                                                                                                                                                                                                                                                                       |
| Krok 8 | <b>show ip dhcp relay information interface { fastEthernet <i>port</i>   gigabitEthernet <i>port</i>   ten-gigabitEthernet <i>port</i>   port-channel <i>port-channel-id</i> }</b><br>Sprawdź konfigurację opcji 82 portu.                                                                                                                                                                                                                                                                                                                                                                                            |

---

Krok 9      **end**  
Powróć do trybu privileged EXEC.

---

Krok 10     **copy running-config startup-config**  
Zapisz ustawienia w pliku konfiguracyjnym.

---

Poniższy przykład prezentuje włączanie opcji 82 na porcie 1/0/7 i konfigurację strategii na replace (zastąp), formatu na normal, circuit-id jako VLAN 20 i remote-id jako Host1:

**Switch#configure**

**Switch(config)#interface gigabitEthernet 1/0/7**

**Switch(config-if)#ip dhcp relay information option**

**Switch(config-if)#ip dhcp relay information strategy replace**

**Switch(config-if)#ip dhcp relay information format normal**

**Switch(config-if)#ip dhcp relay information circuit-id VLAN20**

**Switch(config-if)#ip dhcp relay information remote-id Host1**

**Switch(config-if)#show ip dhcp relay information interface gigabitEthernet 1/0/7**

| Interface | Option 82 Status | Operation | Strategy | Format | Circuit ID | Remote ID | LAG   |
|-----------|------------------|-----------|----------|--------|------------|-----------|-------|
| -----     | -----            | -----     | -----    | -----  | -----      | -----     | ----- |
| Gi1/0/7   | Enable           | Replace   |          | Normal | VLAN20     | Host1     | N/A   |

**Switch(config-if)#end**

**Switch#copy running-config startup-config**

### 2.2.3 Konfiguracja DHCP VLAN Relay

Wykonaj poniższe kroki, aby skonfigurować DHCP VLAN Relay:

---

Krok 1      **configure**  
Uruchom tryb konfiguracji globalnej.

---

Krok 2      Wejść w tryb konfiguracji interfejsu VLAN.  
**interface vlan *vlan-id***  
*vlan-id*: Wyznacz interfejs VLAN. Obsługiwana jest jedynie VLAN 1 (VLAN zarządzający).

---

Krok 3      **ip dhcp relay default-interface**  
Ustaw interfejs management VLAN (VLAN zarządzający) jako domyślny interfejs agenta przekazywania.

---



|        |                                                                                                                                                                                                                                                               |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Krok 4 | <b>ip dhcp relay vlan <i>vid</i> helper-address <i>ip-address</i></b><br>Określ VLAN ID i serwer DHCP.<br><i>vid</i> : Wprowadź ID VLAN, w której hosty mogą dynamicznie pozyskiwać IP z serwera DHCP.<br><i>ip-address</i> : Wprowadź adres IP serwera DHCP. |
| Krok 5 | <b>exit</b><br>Wróć do trybu konfiguracji globalnej.                                                                                                                                                                                                          |
| Krok 6 | <b>show ip dhcp relay</b><br>Sprawdź ustawienia DHCP Relay.                                                                                                                                                                                                   |
| Krok 7 | <b>end</b><br>Powróć do trybu privileged EXEC.                                                                                                                                                                                                                |
| Krok 8 | <b>copy running-config startup-config</b><br>Zapisz ustawienia w pliku konfiguracyjnym.                                                                                                                                                                       |

Poniższy przykład prezentuje ustawianie interfejsu VLAN 1 (VLAN zarządzający) na domyślny interfejs agenta przekazywania i wyznaczenie serwera DHCP przez wpisanie adresu serwera jako 192.168.1.8 na VLAN 10:

```
Switch#configure
```

```
Switch(config)#interface vlan 1
```

```
Switch(config-if)# ip dhcp relay default-interface
```

```
Switch(config-if)#exit
```

```
Switch(config)#ip dhcp relay vlan 10 helper-address 192.168.1.8
```

```
Switch(config)#show ip dhcp relay
```

```
...
```

```
DHCP VLAN relay helper address is configured on the following vlan:
```

```
vlan Helper address
```

```
----- -
```

```
VLAN 10 192.168.1.8
```

```
Switch(config)#end
```

```
Switch#copy running-config startup-config
```

# 3 Konfiguracja DHCP L2 Relay

Aby przeprowadzić konfigurację DHCP L2 Relay, wykonaj poniższe kroki:

- 1) Włącz DHCP L2 Relay.
- 2) Skonfiguruj opcję 82 dla portów.

## 3.1 Przez GUI

### 3.1.1 Włączanie DHCP L2 Relay

Wybierz z menu **L3 FEATURES > DHCP Service > DHCP L2 Relay > Global Config**, aby wyświetlić poniższą stronę.

Rys. 3-1 Włączanie DHCP L2 Relay

Global Config

DHCP L2 Relay:  Enable Apply

VLAN Config

Filter by VLAN: From  To  Apply

| <input type="checkbox"/>            | VLAN | Status   |
|-------------------------------------|------|----------|
| <input checked="" type="checkbox"/> | 1    | Disabled |
| <input type="checkbox"/>            | 8    | Disabled |

Total: 2 1 entry selected. Cancel Apply

Wykonaj poniższe kroki, aby włączyć DHCP L2 Relay globalnie dla wybranej sieci VLAN:

- 1) W sekcji **Global Config** włącz globalnie DHCP L2 Relay. Kliknij **Apply**.

---

DHCP L2 Relay      Włącz DHCP Relay globalnie.

---

- 2) W sekcji **VLAN Config** włącz DHCP L2 Relay dla wybranej sieci VLAN. Kliknij **Apply**.

---

VLAN      Informuje o VLAN ID.

---



---

Status (Stan)      Włącz DHCP L2 Relay dla wybranej sieci VLAN.

---

### 3.1.1 Konfiguracja opcji 82 dla portów

Wybierz z menu **L3 FEATURES > DHCP Service > DHCP L2 Relay > Port Config**, aby wyświetlić następującą stronę.

Rys. 3-2 Konfiguracja opcji 82 dla portów

| Port Config                         |        |                   |                  |        |                         |            |                        |           |       |
|-------------------------------------|--------|-------------------|------------------|--------|-------------------------|------------|------------------------|-----------|-------|
| UNIT1                               |        | LAGS              |                  |        |                         |            |                        |           |       |
| <input type="checkbox"/>            | Port   | Option 82 Support | Option 82 Policy | Format | Circuit ID Customizaton | Circuit ID | Remote ID Customizaton | Remote ID | LAG   |
| <input checked="" type="checkbox"/> | 1/0/1  | Disabled          | Keep             | Normal | Disabled                |            | Disabled               |           | ---   |
| <input type="checkbox"/>            | 1/0/2  | Disabled          | Keep             | Normal | Disabled                |            | Disabled               |           | ---   |
| <input type="checkbox"/>            | 1/0/3  | Disabled          | Keep             | Normal | Disabled                |            | Disabled               |           | ---   |
| <input type="checkbox"/>            | 1/0/4  | Disabled          | Keep             | Normal | Disabled                |            | Disabled               |           | ---   |
| <input type="checkbox"/>            | 1/0/5  | Disabled          | Keep             | Normal | Disabled                |            | Disabled               |           | ---   |
| <input type="checkbox"/>            | 1/0/6  | Disabled          | Keep             | Normal | Disabled                |            | Disabled               |           | ---   |
| <input type="checkbox"/>            | 1/0/7  | Disabled          | Keep             | Normal | Disabled                |            | Disabled               |           | ---   |
| <input type="checkbox"/>            | 1/0/8  | Disabled          | Keep             | Normal | Disabled                |            | Disabled               |           | ---   |
| <input type="checkbox"/>            | 1/0/9  | Disabled          | Keep             | Normal | Disabled                |            | Disabled               |           | ---   |
| <input type="checkbox"/>            | 1/0/10 | Disabled          | Keep             | Normal | Disabled                |            | Disabled               |           | ---   |
| Total: 10                           |        |                   |                  |        | 1 entry selected.       |            |                        | Cancel    | Apply |

Wykonaj poniższe kroki, aby włączyć DHCP Relay i skonfigurować opcję 82:

1) Wybierz co najmniej jeden port, aby skonfigurować na nim opcję 82.

**Option 82 Support** Zaznacz, czy chcesz włączyć opcję 82. Opcja jest domyślnie wyłączona. Opcja 82 wykorzystywana jest do zapisu lokalizacji DHCP klienta, portu Ethernet, VLAN itd. Jeżeli chcesz zapisać aktualną lokalizację klienta, możesz włączyć opcję 82 na urządzeniu przekaźnikowym, znajdującym się najbliższej niego.

**Option 82 Policy** Wybierz działanie dla pola opcji 82 pakietów żądania DHCP.

**Keep (zachowaj):** Oznacza zachowanie pola opcji 82.

**Replace (zastąp):** Oznacza zastąpienie pola opcji 82 polem wyznaczonym przez przełącznik. Domyślnie Circuit ID zdefiniowany jest jako VLAN i ID portu, który odbiera pakiety DHCP Request (żądanie DHCP). Remote ID to adres MAC urządzenia DHCP Relay, które odbiera pakiety żądania DHCP.

**Drop (odrzuć):** Oznacza odrzucanie pakietów zawierających pole opcji 82.

**Format** Wybierz format pola wartości podopcji opcji 82.

**Normal:** Oznacza zachowanie formatu TLV (ang. type-length-value, typ-długość-wartość).

**Private:** Oznacza, że format pola wartości podopcji zakłada podanie samej wartości.

|                          |                                                                                                                                                                                                                                                                                        |
|--------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Circuit ID Customization | Włącz lub wyłącz Customization of Option 82 (dostosowywanie opcji 82). Jeżeli funkcja jest włączona, należy skonfigurować dane opcji 82 ręcznie. Jeżeli funkcja jest wyłączona, przełącznik automatycznie skonfiguruje VLAN ID i ID portu, który odbiera pakiety DHCP jako circuit ID. |
| Circuit ID               | Wprowadź zindywidualizowany circuit ID, składający się z maks. 64 znaków. Ustawienia circuit ID przełącznika i serwera DHCP powinny być ze sobą kompatybilne.                                                                                                                          |
| Remote ID Customization  | Włącz lub wyłącz przełącznik w celu zdefiniowania pola Remote ID – podopcji opcji 82. Jeżeli jest włączone, możesz ręcznie skonfigurować zdalny ID. Jeżeli jest wyłączone, przełącznik automatycznie skonfiguruje adres MAC przełącznika jako zdalny ID.                               |
| Remote ID                | Wprowadź zindywidualizowany zdalny ID, składający się z maks. 64 znaków. Ustawienia zdalnego ID przełącznika i serwera DHCP powinny być ze sobą kompatybilne.                                                                                                                          |

2) Kliknij **Apply**

## 3.2 Przez CLI

### 3.2.1 Włączanie DHCP L2 Relay

Wykonaj poniższe kroki, aby włączyć DHCP L2 Relay:

|        |                                                                                                                                                                              |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Krok 1 | <b>configure</b><br>Uruchom tryb konfiguracji globalnej.                                                                                                                     |
| Krok 2 | <b>ip dhcp l2relay</b><br>Włącz DHCP L2 Relay.                                                                                                                               |
| Krok 3 | <b>ip dhcp l2relay vlan <i>vlan-list</i></b><br>Włącz DHCP L2 Relay dla wybranych sieci VLAN.<br><i>vlan-list</i> : Wyznacz VLAN, który będzie włączany przez DHCP L2 relay. |
| Krok 5 | <b>show ip dhcp l2relay</b><br>Sprawdź konfigurację DHCP Relay.                                                                                                              |
| Krok 6 | <b>end</b><br>Powróć do trybu privileged EXEC.                                                                                                                               |
| Krok 7 | <b>copy running-config startup-config</b><br>Zapisz ustawienia w pliku konfiguracyjnym.                                                                                      |

Następujący przykład prezentuje włączanie DHCP L2 Relay globalnie i dla VLAN 2:

**Switch#configure**

```
Switch(config)#ip dhcp l2relay
```

```
Switch(config)#ip dhcp l2relay vlan 2
```

```
Switch(config)#show ip dhcp l2relay
```

```
Global Status: Enable
```

```
VLAN ID: 2
```

```
Switch(config)#end
```

```
Switch#copy running-config startup-config
```

### 3.2.2 Konfiguracja opcji 82 dla portów

Wykonaj poniższe kroki, aby skonfigurować opcję 82:

|        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Krok 1 | <b>configure</b><br>Uruchom tryb konfiguracji globalnej.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Krok 2 | <b>interface { fastEthernet <i>port</i>   range fastEthernet <i>port-list</i>   gigabitEthernet <i>port</i>   range gigabitEthernet <i>port-list</i>   ten-gigabitEthernet <i>port</i>   range ten-gigabitEthernet <i>port-list</i> }</b><br>Uruchom tryb konfiguracji interfejsu.                                                                                                                                                                                                                                                                                                              |
| Krok 3 | <b>ip dhcp l2relay information option</b><br>Włącz funkcję opcji 82 na porcie.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Krok 4 | <b>ip dhcp l2relay information strategy { keep   replace   drop }</b><br>Wybierz działanie dla pola opcji 82 pakietów żądania DHCP z hosta. Dostępne są poniższe działania.<br><br>keep: Oznacza zachowanie pola opcji 82.<br><br>replace: Oznacza zastąpienie pola opcji 82 polem wyznaczonym przez przełącznik. Domyślnie Circuit ID zdefiniowany jest jako VLAN i numer portu, który odbiera pakiety DHCP Request (żądanie DHCP). Remote ID to adres MAC urządzenia DHCP Snooping, które odbiera pakiety żądania DHCP.<br><br>drop: Oznacza odrzucanie pakietów zawierających pole opcji 82. |
| Krok 5 | <b>ip dhcp l2relay information format { normal   private }</b><br>Wybierz format pola wartości podopcji opcji 82.<br><br>normal: Oznacza zachowanie formatu TLV (ang. type-length-value, typ-długość-wartość).<br><br>private: Oznacza, że format pola wartości podopcji zakłada podanie samej wartości.                                                                                                                                                                                                                                                                                        |
| Krok 6 | <b>ip dhcp l2relay information circuit-id <i>string</i></b><br>Skonfiguruj circuit ID. Ustawienia circuit ID przełącznika i serwera DHCP powinny być ze sobą kompatybilne.<br><br><i>string</i> : Wprowadź circuit ID, składający się z maks. 64 znaków.                                                                                                                                                                                                                                                                                                                                        |

|         |                                                                                                                                                                                                                                                                   |
|---------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Krok 7  | <b>ip dhcp l2relay information remote-id <i>string</i></b><br>Skonfiguruj remote ID. (zdalny ID). Ustawienia remote ID przełącznika i serwera DHCP powinny być ze sobą kompatybilne.<br><br><i>string</i> : Wprowadź remote ID, składający się z maks. 64 znaków. |
| Krok 8  | <b>show ip dhcp l2relay information interface { fastEthernet <i>port</i>   gigabitEthernet <i>port</i>   port-channel <i>port-channel-id</i> }</b><br>Sprawdź konfigurację opcji 82 portu.                                                                        |
| Krok 9  | <b>end</b><br>Powróć do trybu privileged EXEC.                                                                                                                                                                                                                    |
| Krok 10 | <b>copy running-config startup-config</b><br>Zapisz ustawienia w pliku konfiguracyjnym.                                                                                                                                                                           |

Poniższy przykład prezentuje włączanie opcji 82 na porcie 1/0/7 i konfigurację strategii na replace (zastęp), formatu na normal, circuit-id na VLAN20 i remote-id na Host1:

### Switch#configure

```
Switch(config)#interface gigabitEthernet 1/0/7
```

```
Switch(config-if)#ip dhcp l2relay information option
```

```
Switch(config-if)#ip dhcp l2relay information strategy replace
```

```
Switch(config-if)#ip dhcp l2relay information format normal
```

```
Switch(config-if)#ip dhcp l2relay information circuit-id VLAN20
```

```
Switch(config-if)#ip dhcp l2relay information remote-id Host1
```

```
Switch(config-if)#show ip dhcp l2relay information interface gigabitEthernet 1/0/7
```

| Interface | Option 82 Status | Operation | Strategy | Format | Circuit ID | Remote ID | LAG   |
|-----------|------------------|-----------|----------|--------|------------|-----------|-------|
| -----     | -----            | -----     | -----    | -----  | -----      | -----     | ----- |
| Gi1/0/7   | Enable           | Replace   |          | Normal | VLAN20     | Host1     | N/A   |

```
Switch(config-if)#end
```

```
Switch#copy running-config startup-config
```

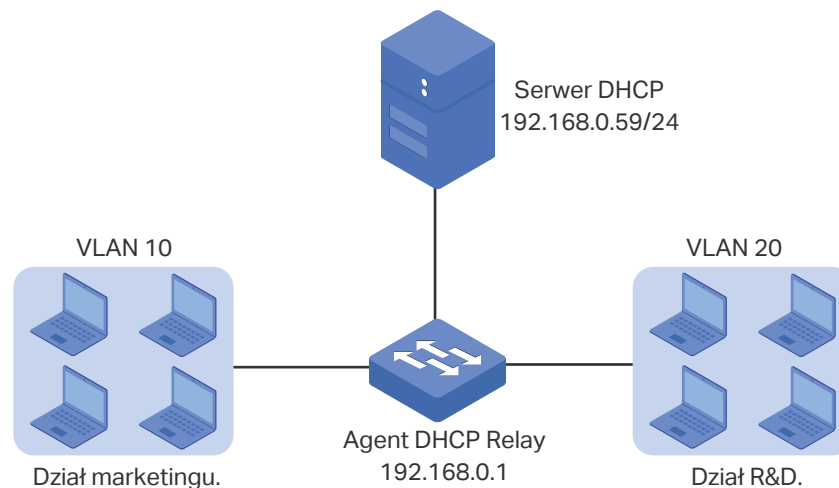
# 4 Przykład wdrożenia DHCP VLAN Relay

## 4.1 Wymagania sieciowe

Dział marketingu i dział R&D należą odpowiednio do dwóch VLAN-ów. W żadnym z tych VLAN-ów nie ma bram sieciowych warstwy 3. Administrator umieszcza jeden serwer DHCP w sieci i chce, aby przydzielał on adresy IP tym dwóm działom.

Jak pokazano na poniższym schemacie topologii sieci, dział marketingu i dział R&D należą odpowiednio do VLAN 10 i VLAN 20. Dział marketingu jest podłączony do portu 1/0/1 agenta relay, a dział R&D podłączony jest do portu 1/0/2 agenta relay.

Rys. 4-1 Topologia sieci dla DHCP VLAN Relay



## 4.2 Schemat konfiguracji

W omawianej sytuacji serwer DHCP i komputery są izolowane poprzez VLAN-y, dlatego żądanie DHCP od klienta nie może być przesyłane bezpośrednio do serwera DHCP. Biorąc pod uwagę, że żaden z VLAN-ów nie ma bramy sieciowej warstwy 3, zaleca się skonfigurować funkcję DHCP VLAN Relay, aby spełnić opisany wyżej warunek.

Konfiguracja wymaga wykonania następujących kroków:

- 1) Utwórz jedną pulę adresów IP DHCP na serwerze DHCP, który jest w segmencie 192.168.0.0/24 sieci.
- 2) Skonfiguruj 802.1Q VLAN na agencie DHCP relay. Dodaj wszystkie komputery z działu marketingu do VLAN 10 i dodaj wszystkie komputery z działu R&D do VLAN 20.
- 3) Skonfiguruj DHCP VLAN Relay na agencie DHCP relay. Włącz globalnie DHCP Relay, wybierz interfejs 1 VLAN-u (domyślny interfejs zarządzania VLAN-u) jako interfejs domyślny agenta relay i ustaw adres serwera DHCP dla VLAN 10 i VLAN 20.

W poniższym przykładzie konfiguracji serwer DHCP reprezentuje przełącznik T1500G-10PS, a agenta DHCP relay przełącznik T2500G-10TS. W poniższych podrozdziałach opisano dwa sposoby przeprowadzenia procedury konfiguracji: przez GUI oraz przez CLI.

## 4.3 Przez GUI

### ■ Konfiguracja serwera DHCP

- 1) Wybierz z menu **L3 FEATURES > DHCP Service > DHCP Server > DHCP Server**, aby wyświetlić poniższą stronę. W sekcji **Global Config** włącz globalnie serwer DHCP.

Rys. 4-2 Konfiguracja serwera DHCP

Global Config

DHCP Server:  Enable

Option 60:  (Optional. 1-64 characters)

Option 138:  (Optional. Format: 192.168.0.1)

Apply

- 2) Wybierz z menu **L3 FEATURES > DHCP Service > DHCP Server > Pool Setting** i kliknij **+ Add**, aby wyświetlić poniższą stronę. Utwórz pulę DHCP dla klientów. Skonfiguruj odpowiednie parametry, tak jak na poniższym obrazku.

Rys. 4-3 Konfiguracja DHCP Pool 1 dla VLAN 10

DHCP Server Pool

Pool Name:  (8 characters maximum)

Network Address:  (Format: 192.168.0.0)

Subnet Mask:  (Format: 255.255.255.0)

Lease Time:  (Optional. 1-2880 min, Default: 120)

▶ Default Gateway:  (Optional. Format: 192.168.0.1)

▶ DNS Server:  (Optional. Format: 192.168.0.1)

▶ NetBIOS Server:  (Optional. Format: 192.168.0.1)

NetBIOS Node Type:  (Optional, b/p/m/h/none)

Next Server Address:  (Optional. Format: 192.168.0.1)

Domain Name:  (0 to 200 characters)

Bootfile:  (0 to 128 characters)

Cancel Create

### ■ Konfiguracja VLAN-ów na agencie relay

- 3) Wybierz z menu **L2 FEATURES > VLAN > 802.1Q VLAN > VLAN Config** i kliknij **+ Add** aby wyświetlić poniższą stronę. Utwórz VLAN 10 i VLAN 20 odpowiednio dla działu marketingu i działu R&D. Dodaj port 1/0/1 do VLAN 10 i port 1/0/2 do VLAN 20.



Rys. 4-4 Tworzenie VLAN 10

### VLAN Config

VLAN ID:  (2-4094, format: 2,4-5,8)

VLAN Name:  (1-16 characters)

#### Untagged Ports

Port:  (Format: 1/0/1, input or choose below)

Select All

**UNIT1**      **LAGS**

1    2    3    4    5    6    7    8    9    10

Selected    Unselected    Not Available

#### Tagged Ports

Port:  (Format: 1/0/1, input or choose below)

Select All

**UNIT1**      **LAGS**

1    2    3    4    5    6    7    8    9    10

Rys. 4-5 Tworzenie VLAN 20

### VLAN Config

VLAN ID:  (2-4094, format: 2,4-5,8)

VLAN Name:  (1-16 characters)

---

Untagged Ports

Port:  (Format: 1/0/1, input or choose below)

UNIT1

1

2

3

4

5

LAGS

6

7

8

9

10

Select All

Selected

Unselected

Not Available

---

Tagged Ports

Port:  (Format: 1/0/1, input or choose below)

UNIT1

1

2

3

4

5

LAGS

6

7

8

9

10

Select All

Cancel

Create

- Konfiguracja DHCP VLAN Relay na agencie relay

- 1) Wybierz z menu **L3 FEATURES > DHCP Service > DHCP Relay > DHCP Relay Config**, aby wyświetlić poniższą stronę. W sekcji **Global Config** włącz DHCP Relay i kliknij **Apply**.

Rys. 4-6 Włącz DHCP Relay

Global Config

---

DHCP Relay:  Enable

DHCP Relay Hops:  (1-16)

DHCP Relay Time Threshold:  seconds (0-65535)

Apply

- 2) Wybierz z menu **L3 FEATURES > DHCP Service > DHCP Relay > DHCP VLAN Relay**, aby wyświetlić poniższą stronę. W sekcji **Default Relay Agent Interface** wybierz interfejs 1 VLAN-u (domyślny interfejs zarządzania VLAN-u) jako interfejs domyślny agenta relay.

Rys. 4-7 Wybieranie domyślnego interfejsu agenta relay

Default Relay Agent Interface

Interface ID:   (1-4094)

IP Address: 192.168.0.1

- 3) Wybierz z menu **L3 FEATURES > DHCP Service > DHCP Relay > DHCP VLAN Relay** i kliknij **+ Add**, aby wyświetlić poniższą stronę. Ustaw adres serwera DHCP dla klientów w sieci VLAN 10 i VLAN 20.

Rys. 4-8 Wybieranie serwera DHCP dla interfejsu VLAN 10

DHCP VLAN Relay

VLAN ID:  (1-4094)

Server Address:  (Format: 192.168.0.1)

Rys. 4-9 Wybieranie serwera DHCP dla interfejsu VLAN 20

DHCP VLAN Relay

VLAN ID:  (1-4094)

Server Address:  (Format: 192.168.0.1)

- 4) Kliknij , aby zapisać ustawienia.

## 4.4 Przez CLI

### ■ Konfiguracja serwera DHCP

- 1) Włącz globalnie usługę DHCP.

```
Switch#configure
```

```
Switch(config)#service dhcp server
```

- 2) Utwórz pulę DHCP i nazwij ją "pool", następnie ustaw jej adres sieciowy jako 192.168.0.0, maskę podsieci jako 255.255.255.0, czas przydziału jako 120 minut, bramę domyślną jako 192.168.0.1.

```
Switch(config)#ip dhcp server pool pool
Switch(dhcp-config)#network 192.168.0.0 255.255.255.0
Switch(dhcp-config)#lease 120
Switch(dhcp-config)#default-gateway 192.168.0.1
Switch(dhcp-config)#dns-server 192.168.0.2
Switch(dhcp-config)#end
Switch#copy running-config startup-config
```

- Konfiguracja VLAN-u na agencie relay

```
Switch#configure
Switch(config)# vlan 10
Switch(config-vlan)#name Marketing
Switch(config-vlan)#exit
Switch(config)#interface gigabitEthernet 1/0/1
Switch(config-if)#switchport general allowed vlan 10 untagged
Switch(config-if)#exit
Switch(config)# vlan 20
Switch(config-vlan)#name RD
Switch(config-vlan)#exit
Switch(config)#interface gigabitEthernet 1/0/2
Switch(config-if)#switchport general allowed vlan 20 untagged
Switch(config-if)#exit
```

- Konfiguracja DHCP VLAN Relay na agencie relay

- 1) Włącz DHCP Relay.

```
Switch(config)#service dhcp relay
```

- 2) Wybierz routowany port 1/0/5 jako domyślny interfejs agenta relay.

```
Switch(config)#interface vlan 1
Switch(config-if)#ip dhcp relay default-interface
Switch(config-if)#exit
```

- 3) Wybierz serwer DHCP dla VLAN 10 i VLAN 20

```
Switch(config)#ip dhcp relay vlan 10 helper-address 192.168.0.59
```

```
Switch(config)#ip dhcp relay vlan 20 helper-address 192.168.0.59
Switch(config)#exit
```

### **Sprawdzanie konfiguracji agenta DHCP Relay**

```
Switch#show ip dhcp relay
```

```
Switch#show ip dhcp relay
```

```
DHCP relay state: enabled
```

```
...
```

```
DHCP relay default relay agent interface:
```

```
Interface: VLAN 1
```

```
IP address: 192.168.0.1
```

```
DHCP vlan relay helper address is configured on the following vlan:
```

| vlan    | Helper address |
|---------|----------------|
| -----   |                |
| VLAN 10 | 192.168.0.59   |
| VLAN 20 | 192.168.0.59   |

# Część 18

## Konfiguracja QoS

### ROZDZIAŁY

1. QoS
2. Konfiguracja usług Class of Service
3. Konfiguracja kontroli przepustowości
4. Konfiguracja Voice VLAN
5. Konfiguracja Auto VoIP
6. Przykłady konfiguracji

# 1 QoS

## 1.1 Informacje ogólne

Wraz z rozbudową sieci i rozwojem aplikacji zwiększa się także znacząco ruch internetowy, co skutkuje przeciążeniami sieci, odrzucaniem pakietów i dużymi opóźnieniami w transmisji. Sieci traktują zwykle każdy ruch jednakowo, na zasadzie FIFO (First In First Out), ale obecnie wiele aplikacji specjalnych, takich jak VoD, wideokonferencje, VoIP, itp, wymaga większej przepustowości lub mniejszych opóźnień w transmisji, aby wydajność tych usług była zadowalająca.

Technologia QoS (Quality of Service) umożliwia klasyfikowanie i nadawanie priorytetów ruchowi w sieci, aby systematyzować ruch zgodnie z wymaganiami użytkowanych usług.

## 1.2 Obsługiwane funkcje

Aby zwiększyć wydajność sieci i zapewnić lepsze wykorzystanie przepustowości, skonfiguruj funkcję class of service, kontroli przepustowości, Voice VLAN oraz Auto VoIP.

### Class of Service

Przełącznik klasyfikuje pakiety przychodzące, mapuje pakiety do kolejek o innym priorytecie, a następnie przesyła pakiety zgodnie z określonymi ustawieniami harmonogramu w celu wdrożenia funkcji QoS.

- Tryb Priority: obsługa trzech trybów - Port Priority, 802.1p Priority oraz DSCP Priority.
- Tryb Scheduler: obsługa dwóch typów - Strict oraz Weighted.

### Bandwidth Control

Funkcja kontroli przepustowości pomaga kontrolować natężenie oraz próg ruchu na każdym porcie w celu zapewnienia wydajnej pracy sieci.

- Funkcja Rate limit umożliwia ograniczanie ruchu przychodzącego/wychodzącego na każdym porcie. W ten sposób przepustowość sieci można efektywniej dzielić i użytkować.
- Funkcja Storm Control pozwala przełącznikowi na monitorowanie pakietów broadcast, pakietów multicast oraz ramek UL (Unknown unicast frames) w sieci. Jeśli poziom transmisji pakietów przekracza ustawiony limit, pakiety są automatycznie odrzucane w celu eliminacji ryzyka burzy broadcastowej.

### Voice VLAN i Auto VoIP

Funkcje Voice VLAN oraz Auto VoIP służą do priorytetyzacji ruchu związanego z transmisją głosu. Ruch głosowy jest zwykle bardziej podatny na zakłócenia niż ruch danych, dlatego

jakość głosu może ulegać znacznemu obniżeniu w przypadku utraty lub opóźnień pakietów. W celu zachowania wysokiej jakości głosu, skonfiguruj funkcję Voice VLAN lub Auto VoIP.

Te dwie funkcje mogą być skonfigurowane na porcie, który pośredniczy wyłącznie w ruchu głosowym lub zarówno głosowym, jak i w ruchu danych. Włączenie Voice VLAN umożliwia zmianę priorytetu 802.1p pakietów głosowych i przesyłanie ich do wybranego VLAN-u. Natomiast funkcja Auto VoIP w połączeniu z funkcją LLDP-MED umożliwia informowanie urządzeń głosowych o wysłaniu skonfigurowanych w określony sposób pakietów.



## 2 Konfiguracja usług Class of Service

Konfigurując usługi class of service możesz:

- skonfigurować priorytetyzację portu;
- skonfigurować priorytetyzację 802.1p;
- skonfigurować priorytetyzację DSCP;
- dostosować ustawienia harmonogramu.

### Wskazówki dotyczące konfiguracji

- Wybierz tryb priorytetyzacji, któremu porty ufają, zgodnie z wymaganiami sieci.

Port może korzystać tylko z jednego trybu priorytetyzacji do klasyfikacji pakietów przychodzących. Przełącznik obsługuje trzy tryby priorytetyzacji: priorytetyzacja portu, priorytetyzacja 802.1P i priorytetyzacja DSCP.

- Priorytetyzacja portu

W tym trybie przełącznik przydziela pakietom priorytety, zgodnie z ich portami odbierającymi, bez względu na pole lub typ pakietu.

- Priorytetyzacja 802.1P

Standard 802.1P określa pierwsze 3 bity tagu 802.1Q poprzez pole PRI. Wartości PRI wahają się od 0 do 7. Priorytetyzacja 802.1P przydziela pakietom priorytet w oparciu o wartość PRI.

W tym trybie przełącznik przydziela priorytety tylko pakietom z tagiem VLAN, bez względu na nagłówek IP pakietów.

- Priorytetyzacja DSCP

Priorytetyzacja DSCP ustala priorytety pakietów w oparciu o pole ToS (Type of Service) w nagłówku IP. RFC2474 określa pole ToS w nagłówku IP pakietu poprzez pole DS. Pierwsze sześć bitów (bit 0 - bit 5) pola DS stanowi priorytet DSCP. Wartości DSCP wahają się od 0 do 63.

W tym trybie przełącznik przydziela priorytety tylko pakietom IP.

- Określ mapowanie 802.1p do kolejek, zgodnie ze swoimi wymaganiami.

W wypadku priorytetyzacji 802.1p pakiety będą przesyłane bezpośrednio, zgodnie z mapowaniem 802.1p do kolejek.

W wypadku priorytetyzacji portu i priorytetyzacji DSCP, będą one w pierwszej kolejności mapowane do priorytetu 802.1p, a następnie mapowane zgodnie z mapowaniem 802.1p do kolejek.

## 2.1 Przez GUI

### 2.1.1 Konfiguracja priorytetyzacji portów

- Konfiguracja Trust Mode i Port to 802.1p Mapping

Wybierz z menu **QoS > Class of Service > Port Priority**, aby wyświetlić poniższą stronę.

Rys. 2-1 Konfiguracja Trust Mode i Port to 802.1p Mapping

| Port Priority Config                |        |                 |            |     |
|-------------------------------------|--------|-----------------|------------|-----|
| UNIT1                               |        | LAGS            |            |     |
| <input type="checkbox"/>            | Port   | 802.1p Priority | Trust Mode | LAG |
| <input checked="" type="checkbox"/> | 1/0/1  | 0               | Untrusted  | --  |
| <input type="checkbox"/>            | 1/0/2  | 0               | Untrusted  | --  |
| <input type="checkbox"/>            | 1/0/3  | 0               | Untrusted  | --  |
| <input type="checkbox"/>            | 1/0/4  | 0               | Untrusted  | --  |
| <input type="checkbox"/>            | 1/0/5  | 0               | Untrusted  | --  |
| <input type="checkbox"/>            | 1/0/6  | 0               | Untrusted  | --  |
| <input type="checkbox"/>            | 1/0/7  | 0               | Untrusted  | --  |
| <input type="checkbox"/>            | 1/0/8  | 0               | Untrusted  | --  |
| <input type="checkbox"/>            | 1/0/9  | 0               | Untrusted  | --  |
| <input type="checkbox"/>            | 1/0/10 | 0               | Untrusted  | --  |

Total: 10      1 entry selected.      Cancel Apply

Wykonaj poniższe kroki, aby skonfigurować parametry priorytetyzacji portów:

1) Wybierz porty, dostosuj priorytetyzację 802.1p i ustaw trust mode jako Untrusted.

|                 |                                                                                                                                                                                                                                                                                                                                                                                                      |
|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 802.1p Priority | Wybierz dla portu mapowanie portu do priorytetu 802.1p. Pakiety przychodzące są w pierwszej kolejności mapowane do priorytetu 802.1p na podstawie mapowania portu do 802.1p, następnie do kolejek TC w oparciu o mapowanie 802.1p do kolejek. Pakiety nietagowane z jednego portu będą mieć przydzieloną wartość priorytetu 802.1p, zgodnie z mapowaniem priorytetyzacji portu do priorytetu 802.1p. |
|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

|            |                                                                                                                     |
|------------|---------------------------------------------------------------------------------------------------------------------|
| Trust Mode | Ustaw ten tryb jako Untrusted. W tym trybie pakiety będą przetwarzane zgodnie z konfiguracją priorytetyzacji portu. |
|------------|---------------------------------------------------------------------------------------------------------------------|

2) Kliknij **Apply**.

- Konfiguracja mapowania 802.1p do kolejek

Wybierz z menu **QoS > Class of Service > 802.1p Priority**, aby wyświetlić poniższą stronę.

Rys. 2-2 Konfiguracja mapowania 802.1p do kolejek

#### 802.1p to Queue Mapping

| 802.1p Priority | Queue                             |
|-----------------|-----------------------------------|
| 0:              | <input type="text" value="TC-1"/> |
| 1:              | <input type="text" value="TC-0"/> |
| 2:              | <input type="text" value="TC-2"/> |
| 3:              | <input type="text" value="TC-3"/> |
| 4:              | <input type="text" value="TC-4"/> |
| 5:              | <input type="text" value="TC-5"/> |
| 6:              | <input type="text" value="TC-6"/> |
| 7:              | <input type="text" value="TC-7"/> |

[Apply](#)

#### 802.1p Remap

| 802.1p Priority | Remap                          |
|-----------------|--------------------------------|
| 0:              | <input type="text" value="0"/> |
| 1:              | <input type="text" value="1"/> |
| 2:              | <input type="text" value="2"/> |
| 3:              | <input type="text" value="3"/> |
| 4:              | <input type="text" value="4"/> |
| 5:              | <input type="text" value="5"/> |
| 6:              | <input type="text" value="6"/> |
| 7:              | <input type="text" value="7"/> |

[Apply](#)

W sekcji **802.1p to Queue Mapping** skonfiguruj mapowania i kliknij **Apply**.

|                        |                                                                                                                               |
|------------------------|-------------------------------------------------------------------------------------------------------------------------------|
| <b>802.1p Priority</b> | Wartość priorytetu 802.1p. W przypadku usługi QoS, priorytetyzacja 802.1p jest częścią usługi class of service.               |
| <b>Queue</b>           | Wybierz kolejkę TC dla wybranego priorytetu 802.1p. Pakiety z tym priorytetem 802.1p będą umieszczane w odpowiedniej kolejce. |

## 2.1.2 Konfiguracja priorytetyzacji 802.1p

### ■ Konfiguracja Trust Mode

Wybierz z menu **QoS > Class of Service > Port Priority**, aby wyświetlić poniższą stronę.

Rys. 2-3 Konfiguracja Trust Mode

Port Priority Config

---

UNIT1

LAGS

| <input type="checkbox"/>            | Port   | 802.1p Priority | Trust Mode | LAG |
|-------------------------------------|--------|-----------------|------------|-----|
| <input checked="" type="checkbox"/> | 1/0/1  | 0               | Untrusted  | --  |
| <input type="checkbox"/>            | 1/0/2  | 0               | Untrusted  | --  |
| <input type="checkbox"/>            | 1/0/3  | 0               | Untrusted  | --  |
| <input type="checkbox"/>            | 1/0/4  | 0               | Untrusted  | --  |
| <input type="checkbox"/>            | 1/0/5  | 0               | Untrusted  | --  |
| <input type="checkbox"/>            | 1/0/6  | 0               | Untrusted  | --  |
| <input type="checkbox"/>            | 1/0/7  | 0               | Untrusted  | --  |
| <input type="checkbox"/>            | 1/0/8  | 0               | Untrusted  | --  |
| <input type="checkbox"/>            | 1/0/9  | 0               | Untrusted  | --  |
| <input type="checkbox"/>            | 1/0/10 | 0               | Untrusted  | --  |

Total: 10
1 entry selected.

Cancel
Apply

Wykonaj poniższe kroki, aby skonfigurować trust mode:

- 1) Wybierz porty i ustaw trust mode jako Trust 802.1p.

#### Trust Mode

Ustaw ten tryb jako Trust 802.1p. W tym trybie pakiety tagowane będą przetwarzane zgodnie z konfiguracją priorytetyzacji 802.1p, a pakiety nietagowane zgodnie z konfiguracją priorytetyzacji portu.

- 2) Kliknij **Apply**.

- Konfiguracja mapowania 802.1p do kolejek i remapowania 802.1p

Wybierz z menu **QoS > Class of Service > 802.1p Priority**, aby wyświetlić poniższą stronę.

Rys. 2-4 Konfiguracja mapowania 802.1p do kolejek i remapowania 802.1p

#### 802.1p to Queue Mapping

| 802.1p Priority | Queue |
|-----------------|-------|
| 0:              | TC-1  |
| 1:              | TC-0  |
| 2:              | TC-2  |
| 3:              | TC-3  |
| 4:              | TC-4  |
| 5:              | TC-5  |
| 6:              | TC-6  |
| 7:              | TC-7  |

Apply

#### 802.1p Remap

| 802.1p Priority | Remap |
|-----------------|-------|
| 0:              | 0     |
| 1:              | 1     |
| 2:              | 2     |
| 3:              | 3     |
| 4:              | 4     |
| 5:              | 5     |
| 6:              | 6     |
| 7:              | 7     |

Apply

Wykonaj poniższe kroki, aby skonfigurować parametry priorytetyzacji 802.1p:

1) W sekcji **802.1p to Queue Mapping** skonfiguruj mapowania i kliknij **Apply**.

|                        |                                                                                                                                                                                                                                                                                                                                                 |
|------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>802.1p Priority</b> | Wartość priorytetu 802.1p. W przypadku usługi QoS, priorytetyzacja 802.1p jest częścią usługi class of service. Standard IEEE 802.1P określa pierwsze 3 bity tagu 802.1Q poprzez pole PRI. Wartości PRI są określane priorytetem 802.1p i wykorzystywane do określania priorytetu pakietów warstwy 2. Ta funkcja wymaga pakietów z tagiem VLAN. |
|------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

|              |                                                                                                                               |
|--------------|-------------------------------------------------------------------------------------------------------------------------------|
| <b>Queue</b> | Wybierz kolejkę TC dla wybranego priorytetu 802.1p. Pakiety z tym priorytetem 802.1p będą umieszczane w odpowiedniej kolejce. |
|--------------|-------------------------------------------------------------------------------------------------------------------------------|

2) (Opcjonalnie) W sekcji **802.1p Remap** skonfiguruj 802.1p na mapowania 802.1p i kliknij **Apply**.

**802.1p Priority** Wartość priorytetu 802.1p. W przypadku usługi QoS, priorytetyzacja 802.1p jest częścią usługi class of service. Standard IEEE 802.1P określa pierwsze 3 bity tagu 802.1Q poprzez pole PRI. Wartości PRI są określane priorytetem 802.1p i wykorzystywane do określania priorytetu pakietów warstwy 2. Ta funkcja wymaga pakietów z tagiem VLAN.

**Remap** Wybierz priorytety 802.1p, do których oryginalne priorytety 802.1p będą remapowane. Remapowanie 802.1p służy modyfikacji priorytetów 802.1p pakietów przychodzących. Gdy przełącznik wykryje pakiety z żądanymi priorytetami 802.1p, zmieni wartość priorytetów 802.1p zgodnie z mapą.

### Uwaga:

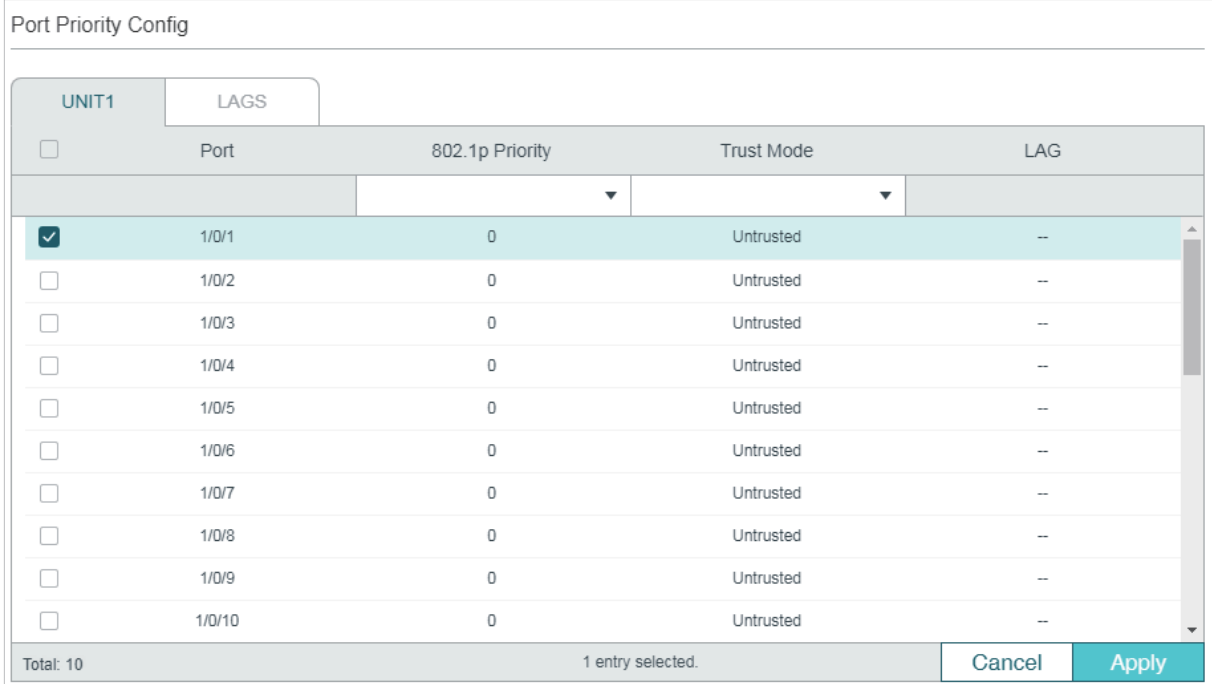
W trybie Trust 802.1p pakietom nietagowanym zostanie przydzielony priorytet 802.1p w oparciu o mapowanie portu do 802.1p i zostaną one przesłane zgodnie z mapowaniem 802.1p do kolejek.

## 2.1.3 Konfiguracja priorytetyzacji DSCP

### ■ Konfiguracja Trust Mode

Wybierz z menu **QoS > Class of Service > Port Priority**, aby wyświetlić poniższą stronę.

Rys. 2-5 Konfiguracja Trust Mode



Port Priority Config

| UNIT1                               | LAGS | Port   | 802.1p Priority | Trust Mode | LAG |
|-------------------------------------|------|--------|-----------------|------------|-----|
| <input checked="" type="checkbox"/> |      | 1/0/1  | 0               | Untrusted  | --  |
| <input type="checkbox"/>            |      | 1/0/2  | 0               | Untrusted  | --  |
| <input type="checkbox"/>            |      | 1/0/3  | 0               | Untrusted  | --  |
| <input type="checkbox"/>            |      | 1/0/4  | 0               | Untrusted  | --  |
| <input type="checkbox"/>            |      | 1/0/5  | 0               | Untrusted  | --  |
| <input type="checkbox"/>            |      | 1/0/6  | 0               | Untrusted  | --  |
| <input type="checkbox"/>            |      | 1/0/7  | 0               | Untrusted  | --  |
| <input type="checkbox"/>            |      | 1/0/8  | 0               | Untrusted  | --  |
| <input type="checkbox"/>            |      | 1/0/9  | 0               | Untrusted  | --  |
| <input type="checkbox"/>            |      | 1/0/10 | 0               | Untrusted  | --  |

Total: 10      1 entry selected.     

Wykonaj poniższe kroki, aby skonfigurować trust mode:

1) Wybierz porty i ustaw trust mode jako Trust DSCP.

**Trust Mode** Ustaw ten tryb jako Trust DSCP. W tym trybie pakiety IP będą przetwarzane zgodnie z konfiguracją priorytetyzacji DSCP, a pakiety non-IP zgodnie z konfiguracją priorytetyzacji portu.

2) Kliknij **Apply**.

- Konfiguracja mapowania 802.1p do kolejek

Wybierz z menu **QoS > Class of Service > 802.1p Priority**, aby wyświetlić poniższą stronę.

Rys. 2-6 Konfiguracja mapowania 802.1p do kolejek

#### 802.1p to Queue Mapping

| 802.1p Priority | Queue                             |
|-----------------|-----------------------------------|
| 0:              | <input type="text" value="TC-1"/> |
| 1:              | <input type="text" value="TC-0"/> |
| 2:              | <input type="text" value="TC-2"/> |
| 3:              | <input type="text" value="TC-3"/> |
| 4:              | <input type="text" value="TC-4"/> |
| 5:              | <input type="text" value="TC-5"/> |
| 6:              | <input type="text" value="TC-6"/> |
| 7:              | <input type="text" value="TC-7"/> |

#### 802.1p Remap

| 802.1p Priority | Remap                          |
|-----------------|--------------------------------|
| 0:              | <input type="text" value="0"/> |
| 1:              | <input type="text" value="1"/> |
| 2:              | <input type="text" value="2"/> |
| 3:              | <input type="text" value="3"/> |
| 4:              | <input type="text" value="4"/> |
| 5:              | <input type="text" value="5"/> |
| 6:              | <input type="text" value="6"/> |
| 7:              | <input type="text" value="7"/> |

W sekcji **802.1p to Queue Mapping** skonfiguruj mapowania i kliknij **Apply**.

|                        |                                                                                                                               |
|------------------------|-------------------------------------------------------------------------------------------------------------------------------|
| <b>802.1p Priority</b> | Wartość priorytetu 802.1p. W przypadku usługi QoS, priorytetyzacja 802.1p jest częścią usługi class of service.               |
| <b>Queue</b>           | Wybierz kolejkę TC dla wybranego priorytetu 802.1p. Pakiety z tym priorytetem 802.1p będą umieszczane w odpowiedniej kolejce. |

- Konfiguracja mapowania DSCP do 802.1p i remapowania DSCP

Wybierz z menu **QoS > Class of Service > DSCP Priority**, aby wyświetlić poniższą stronę.

Rys. 2-7 Konfiguracja mapowania DSCP do 802.1p i remapowania DSCP

| <input type="checkbox"/>            | DSCP Priority | 802.1p Priority | DSCP Remap     |
|-------------------------------------|---------------|-----------------|----------------|
| <input checked="" type="checkbox"/> | 0             | 0               | 0 be (000000)  |
| <input type="checkbox"/>            | 1             | 0               | 1              |
| <input type="checkbox"/>            | 2             | 0               | 2              |
| <input type="checkbox"/>            | 3             | 0               | 3              |
| <input type="checkbox"/>            | 4             | 0               | 4              |
| <input type="checkbox"/>            | 5             | 0               | 5              |
| <input type="checkbox"/>            | 6             | 0               | 6              |
| <input type="checkbox"/>            | 7             | 0               | 7              |
| <input type="checkbox"/>            | 8             | 1               | 8 cs1 (001000) |
| <input type="checkbox"/>            | 9             | 1               | 9              |

Total: 64      1 entry selected.     

Wykonaj poniższe kroki, aby skonfigurować priorytetyzację DSCP:

1) W sekcji **DSCP Priority Config** skonfiguruj mapowanie 802.1p i remapowanie DSCP.

|                      |                                                                                                                                                                                                                                                                                                            |
|----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>DSCP Priority</b> | Wartość priorytetu DSCP. Priorytetyzacja DSCP służy klasyfikacji pakietów w oparciu o wartość DSCP i mapowaniu ich do różnych kolejek. ToS (Type of Service) to część nagłówka IP, a DSCP wykorzystuje pierwsze sześć bitów ToS do ustalania priorytetów pakietów IP. Wartości DSCP wahają się od 0 do 63. |
|----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

|                        |                                                                                                                                                                                                                                                                                                                                             |
|------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>802.1p Priority</b> | Określ mapowanie DSCP do 802.1p. Pakiety przychodzące są najpierw mapowane do priorytetu 802.1p, w oparciu o mapowania DSCP do 802.1p, a następnie do kolejek TC, zgodnie z mapowaniami 802.1p do kolejek. Nietagowanym pakietem IP z żadaną wartością DSCP będą nadawane wartości priorytetów 802.1p, zgodnie z mapowaniem DSCP do 802.1p. |
|------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

|                   |                                                                                                                                                                                                        |
|-------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>DSCP Remap</b> | (Opcjonalnie) Wybierz priorytet DSCP, do którego oryginalny priorytet DSCP zostanie zremapowany. Gdy przełącznik wykryje pakiety z żadaną wartością DSCP, zmieni wartość pakietów DSCP zgodnie z mapą. |
|-------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

2) Kliknij **Apply**.

 **Uwaga:**

W trybie Trust DSCP pakietom non-IP zostanie nadany priorytet 802.1p w oparciu o mapowanie portu do 802.1p i zostaną one przesłane zgodnie z mapowaniem 802.1p do kolejek.

## 2.1.4 Konfiguracja ustawień harmonogramu

Dostosuj ustawienia harmonogramu, aby kontrolować sekwencję przesyłania różnych kolejek TC w przypadku przeciążenia.





Wybierz z menu **QoS > Class of Service > Scheduler Settings**, aby wyświetlić poniższą stronę.

Rys. 2-8 Konfiguracja ustawień harmonogramu

Scheduler Config

UNIT1      LAGS





Port 1/0/1

| <input type="checkbox"/>            | Queue TC-id | Scheduler Type    | Queue Weight | Management Type                                                            |
|-------------------------------------|-------------|-------------------|--------------|----------------------------------------------------------------------------|
| <input checked="" type="checkbox"/> | 0           | Weighted          | 1            | Taildrop                                                                   |
| <input type="checkbox"/>            | 1           | Weighted          | 1            | Taildrop                                                                   |
| <input type="checkbox"/>            | 2           | Weighted          | 1            | Taildrop                                                                   |
| <input type="checkbox"/>            | 3           | Weighted          | 1            | Taildrop                                                                   |
| <input type="checkbox"/>            | 4           | Weighted          | 1            | Taildrop                                                                   |
| <input type="checkbox"/>            | 5           | Weighted          | 1            | Taildrop                                                                   |
| <input type="checkbox"/>            | 6           | Weighted          | 1            | Taildrop                                                                   |
| <input type="checkbox"/>            | 7           | Weighted          | 1            | Taildrop                                                                   |
| Total: 8                            |             | 1 entry selected. |              | <input type="button" value="Cancel"/> <input type="button" value="Apply"/> |

Wykonaj poniższe kroki, aby skonfigurować tryb harmonogramu:

- 1) W sekcji **Scheduler Config** wybierz port.
- 2) Wybierz kolejki i skonfiguruj parametry.

| Queue TC-id                  | ID kolejki priorytetyzacji.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p><b>Scheduler Type</b></p> | <p>Wybierz typ harmonogramu dla danej kolejki. W przypadku przeciążenia sieci, kolejka ruchu wychodzącego określi sekwencję przesyłania pakietów zgodnie z wybranym typem.</p> <p><b>Strict:</b> W tym trybie kolejka ruchu wychodzącego skorzysta z SP (Strict Priority) do przetwarzania ruchu w różnych kolejkach. W przypadku przeciążenia sieci, ruch będzie przesyłany ściśle według priorytetów kolejek. Kolejka o wyższym poziomie priorytetu wykorzystuje całą przepustowość. Pakiety w kolejkach o niższym poziomie priorytetu są wysyłane tylko wtedy, gdy kolejka o wyższym poziomie priorytetu jest pusta.</p> <p><b>Weighted:</b> W tym trybie kolejka ruchu wychodzącego skorzysta z WRR (Weighted Round Robin) do przetwarzania ruchu w różnych kolejkach. W przypadku przeciążenia sieci, cały ruch będzie przesyłany, ale przepustowość sieci zostanie przydzielona kolejkom na podstawie wagi kolejek.</p> |

|                 |                                                                                                                                         |
|-----------------|-----------------------------------------------------------------------------------------------------------------------------------------|
| Queue Weight    | Określ wagę daną kolejki. Ta wartość może być ustawiona tylko w trybie Weighted. Prawidłowe wartości wahają się od 1 do 127.            |
| Management Type | Typ zarządzania kolejek. Przełącznik obsługuje tryb Taildrop. Gdy przesyłany ruch przekroczy limit, nadmiarowy ruch zostanie odrzucony. |

### 3) Kliknij **Apply**.

#### Uwaga:

Funkcja ACL Redirect sprawia, że przełącznik mapuje wszystkie pakiety, który spełniają reguły ACL do nowej kolejki TC, niezależnie od ustawień relacji mapowań, które zostały skonfigurowane w tej sekcji.

## 2.2 Przez CLI

### 2.2.1 Konfiguracja priorytetyzacji portów

- Konfiguracja Trust Mode i mapowania portu do 802.1p

Wykonaj poniższe kroki, aby skonfigurować trust mode i mapowanie portu do 802.1p:

|        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Krok 1 | <b>configure</b><br>Uruchom tryb konfiguracji globalnej                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Krok 2 | <b>interface {fastEthernet <i>port</i>   range fastEthernet <i>port-list</i>   gigabitEthernet <i>port</i>   range gigabitEthernet <i>port-list</i>   ten-gigabitEthernet <i>port</i>   range ten-gigabitEthernet <i>port-list</i>   port-channel <i>port-channel-id</i>   range port-channel <i>port-channel-list</i>}</b><br>Uruchom tryb konfiguracji interfejsu.                                                                                                                                                                                                 |
| Krok 3 | <b>qos trust mode {untrust   dot1p   dscp}</b><br>Wybierz trust mode dla portu. Domyślnym trybem jest untrust. Poniższe polecenie ustawia trust mode jako untrust.<br><br><i>untrust</i> : Ustawia dla portu tryb untrust. W tym trybie pakiety będą przetwarzane zgodnie z konfiguracją priorytetyzacji portu.                                                                                                                                                                                                                                                      |
| Krok 4 | <b>qos port-priority {dot1p-priority}</b><br>Wybierz dla portu mapowanie portu do priorytetu 802.1p. Pakiety przychodzące są w pierwszej kolejności mapowane do priorytetu 802.1p na podstawie mapowania portu do 802.1p, następnie do kolejek TC w oparciu o mapowanie 802.1p do kolejek. Pakiety nietagowane z jednego portu będą mieć przydzieloną wartość priorytetu 802.1p, zgodnie z mapowaniem priorytetyzacji portu do priorytetu 802.1p.<br><br><i>dot1p-priority</i> : Uzupełnij priorytet 802.1p wartością z przedziału 0 - 7. Wartością domyślną jest 0. |
| Krok 5 | <b>show qos trust interface [fastEthernet <i>port</i>   gigabitEthernet <i>port</i>   ten-gigabitEthernet <i>port</i>   port-channel <i>port-channel-id</i>]</b><br>Sprawdź konfigurację trust mode dla portów.                                                                                                                                                                                                                                                                                                                                                      |

---

Krok 6 **show qos port-priority interface [fastEthernet *port* | gigabitEthernet *port* | ten-gigabitEthernet *port* | port-channel *port-channel-id*]**

Sprawdź mapowania portu do 802.1p.

---

Krok 7 **end**

Powróć do trybu privileged EXEC.

---

Krok 8 **copy running-config startup-config**

Zapisz ustawienia w pliku konfiguracyjnym.

---

## ■ Konfiguracja mapowania 802.1p do kolejek

Wykonaj poniższe kroki, aby skonfigurować mapowanie 802.1p do kolejek:

---

Krok 1 **configure**

Uruchom tryb konfiguracji globalnej

---

Krok 2 **qos cos-map {dot1p-priority} {tc-queue}**

Określ mapowanie 802.1p do kolejek. Pakiety z żądanym priorytetem 802.1p będą umieszczane w odpowiedniej kolejce. Domyślnie priorytety 802.1p od 0 do 7 są odpowiednio mapowane do: TC-1, TC-0, TC-2, TC-3, TC-4, TC-5, TC-6, TC-7.

*dot1p-priority*: Uzupełnij priorytet 802.1p. Prawidłowe wartości wahają się od 0 do 7.

*tc-queue*: Podaj ID kolejki TC. Prawidłowe wartości wahają się od 0 do 7.

---

Krok 3 **show qos cos-map**

Sprawdź mapowanie 802.1p do kolejek.

---

Krok 4 **end**

Powróć do trybu privileged EXEC.

---

Krok 5 **copy running-config startup-config**

Zapisz ustawienia w pliku konfiguracyjnym.

---

TPoniższy schemat przedstawia przykładowe ustawianie trust mode portu 1/0/1 jako untrust, mapowania portu 1/0/1 do priorytetu 1 802.1p i mapowania priorytetu 1 802.1p do TC3:

```
Switch#configure
```

```
Switch(config)#interface gigabitEthernet 1/0/1
```

```
Switch(config-if)#qos trust mode untrust
```

```
Switch(config-if)#qos port-priority 1
```

```
Switch(config-if)#exit
```

```
Switch(config)#qos cos-map 1 3
```

```
Switch(config)#show qos trust interface gigabitEthernet 1/0/1
```

```
Port Trust Mode LAG
----- -
Gi1/0/1 untrust N/A
```

```
Switch(config)#show qos port-priority interface gigabitEthernet 1/0/1
```

```
Port CoS Value LAG
----- -
Gi1/0/1 CoS 1 N/A
```

```
Switch(config)#show qos cos-map
```

```
-----+-----+-----+-----+-----+-----+-----+-----+-----
Dot1p Value |0 |1 |2 |3 |4 |5 |6 |7
-----+-----+-----+-----+-----+-----+-----+-----+-----
TC |TC0 |TC3 |TC2 |TC3 |TC4 |TC5 |TC6 |TC7
-----+-----+-----+-----+-----+-----+-----+-----+-----
```

```
Switch(config)#end
```

```
Switch#copy running-config startup-config
```

## 2.2.2 Konfiguracja priorytetyzacji 802.1p

### ■ Konfiguracja Trust Mode

Wykonaj poniższe kroki, aby skonfigurować trust mode:

---

|        |                                     |
|--------|-------------------------------------|
| Krok 1 | <b>configure</b>                    |
|        | Uruchom tryb konfiguracji globalnej |

---

|        |                                                                                                                                                                                                                                                                                                                                                                                                                          |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Krok 2 | <p><b>interface {fastEthernet <i>port</i>   range fastEthernet <i>port-list</i>   gigabitEthernet <i>port</i>   range gigabitEthernet <i>port-list</i>   ten-gigabitEthernet <i>port</i>   range ten-gigabitEthernet <i>port-list</i>   port-channel <i>port-channel-id</i>   range port-channel <i>port-channel-list</i>}</b></p> <p>Uruchom tryb konfiguracji interfejsu.</p>                                          |
| Krok 3 | <p><b>qos trust mode {untrust   dot1p   dscp}</b></p> <p>Wybierz trust mode dla portu. Domyślnie ustawiony jest tryb untrust. Za pomocą poniższego polecenia ustawimy trust mode jako dot1p.</p> <p><i>dot1p</i>: Ustawia tryb portów jako dot1p. W tym trybie pakiety tagowane będą przetwarzane zgodnie z konfiguracją priorytetyzacji 802.1p, a pakiety nietagowane zgodnie z konfiguracją priorytetyzacji portu.</p> |
| Krok 4 | <p><b>show qos trust interface [fastEthernet <i>port</i>   gigabitEthernet <i>port</i>   ten-gigabitEthernet <i>port</i>   port-channel <i>port-channel-id</i>]</b></p> <p>Sprawdź trust mode portów.</p>                                                                                                                                                                                                                |
| Krok 5 | <p><b>end</b></p> <p>Powróć do trybu privileged EXEC.</p>                                                                                                                                                                                                                                                                                                                                                                |
| Krok 6 | <p><b>copy running-config startup-config</b></p> <p>Zapisz ustawienia w pliku konfiguracyjnym.</p>                                                                                                                                                                                                                                                                                                                       |

#### ■ Konfiguracja mapowania 802.1p do kolejek i remapowania 802.1p

Wykonaj poniższe kroki, aby skonfigurować mapowanie 802.1p do kolejek i remapowanie 802.1p:

|        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Krok 1 | <p><b>configure</b></p> <p>Uruchom tryb konfiguracji globalnej</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Krok 2 | <p><b>qos cos-map {dot1p-priority} {tc-queue}</b></p> <p>Określ mapowanie 802.1p do kolejek. Pakiety z żądanym priorytetem 802.1p będą umieszczane w odpowiednich kolejkach. Domyślnie priorytety 802.1p od 0 do 7 są odpowiednio mapowane do: TC-1, TC-0, TC-2, TC-3, TC-4, TC-5, TC-6, TC-7.</p> <p><i>dot1p-priority</i>: Uzupełnij priorytet 802.1p. Prawidłowe wartości wahają się od 0 do 7.</p> <p><i>tc-queue</i>: Podaj ID kolejki TC. Prawidłowe wartości wahają się od 0 do 7.</p>                                                                                                                                                                                                                                                         |
| Krok 3 | <p><b>qos dot1p-remap {dot1p-priority} {new-dot1p-priority}</b></p> <p>(Opcjonalnie) Określ mapowania 802.1p do 802.1p. Remapowanie 802.1p służy modyfikacji priorytetów 802.1p pakietów przychodzących. Gdy przełącznik wykryje pakiety z żądanymi priorytetami 802.1p, zmieni wartość priorytetów 802.1p zgodnie z mapą. Domyślnie oryginalny priorytet 802.1p o wartości 0 jest mapowany do priorytetu 802.1p o wartości 0, oryginalny priorytet 802.1p o wartości 1 jest mapowany do priorytetu 802.1p o wartości 1, itd.</p> <p><i>dot1p-priority</i>: Podaj oryginalny priorytet 802.1p. Prawidłowe wartości wahają się od 0 do 7.</p> <p><i>new-dot1p-priority</i>: Podaj nowy priorytet 802.1p. Prawidłowe wartości wahają się od 0 do 7.</p> |

- 
- Krok 4     **show qos cos-map**  
Sprawdź mapowania 802.1p do kolejek.
- 
- Krok 5     **show qos dot1p-remap**  
Sprawdź mapowania 802.1p do 802.1p.
- 
- Krok 6     **end**  
Powróć do trybu uprzywilejowanego (privileged EXEC mode).
- 
- Krok 7     **copy running-config startup-config**  
Zapisz ustawienia w pliku konfiguracyjnym.
- 

 **Uwaga:**

W trybie Trust 802.1p pakietom nietagowanym będą przydzielane priorytety 802.1p w oparciu o mapowanie portu do 802.1p i będą one przesyłane zgodnie z mapowaniem 802.1p do kolejek.

Poniższy schemat przedstawia przykładowe ustawianie trust mode portu 1/0/1 jako dot1p, mapowanie priorytetu 3 802.1p do TC4 i konfigurację mapowania oryginalnego priorytetu 1 802.1p do priorytetu 3 802.1p:

**Switch#configure**

**Switch(config)#interface gigabitEthernet 1/0/1**

**Switch(config-if)#qos trust mode dot1p**

**Switch(config-if)#exit**

**Switch(config)#qos cos-map 3 4**

**Switch(config)#qos dot1p-remap 1 3**

**Switch(config)#show qos trust interface gigabitEthernet 1/0/1**

| Port    | Trust Mode   | LAG   |
|---------|--------------|-------|
| -----   | -----        | ----- |
| Gi1/0/1 | trust 802.1P | N/A   |

**Switch(config)#show qos cos-map**

```

-----+-----+-----+-----+-----+-----+-----+-----
Dot1p Value |0 |1 |2 |3 |4 |5 |6 |7
-----+-----+-----+-----+-----+-----+-----+-----
TC |TC0 |TC1 |TC2 |TC4 |TC4 |TC5 |TC6 |TC7
-----+-----+-----+-----+-----+-----+-----+-----

```

**Switch(config)#show qos dot1p-remap**

|             |       |          |       |       |       |       |       |       |       |
|-------------|-------|----------|-------|-------|-------|-------|-------|-------|-------|
| Dot1p Value | 0     | <b>1</b> | 2     | 3     | 4     | 5     | 6     | 7     | LAG   |
|             | ----- | -----    | ----- | ----- | ----- | ----- | ----- | ----- | ----- |
| Dot1p Remap | 0     | <b>3</b> | 2     | 3     | 4     | 5     | 6     | 7     | N/A   |

**Switch(config)#end**

**Switch#copy running-config startup-config**

## 2.2.3 Konfiguracja priorytetyzacji DSCP

### ■ Konfiguracja Trust Mode

Wykonaj poniższe kroki, aby skonfigurować trust mode:

|        |                                                                                                                                                                                                                                                                                                                                                                          |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Krok 1 | <b>configure</b><br>Uruchom tryb konfiguracji globalnej                                                                                                                                                                                                                                                                                                                  |
| Krok 2 | <b>interface {fastEthernet <i>port</i>   range fastEthernet <i>port-list</i>   gigabitEthernet <i>port</i>   range gigabitEthernet <i>port-list</i>   ten-gigabitEthernet <i>port</i>   range ten-gigabitEthernet <i>port-list</i>   port-channel <i>port-channel-id</i>   range port-channel <i>port-channel-list</i>}</b><br>Uruchom tryb konfiguracji interfejsu.     |
| Krok 3 | <b>qos trust mode {untrust   dot1p   dscp}</b><br>Wybierz trust mode dla portu. Domyślnym trybem jest untrust. Poniższe polecenie ustawia trust mode jako dscp.<br><br><i>dscp</i> : Ustawia tryb portu jako dscp. W tym trybie pakiety IP będą przetwarzane zgodnie z konfiguracją priorytetyzacji DSCP, a pakiety non-IP zgodnie z konfiguracją priorytetyzacji portu. |
| Krok 4 | <b>show qos trust interface [fastEthernet <i>port</i>   gigabitEthernet <i>port</i>   ten-gigabitEthernet <i>port</i>   port-channel <i>port-channel-id</i>]</b><br>Sprawdź trust mode portów.                                                                                                                                                                           |
| Krok 5 | <b>end</b><br>Powróć do trybu privileged EXEC.                                                                                                                                                                                                                                                                                                                           |
| Krok 6 | <b>copy running-config startup-config</b><br>Zapisz ustawienia w pliku konfiguracyjnym.                                                                                                                                                                                                                                                                                  |

### ■ Konfiguracja mapowania 802.1p do kolejek

Wykonaj poniższe kroki, aby skonfigurować mapowanie 802.1p do kolejek:

|        |                                                         |
|--------|---------------------------------------------------------|
| Krok 1 | <b>configure</b><br>Uruchom tryb konfiguracji globalnej |
|--------|---------------------------------------------------------|

- 
- Krok 2     **qos cos-map {dot1p-priority} {tc-queue}**
- Określ mapowanie 802.1p do kolejek. Pakiety z żądanym priorytetem 802.1p będą umieszczane w odpowiednich kolejkach. Domyślnie priorytety 802.1p od 0 do 7 są odpowiednio mapowane do: TC-1, TC-0, TC-2, TC-3, TC-4, TC-5, TC-6, TC-7.
- dot1p-priority:* Uzupełnij priorytet 802.1p. Prawidłowe wartości wahają się od 0 do 7.
- tc-queue:* Podaj ID kolejki TC. Prawidłowe wartości wahają się od 0 do 7.
- 
- Krok 3     **show qos cos-map**
- Sprawdź mapowania 802.1p do kolejek.
- 
- Krok 4     **end**
- Powróć do trybu uprzywilejowanego (privileged EXEC mode).
- 
- Krok 5     **copy running-config startup-config**
- Zapisz ustawienia w pliku konfiguracyjnym.
- 

#### ■ Konfiguracja mapowania DSCP do 802.1p i remapowania DSCP Remp

Wykonaj poniższe kroki, aby skonfigurować mapowanie DSCP do 802.1p i remapowanie DSCP:

- 
- Krok 1     **configure**
- Uruchom tryb konfiguracji globalnej
- 
- Krok 2     **qos dscp-map {dscp-value-list} {dot1p-priority}**
- Określ mapowanie DSCP do 802.1p. Pakiety przychodzące są najpierw mapowane do priorytetu 802.1p, w oparciu o mapowania DSCP do 802.1p, a następnie do kolejek TC, zgodnie z mapowaniami 802.1p do kolejek. Nietagowanym pakietom IP z żądaną wartością DSCP będą nadawane wartości priorytetów 802.1p, zgodnie z mapowaniem DSCP do 802.1p. Domyślnie priorytety 0-7 DSCP są mapowane do priorytetu 802.1p o wartości 0, priorytety 8-15 DSCP są mapowane do priorytetu 802.1p o wartości 1, itd.
- dscp-value-list:* Podaj listę wartości DSCP w formacie "1-3,5,7". Prawidłowe wartości wahają się od 0 do 63.
- dot1p-priority:* Określ priorytet 802.1p. Prawidłowe wartości wahają się od 0 do 7.
- 
- Krok 3     **qos dscp-remap {dscp-value-list} {dscp-remap-value}**
- (Opcjonalnie) Określ mapowania DSCP do DSCP. Remapowanie DSCP służy modyfikacji priorytetów DSCP pakietów przychodzących. Gdy przełącznik wykryje pakiety z żądanymi priorytetami DSCP, zmieni wartość priorytetów DSCP zgodnie z mapą. Domyślnie oryginalny priorytet DSCP o wartości 0 jest mapowany do priorytetu DSCP o wartości 0, oryginalny priorytet DSCP o wartości 1 jest mapowany do priorytetu DSCP o wartości 1, itd.
- dscp-value-list:* Podaj listę oryginalnych priorytetów w formacie "1-3,5,7". Prawidłowe wartości wahają się od 0 do 63.
- dscp-remap-value:* Podaj nowy priorytet DSCP. Prawidłowe wartości wahają się od 0 do 63.
-



- 
- Krok 4     **show qos dscp-map**  
Sprawdź mapowania DSCP do kolejek.
- 
- Krok 5     **show qos dscp-remap**  
Sprawdź mapowania DSCP do DSCP.
- 
- Krok 6     **end**  
Powróć do trybu uprzywilejowanego (privileged EXEC mode).
- 
- Krok 7     **copy running-config startup-config**  
Zapisz ustawienia w pliku konfiguracyjnym.
- 

 **Uwaga:**

W trybie Trust DSCP pakietom non-IP będą przydzielane priorytety 802.1p w oparciu o mapowanie portu do 802.1p i będą one przesyłane zgodnie z mapowaniem 802.1p do kolejek.

Poniższy schemat przedstawia przykładowe ustawianie trust mode portu 1/0/1 jako dscp, mapowanie priorytetu 3 802.1p do TC4, mapowanie priorytetów 1-3,5,7 DSCP do priorytetu 3 802.1p i konfigurację mapowania oryginalnego priorytetu 9 DSCP do priorytetu 5 DSCP:

**Switch#configure**

**Switch(config)#interface gigabitEthernet 1/0/1**

**Switch(config-if)#qos trust mode dscp**

**Switch(config-if)#exit**

**Switch(config)#qos cos-map 3 4**

**Switch(config)#qos dscp-map 1-3,5,7 3**

**Switch(config)#qos dscp-remap 9 5**

**Switch(config)#show qos trust interface gigabitEthernet 1/0/1**

| Port    | Trust Mode | LAG   |
|---------|------------|-------|
| -----   | -----      | ----- |
| Gi1/0/1 | trust DSCP | N/A   |

**Switch(config)#show qos cos-map**

```
-----+-----+-----+-----+-----+-----+-----+-----+-----
```

| Dot1p Value | 0     | 1     | 2     | 3     | 4     | 5     | 6     | 7     |
|-------------|-------|-------|-------|-------|-------|-------|-------|-------|
| -----       | ----- | ----- | ----- | ----- | ----- | ----- | ----- | ----- |
| TC          | TC0   | TC1   | TC2   | TC4   | TC4   | TC5   | TC6   | TC7   |
| -----       | ----- | ----- | ----- | ----- | ----- | ----- | ----- | ----- |

**Switch(config)#show qos dscp-map**

```

DSCP: 0 1 2 3 4 5 6 7
DSCP to 802.1P 0 3 3 3 0 3 0 3

DSCP: 8 9 10 11 12 13 14 15
DSCP to 802.1P 1 1 1 1 1 1 1 1

DSCP: 16 17 18 19 20 21 22 23
DSCP to 802.1P 2 2 2 2 2 2 2 2

DSCP: 24 25 26 27 28 29 30 31
DSCP to 802.1P 3 3 3 3 3 3 3 3

DSCP: 32 33 34 35 36 37 38 39
DSCP to 802.1P 4 4 4 4 4 4 4 4

DSCP: 40 41 42 43 44 45 46 47
DSCP to 802.1P 5 5 5 5 5 5 5 5

DSCP: 48 49 50 51 52 53 54 55
DSCP to 802.1P 6 6 6 6 6 6 6 6

DSCP: 56 57 58 59 60 61 62 63
DSCP to 802.1P 7 7 7 7 7 7 7 7

```

**Switch(config)#show qos dscp-remap**

```

DSCP: 0 1 2 3 4 5 6 7
DSCP remap value 0 1 2 3 4 5 6 7

DSCP: 8 9 10 11 12 13 14 15

```

```

DSCP remap value 8 5 10 11 12 13 14 15

DSCP: 16 17 18 19 20 21 22 23
DSCP remap value 16 17 18 19 20 21 22 23

DSCP: 24 25 26 27 28 29 30 31
DSCP remap value 24 25 26 27 28 29 30 31

DSCP: 32 33 34 35 36 37 38 39
DSCP remap value 32 33 34 35 36 37 38 39

DSCP: 40 41 42 43 44 45 46 47
DSCP remap value 40 41 42 43 44 45 46 47

DSCP: 48 49 50 51 52 53 54 55
DSCP remap value 48 49 50 51 52 53 54 55

DSCP: 56 57 58 59 60 61 62 63
DSCP remap value 56 57 58 59 60 61 62 63

```

**Switch(config-if)#end**

**Switch#copy running-config startup-config**

## 2.2.4 Konfiguracja ustawień harmonogramu

Wykonaj poniższe kroki, aby dostosować ustawienia harmonogramu, w celu kontroli sekwencji przesyłania różnych kolejek TC w przypadku przeciążenia sieci.

Krok 1     **configure**

Uruchom tryb konfiguracji globalnej.

Krok 2     **interface {fastEthernet *port* | range fastEthernet *port-list* | gigabitEthernet *port* | range gigabitEthernet *port-list* | ten-gigabitEthernet *port* | range ten-gigabitEthernet *port-list* | port-channel *port-channel-id* | range port-channel *port-channel-list*}**

Uruchom tryb konfiguracji interfejsu.

**Krok 3** `qos queue tc-queue mode {sp | wrr} [weight weight]`

Wybierz typ harmonogramu dla danej kolejki. W przypadku przeciążenia sieci, kolejka ruchu wychodzącego określi sekwencję przesyłania pakietów zgodnie z wybranym typem. Domyślnie ustawionym trybem jest wrr, a wagą wszystkich kolejek wartość 1.

*tc-queue*: Podaj ID kolejki TC. Prawidłowe wartości wahają się od 0 do 7.

*sp*: W tym trybie kolejka ruchu wychodzącego skorzysta z SP (Strict Priority) do przetwarzania ruchu w różnych kolejkach. W przypadku przeciążenia sieci, ruch będzie przesyłany ściśle według priorytetów kolejek. Kolejka o wyższym poziomie priorytetu wykorzystuje całą przepustowość. Pakiety w kolejkach o niższym poziomie priorytetu są wysyłane tylko wtedy, gdy kolejka o wyższym poziomie priorytetu jest pusta.

*wrr*: W tym trybie kolejka ruchu wychodzącego skorzysta z WRR (Weighted Round Robin) do przetwarzania ruchu w różnych kolejkach. W przypadku przeciążenia sieci, cały ruch będzie przesyłany, ale przepustowość sieci zostanie przydzielona kolejkom na podstawie wagi kolejek.

*weight*: Określ wagę danej kolejki. Ta wartość może być ustawiona tylko w trybie wrr. Prawidłowe wartości wahają się od 1 do 127.

**Krok 4** `show qos queue interface [fastEthernet port | gigabitEthernet port | ten-gigabitEthernet port | port-channel port-channel-id]`

Sprawdź ustawienia harmonogramu.

**Krok 5** `end`

Powrót do trybu privileged EXEC.

**Krok 6** `copy running-config startup-config`

Zapisz ustawienia w pliku konfiguracyjnym.

 **Uwaga:**

Funkcja ACL Redirect sprawia, że przełącznik mapuje wszystkie pakiety, który spełniają reguły ACL do nowej kolejki TC, niezależnie od ustawień relacji mapowań, które zostały skonfigurowane w tej sekcji. .

Poniższy schemat przedstawia przykładową konfigurację ustawień harmonogramu dla portu 1/0/1. Tryb harmonogramu TC1 zostanie skonfigurowany na tryb sp, tryb harmonogramu TC4 na tryb wrr, a waga kolejki na 5.

**Switch#configure**

```
Switch(config)#interface gigabitEthernet 1/0/1
```

```
Switch(config-if)#qos queue 1 mode sp
```

```
Switch(config-if)#qos queue 4 mode wrr weight 5
```

```
Switch(config-if)#show qos queue interface gigabitEthernet 1/0/1
```

```
Gi1/0/1----LAG: N/A
```

```
Queue Schedule Mode Weight
```

```

```

---

|     |        |     |
|-----|--------|-----|
| TC0 | WRR    | 1   |
| TC1 | Strict | N/A |
| TC2 | WRR    | 1   |
| TC3 | WRR    | 1   |
| TC4 | WRR    | 5   |
| TC5 | WRR    | 1   |
| TC6 | WRR    | 1   |
| TC7 | WRR    | 1   |

**Switch(config-if)#end**

**Switch#copy running-config startup-config**

# 3 Konfiguracja kontroli przepustowości

Konfiguracja kontroli przepustowości umożliwia:

- Konfigurację limitu prędkości
- Konfigurację Storm Control

## 3.1 Przez GUI

### 3.1.1 Konfiguracja limitu prędkości

Wybierz z menu **QoS > Bandwidth Control > Rate Limit**, aby wyświetlić poniższą stronę.

Rys. 3-1 Konfiguracja limitu prędkości

| Rate Limit Config                   |        |                                |                               |     |
|-------------------------------------|--------|--------------------------------|-------------------------------|-----|
| UNIT1                               |        | LAGS                           |                               |     |
| <input type="checkbox"/>            | Port   | Ingress Rate (0-1,000,000Kbps) | Egress Rate (0-1,000,000Kbps) | LAG |
| <input checked="" type="checkbox"/> | 1/0/1  | 0                              | 0                             | --  |
| <input type="checkbox"/>            | 1/0/2  | 0                              | 0                             | --  |
| <input type="checkbox"/>            | 1/0/3  | 0                              | 0                             | --  |
| <input type="checkbox"/>            | 1/0/4  | 0                              | 0                             | --  |
| <input type="checkbox"/>            | 1/0/5  | 0                              | 0                             | --  |
| <input type="checkbox"/>            | 1/0/6  | 0                              | 0                             | --  |
| <input type="checkbox"/>            | 1/0/7  | 0                              | 0                             | --  |
| <input type="checkbox"/>            | 1/0/8  | 0                              | 0                             | --  |
| <input type="checkbox"/>            | 1/0/9  | 0                              | 0                             | --  |
| <input type="checkbox"/>            | 1/0/10 | 0                              | 0                             | --  |

Total: 10      1 entry selected.     

Wykonaj poniższe kroki, aby skonfigurować funkcję limitu prędkości:

- 1) Wybierz porty i skonfiguruj górny limit prędkości odbierania i wysyłania pakietów.

**Ingress Rate (0-1,000,000Kbps)**

Skonfiguruj górny limit prędkości odbierania pakietów na porcie. Prawidłowe wartości wahają się od 0 do 1000000 kb/s, a 0 oznacza, że limit prędkości na wejściu jest wyłączony.

**Egress Rate (0-1,000,000Kbps)**

Skonfiguruj przepustowość wysyłania pakietów na porcie. Prawidłowe wartości wahają się od 0 do 1000000 Kb/s, a 0 oznacza, że limit prędkości na wyjściu jest wyłączony.

- 2) Kliknij **Apply**.

### 3.1.2 Konfiguracja Storm Control

Wybierz z menu **QoS > Bandwidth Control > Storm Control**, aby wyświetlić poniższą stronę.

Rys. 3-2 Konfiguracja Storm Control

Storm Control Config

UNIT1
LAGS
↻ Recover

| <input type="checkbox"/>            | Port   | Rate Mode | Broadcast Threshold (0-1,000,000) | Multicast Threshold (0-1,000,000) | UL-Frame Threshold (0-1,000,000) | Action | Recover Time | LAG |
|-------------------------------------|--------|-----------|-----------------------------------|-----------------------------------|----------------------------------|--------|--------------|-----|
|                                     |        | kbps      |                                   |                                   |                                  |        |              |     |
| <input checked="" type="checkbox"/> | 1/0/1  | kbps      | 0                                 | 0                                 | 0                                | Drop   | 0            | --- |
| <input type="checkbox"/>            | 1/0/2  | kbps      | 0                                 | 0                                 | 0                                | Drop   | 0            | --- |
| <input type="checkbox"/>            | 1/0/3  | kbps      | 0                                 | 0                                 | 0                                | Drop   | 0            | --- |
| <input type="checkbox"/>            | 1/0/4  | kbps      | 0                                 | 0                                 | 0                                | Drop   | 0            | --- |
| <input type="checkbox"/>            | 1/0/5  | kbps      | 0                                 | 0                                 | 0                                | Drop   | 0            | --- |
| <input type="checkbox"/>            | 1/0/6  | kbps      | 0                                 | 0                                 | 0                                | Drop   | 0            | --- |
| <input type="checkbox"/>            | 1/0/7  | kbps      | 0                                 | 0                                 | 0                                | Drop   | 0            | --- |
| <input type="checkbox"/>            | 1/0/8  | kbps      | 0                                 | 0                                 | 0                                | Drop   | 0            | --- |
| <input type="checkbox"/>            | 1/0/9  | kbps      | 0                                 | 0                                 | 0                                | Drop   | 0            | --- |
| <input type="checkbox"/>            | 1/0/10 | kbps      | 0                                 | 0                                 | 0                                | Drop   | 0            | --- |
| Total: 10                           |        |           | 1 entry selected.                 |                                   |                                  | Cancel | Apply        |     |

Wykonaj poniższe kroki, aby skonfigurować funkcje Storm Control:

- Wybierz port i skonfiguruj górny limit prędkości przesyłania pakietów broadcast, pakietów multicast i ramek unknown unicast (UL-frames).

#### Rate Mode

Wybierz tryb prędkości dla progu transmisji broadcast, progu transmisji multicastowej i progu UL-Frame na danym porcie.

**kbps:** Przełącznik ograniczy maksymalną prędkość w kilobitach na sekundę dla określonych rodzajów ruchu.

**ratio:** Przełącznik ograniczy przydzielanie przepustowości dla określonych rodzajów ruchu.

#### Broadcast Threshold (0-1,000,000)

Podaj górny limit prędkości odbierania pakietów broadcast. Prawidłowe wartości zależą od trybów prędkości. 0 oznacza, że próg transmisji broadcast jest wyłączony. Transmisja broadcast, która przekroczy ustawiony limit, będzie przetwarzana zgodnie z ustawieniami opcji Action.

#### Multicast Threshold (0-1,000,000)

Podaj górny limit prędkości odbierania pakietów multicast. Prawidłowe wartości zależą od trybów prędkości. 0 oznacza, że próg transmisji multicastowej jest wyłączony. Transmisja multicastowa, która przekroczy ustawiony limit, będzie przetwarzana zgodnie z ustawieniami opcji Action.

|                                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|----------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| UL-Frame Threshold (0-1,000,000) | Podaj górny limit prędkości odbierania UL-frames. Prawidłowe wartości zależą od trybów prędkości. 0 oznacza, że próg transmisji unknown unicast jest wyłączony. Transmisja unknown unicast, która przekroczy ustawiony limit, będzie przetwarzana zgodnie z ustawieniami opcji Action.                                                                                                                                                         |
| Action                           | Wybierz działanie, które podejmie przełącznik, gdy transmisja przekroczy ustawiony limit.<br><br><b>Drop:</b> Działanie odrzucające. Port odrzuci kolejne pakiety, gdy transmisja przekroczy dozwolony limit.<br><br><b>Shutdown:</b> Działanie wyłączające. Port zostanie wyłączony, gdy transmisja przekroczy dozwolony limit.                                                                                                               |
| Recover Time                     | Podaj czas do przywrócenia portu. Uzupelnienie tej wartości możliwe jest tylko, gdy ustawionym działaniem jest Shutdown. Prawidłowe wartości wahają się od 0 do 3600 sekund. Gdy port zostaje wyłączony, ponownie może być uruchomiony dopiero, gdy upłynie czas do przywrócenia portu. Jeżeli ustawioną wartością jest 0, oznacza to, że port nie zostanie przywrócony do normalnego działania automatycznie, więc trzeba go włączyć ręcznie. |

## 2) Kliknij **Apply**.

### Uwaga:

Rate limit / storm control powinny mieć tą samą wartość dla portów z tej samej grupy agregacji łączy, aby agregacja portów powiodła się.

## 3.2 Przez CLI

### 3.2.1 Konfiguracja limitu prędkości

Wykonaj poniższe kroki, aby skonfigurować górny limit prędkości odbierania i wysyłania pakietów na porcie:

|        |                                                                                                                                                                                                                                                                                                                                                                      |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Krok 1 | <b>configure</b><br>Uruchom tryb konfiguracji globalnej.                                                                                                                                                                                                                                                                                                             |
| Krok 2 | <b>interface {fastEthernet <i>port</i>   range fastEthernet <i>port-list</i>   gigabitEthernet <i>port</i>   range gigabitEthernet <i>port-list</i>   ten-gigabitEthernet <i>port</i>   range ten-gigabitEthernet <i>port-list</i>   port-channel <i>port-channel-id</i>   range port-channel <i>port-channel-list</i>}</b><br>Uruchom tryb konfiguracji interfejsu. |



**Krok 3** `bandwidth {ingress ingress-rate | egress egress-rate}`

Skonfiguruj górny limit prędkości odbierania i wysyłania pakietów na porcie.

*ingress-rate*: Skonfiguruj górny limit prędkości odbierania pakietów na porcie. Prawidłowe wartości wahają się od 0 do 1000000 kb/s.

*egress-rate*: Skonfiguruj przepustowość wysyłania pakietów na porcie. Prawidłowe wartości wahają się od 0 do 1000000 Kb/s.

**Krok 4** `show bandwidth interface [fastEthernet port | gigabitEthernet port | ten-gigabitEthernet port | port-channel port-channel-id]`

Sprawdź limit prędkości na wejściu/wyjściu dla przesyłania pakietów na porcie lub w grupie agregacji łączy. Jeżeli żaden port lub LAG nie zostanie podany, polecenie pokaże górny limit prędkości na wejściu/wyjściu dla wszystkich portów lub grup agregacji łączy.

**Krok 5** `end`

Powróć do trybu privileged EXEC.

**Krok 6** `copy running-config startup-config`

Zapisz ustawienia w pliku konfiguracyjnym.

Poniższy schemat przedstawia przykładową konfigurację prędkości na wejściu do wartości 5120 kb/s prędkości na wyjściu do wartości 1024 Kb/s dla portu 1/0/5:

**Switch#configure****Switch(config)#interface gigabitEthernet 1/0/5****Switch(config-if)#bandwidth ingress 5120 egress 1024****Switch(config-if)#show bandwidth interface gigabitEthernet 1/0/5**

| Port    | IngressRate(Kbps) | EgressRate(Kbps) | LAG   |
|---------|-------------------|------------------|-------|
| -----   | -----             | -----            | ----- |
| Gi1/0/5 | 5120              | 1024             | N/A   |

**Switch(config-if)#end****Switch#copy running-config startup-config**

### 3.2.2 Konfiguracja Storm Control

Wykonaj poniższe kroki, aby skonfigurować górny limit prędkości przesyłania pakietów broadcast, pakietów multicast i ramek unknown unicast na porcie:

**Krok 1** `configure`

Uruchom tryb konfiguracji globalnej

---

|        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Krok 2 | <p><b>interface {fastEthernet <i>port</i>   range fastEthernet <i>port-list</i>   gigabitEthernet <i>port</i>   range gigabitEthernet <i>port-list</i>   ten-gigabitEthernet <i>port</i>   range ten-gigabitEthernet <i>port-list</i>   port-channel <i>port-channel-id</i>   range port-channel <i>port-channel-list</i>}</b></p> <p>Uruchom tryb konfiguracji interfejsu.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Krok 3 | <p><b>storm-control rate-mode {kbps   ratio}</b></p> <p>Wybierz tryb prędkości dla progu transmisji broadcast, progu transmisji multicastowej i progu UL-Frame na danym porcie.</p> <p><i>kbps</i>: Przełącznik ograniczy maksymalną prędkość w kilobitach na sekundę dla określonych rodzajów ruchu.</p> <p><i>ratio</i>: Przełącznik ograniczy przydzielanie przepustowości dla określonych rodzajów ruchu.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Krok 4 | <p><b>storm-control broadcast <i>rate</i></b></p> <p>Podaj górny limit prędkości odbierania pakietów broadcast. Transmisja broadcast, która przekroczy ustawiony limit, będzie przetwarzana zgodnie z ustawieniami opcji Action.</p> <p><i>rate</i>: Wprowadź górny limit. W trybie kb/s prawidłowe wartości to 1 - 1000000 kb/s. W trybie ratio prawidłowe wartości to 1 - 100 procent.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Krok 5 | <p><b>storm-control multicast <i>rate</i></b></p> <p>Podaj górny limit prędkości odbierania pakietów multicast. Transmisja multicastowa, która przekroczy ustawiony limit, będzie przetwarzana zgodnie z ustawieniami opcji Action.</p> <p><i>rate</i>: Wprowadź górny limit. W trybie kb/s prawidłowe wartości to 1 - 1000000 kb/s. W trybie ratio prawidłowe wartości to 1 - 100 procent.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Krok 6 | <p><b>storm-control unicast <i>rate</i></b></p> <p>Podaj górny limit prędkości odbierania UL-frames. Transmisja unknown unicast, która przekroczy ustawiony limit, będzie przetwarzana zgodnie z ustawieniami opcji Action.</p> <p><i>rate</i>: Wprowadź górny limit. W trybie kb/s prawidłowe wartości to 1 - 1000000 kb/s. W trybie ratio prawidłowe wartości to 1 - 100 procent.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Krok 7 | <p><b>storm-control exceed {drop   shutdown} [<b>recover-time <i>time</i></b>]</b></p> <p>Wybierz działanie i podaj czas do przywrócenia portu. Przełącznik podejmie to działanie, gdy transmisja przekroczy ustawiony limit. Domyślnym ustawieniem jest drop.</p> <p><b>drop</b>: Działanie odrzucające. Port odrzuci kolejne pakiety, gdy transmisja przekroczy dozwolony limit.</p> <p><b>shutdown</b>: Działanie wyłączające. Port zostanie wyłączony, gdy transmisja przekroczy dozwolony limit.</p> <p><b>time</b>: Podaj czas do przywrócenia portu. Uzupełnienie tej wartości możliwe jest tylko, gdy ustawionym działaniem jest Shutdown. Prawidłowe wartości wahają się od 0 do 3600 sekund. Gdy port zostaje wyłączony, ponownie może być uruchomiony dopiero, gdy upłynie czas do przywrócenia portu. Jeżeli ustawioną wartością jest 0, oznacza to, że port nie zostanie przywrócony do normalnego działania automatycznie, więc trzeba go włączyć ręcznie.</p> |

---

**Krok 8 storm-control recover**

(Opcjonalnie) Przywróć port ręcznie. Jeżeli ustawioną wartością jest 0, oznacza to, że port nie zostanie przywrócony do normalnego działania automatycznie. Musisz wtedy skorzystać z tego polecenia, aby przywrócić port ręcznie.

**Krok 9 show storm-control interface [fastEthernet port | gigabitEthernet port | ten-gigabitEthernet port | port-channel port-channel-id]**

Sprawdź ustawienia storm control portu lub grupy agregacji łączy. Jeżeli żaden port lub LAG nie zostanie podany, polecenie pokaże ustawienia storm control dla wszystkich portów lub grup agregacji łączy.

**Krok 10 end**

Powróć do trybu privileged EXEC.

**Krok 11 copy running-config startup-config**

Zapisz ustawienia w pliku konfiguracyjnym.

Poniższy schemat przedstawia przykładowy sposób ustawiania górnego limitu prędkości dla pakietów broadcast jako 1024 kb/s, działania jako shutdown i czasu do przywrócenia portu jako 10 dla portu 1/0/5:

```
Switch#configure
```

```
Switch(config)#interface gigabitEthernet 1/0/5
```

```
Switch(config-if)#storm-control rate-mode kbps
```

```
Switch(config-if)#storm-control broadcast 1024
```

```
Switch(config-if)#storm-control exceed shutdown recover-time 10
```

```
Switch(config-if)#show storm-control interface gigabitEthernet 1/0/5
```

| Port    | Rate Mode | BcRate | McRate | UIRate | Exceed   | Recover Time | LAG   |
|---------|-----------|--------|--------|--------|----------|--------------|-------|
| -----   | -----     | -----  | -----  | -----  | -----    | -----        | ----- |
| Gi1/0/5 | kbps      | 1024   | 0      | 0      | shutdown | 10           | N/A   |

```
Switch(config-if)#end
```

```
Switch#copy running-config startup-config
```

# 4 Konfiguracja Voice VLAN

Wykonaj poniższe kroki, aby przeprowadzić proces konfiguracji Voice VLAN:

- 1) Utwórz 802.1Q VLAN
- 2) Skonfiguruj adresy OUI
- 3) Skonfiguruj globalnie Voice VLAN
- 4) Dodaj porty do Voice VLAN-u

## Wskazówki dotyczące konfiguracji

- Przed konfiguracją voice VLAN konieczne jest utworzenie 802.1Q VLAN dla transmisji głosowej. Szczegółowe informacje o konfiguracji 802.1Q VLAN znajdziesz w rozdziale *Konfiguracja 802.1Q VLAN*.
- VLAN 1 jest domyślnym VLAN-em i nie można go skonfigurować do Voice VLAN-u.
- Tylko jeden VLAN może być Voice VLAN-em na przełączniku.

## 4.1 Przez GUI

### 4.1.1 Konfiguracja adresów OUI

Adres OUI pełni rolę unikalnego identyfikatora producenta urządzenia, przypisanego mu przez IEEE (Institute of Electrical and Electronics Engineers). Przełącznik wykorzystuje ten adres to identyfikowania pakietów voice.

Jeżeli w tabeli OUI nie ma adresu OUI twojego urządzenia głosowego, dodaj nowy adres OUI do tabeli.

Wybierz z menu **QoS > Voice VLAN > OUI Config**, aby wyświetlić poniższą stronę.

Rys. 4-1 Konfiguracja adresów OUI

| OUI Config                                              |          |         |             |
|---------------------------------------------------------|----------|---------|-------------|
| UNIT1 <span style="float: right;">+ Add - Delete</span> |          |         |             |
| <input type="checkbox"/>                                | OUI      | Status  | Description |
| <input type="checkbox"/>                                | 00:01:E3 | Default | SIEMENS     |
| <input type="checkbox"/>                                | 00:03:6B | Default | CISCO1      |
| <input type="checkbox"/>                                | 00:12:43 | Default | CISCO2      |
| <input type="checkbox"/>                                | 00:0F:E2 | Default | H3C         |
| <input type="checkbox"/>                                | 00:60:B9 | Default | NITSUKO     |
| <input type="checkbox"/>                                | 00:D0:1E | Default | PINTEL      |
| <input type="checkbox"/>                                | 00:E0:75 | Default | VERILINK    |
| <input type="checkbox"/>                                | 00:E0:BB | Default | 3COM        |
| <input type="checkbox"/>                                | 00:04:0D | Default | AVAYA1      |
| <input type="checkbox"/>                                | 00:1B:4F | Default | AVAYA2      |
| Total: 11                                               |          |         |             |

Wykonaj poniższe kroki, aby skonfigurować adresy OUI:

- 1) Kliknij **+ Add**, aby wyświetlić poniższą stronę.

Rys. 4-2 Tworzenie wpisu OUI

**OUI**

OUI:  (Format: 00:00:00)

Description:  (1-16 characters)

- 2) Podaj adres OUI i uzupełnij opis.

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>OUI</b>         | Podaj adres OUI swojego urządzenia głosowego. Adres OUI potrzebny jest przełącznikowi do identyfikacji pakietów voice. Adres OUI to 24 pierwsze bity adresu MAC, pełniące rolę unikalnego identyfikatora producenta urządzenia, przypisanego mu przez IEEE (Institute of Electrical and Electronics Engineers). Jeżeli źródłowy adres MAC pakietu jest zgodny z adresami OUI z listy OUI, przełącznik klasyfikuje pakiet jako pakiet voice i nadaje mu priorytet w transmisji. |
| <b>Description</b> | Uzupełnij opis adresu OUI dla jego łatwiejszej identyfikacji.                                                                                                                                                                                                                                                                                                                                                                                                                  |

- 3) Kliknij **Create**.

## 4.1.2 Konfiguracja globalna Voice VLAN

Wybierz z menu **QoS > Voice VLAN > Global Config**, aby wyświetlić poniższą stronę.

Rys. 4-3 Konfiguracja globalna Voice VLAN

**Global Config**

Voice VLAN:  Enable

VLAN ID:  (2-4094)

Priority:

[Apply](#)

Wykonaj poniższe kroki, aby skonfigurować globalnie Voice VLAN:

- 1) Włącz funkcję Voice VLAN i skonfiguruj parametry.

|          |                                                                                                                                                                                                                                          |
|----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| VLAN ID  | Podaj ID 802.1Q VLAN, aby ustawić 802.1Q VLAN jako Voice VLAN.                                                                                                                                                                           |
| Priority | Wybierz priorytet, który zostanie przypisany pakietom voice, pamiętając, że im wyższa wartość, tym wyższy priorytet. Tryb harmonogramu priorytetu IEEE 802.1p możesz skonfigurować poprzez usługę Class of Service, jeżeli to konieczne. |

- 2) Kliknij **Apply**.

### 4.1.3 Dodawanie portów do Voice VLAN

Wybierz z menu **QoS > Voice VLAN > Port Config**, aby wyświetlić poniższą stronę.

Rys. 4-4 Dodawanie portów do Voice VLAN

**Port Config**

UNIT1 | LAGS

|                                     | Port   | Voice VLAN | Operational Status |
|-------------------------------------|--------|------------|--------------------|
| <input checked="" type="checkbox"/> | 1/0/1  | Disabled   | Inactive           |
| <input type="checkbox"/>            | 1/0/2  | Disabled   | Inactive           |
| <input type="checkbox"/>            | 1/0/3  | Disabled   | Inactive           |
| <input type="checkbox"/>            | 1/0/4  | Disabled   | Inactive           |
| <input type="checkbox"/>            | 1/0/5  | Disabled   | Inactive           |
| <input type="checkbox"/>            | 1/0/6  | Disabled   | Inactive           |
| <input type="checkbox"/>            | 1/0/7  | Disabled   | Inactive           |
| <input type="checkbox"/>            | 1/0/8  | Disabled   | Inactive           |
| <input type="checkbox"/>            | 1/0/9  | Disabled   | Inactive           |
| <input type="checkbox"/>            | 1/0/10 | Disabled   | Inactive           |

Total: 10      1 entry selected.

[Cancel](#)   [Apply](#)

Wykonaj poniższe kroki, aby skonfigurować globalnie Voice VLAN:

- 1) Wybierz porty i zaznacz Enable w polu Voice VLAN.

|            |                                                                                                |
|------------|------------------------------------------------------------------------------------------------|
| Voice VLAN | Zaznacz Enable, aby włączyć funkcję Voice VLAN na portach i dodaj wybrane porty do Voice VLAN. |
|------------|------------------------------------------------------------------------------------------------|

|                 |                                                               |
|-----------------|---------------------------------------------------------------|
| Optional Status | Stan Voice VLAN na danym porcie.                              |
|                 | <b>Active:</b> Funkcja Voice VLAN jest włączona na porcie.    |
|                 | <b>Inactive:</b> Funkcja Voice VLAN jest wyłączona na porcie. |

2) Kliknij **Apply**.

## 4.2 Przez CLI

Wykonaj poniższe kroki, aby skonfigurować Voice VLAN:

|        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Krok 1 | <b>configure</b><br>Uruchom tryb konfiguracji globalnej.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Krok 2 | <b>show voice vlan oui-table</b><br>Sprawdź czy adres OUI twojego urządzenia głosowego znajduje się w tabeli OUI.<br><br>Adres OUI potrzebny jest przełącznikowi do identyfikacji pakietów voice. Adres OUI to 24 pierwsze bity adresu MAC, pełniące rolę unikalnego identyfikatora producenta urządzenia, przypisanego mu przez IEEE (Institute of Electrical and Electronics Engineers). Jeżeli źródłowy adres MAC pakietu jest zgodny z adresami OUI z listy OUI, przełącznik klasyfikuje pakiet jako pakiet voice i nadaje mu priorytet w transmisji. |
| Krok 3 | <b>voice vlan oui <i>oui-prefix</i> <i>oui-desc</i> <i>string</i></b><br>Jeżeli w tabeli OUI nie ma adresu OUI twojego urządzenia głosowego, dodaj nowy adres OUI do tabeli.<br><br><i>oui-prefix</i> : Podaj adres OUI swojego urządzenia głosowego w formacie XX:XX:XX.<br><br><i>string</i> : Uzupełnij opis adresu OUI dla jego łatwiejszej identyfikacji. Opis może zawierać maksymalnie 16 znaków.                                                                                                                                                  |
| Krok 4 | <b>voice vlan <i>vid</i></b><br>Włącz funkcję Voice VLAN i ustaw 802.1Q VLAN jako Voice VLAN.<br><br><i>vid</i> : Podaj ID 802.1Q VLAN, aby ustawić 802.1Q VLAN jako Voice VLAN.                                                                                                                                                                                                                                                                                                                                                                          |
| Krok 5 | <b>voice vlan priority <i>pri</i></b><br>Wybierz priorytet, który zostanie przypisany pakietom voice.<br><br><i>pri</i> : Wybierz priorytet, który zostanie przypisany pakietom voice, pamiętając, że im wyższa wartość, tym wyższy priorytet. Prawidłowe wartości wahają się od 0 do 7, a wartością domyślną jest 7. Tryb harmonogramu priorytetu IEEE 802.1p możesz skonfigurować poprzez usługę Class of Service, jeżeli to konieczne.                                                                                                                 |
| Krok 6 | <b>interface {fastEthernet <i>port</i>   range fastEthernet <i>port-list</i>   gigabitEthernet <i>port</i>   range gigabitEthernet <i>port-list</i>   ten-gigabitEthernet <i>port</i>   range ten-gigabitEthernet <i>port-list</i>   port-channel <i>port-channel-id</i>   range port-channel <i>port-channel-list</i>}</b><br>Uruchom tryb konfiguracji interfejsu.                                                                                                                                                                                      |
| Krok 7 | <b>voice vlan</b><br>Włącz funkcję Voice VLAN na portach i dodaj wybrane porty do Voice VLAN.                                                                                                                                                                                                                                                                                                                                                                                                                                                             |

Krok 8 **show voice vlan interface**  
Przejrzyj konfigurację Voice VLAN.

Krok 8 **end**  
Powróć do trybu privileged EXEC.

Krok 9 **copy running-config startup-config**  
Zapisz ustawienia w pliku konfiguracyjnym.

Poniższy schemat przedstawia przykładowy sposób otwierania tabeli OUI, ustawiania VLAN 8 jako Voice VLAN, ustawiania priorytetu jako 6 i włączania funkcji Voice VLAN na porcie 1/0/3:

### Switch#configure

#### Switch(config)#show voice vlan oui-table

```
00:01:E3 Default SIEMENS
00:03:6B Default CISCO1
00:12:43 Default CISCO2
00:0F:E2 Default H3C
00:60:B9 Default NITSUKO
00:D0:1E Default PINTEL
00:E0:75 Default VERILINK
00:E0:BB Default 3COM
00:04:0D Default AVAYA1
00:1B:4F Default AVAYA2
00:04:13 Default SNOM
```

#### Switch(config)#voice vlan 8

#### Switch(config)#voice vlan priority 6

#### Switch(config)#interface gigabitEthernet 1/0/3

#### Switch(config-if)#voice vlan

#### Switch(config-if)#show voice vlan interface

```
Voice VLAN ID 8
Priority 6

Interface Voice VLAN Mode Operational Status LAG
----- -
```



|         |          |      |     |
|---------|----------|------|-----|
| Gi1/0/1 | disabled | Down | N/A |
| Gi1/0/2 | disabled | Down | N/A |
| Gi1/0/3 | enabled  | Up   | N/A |
| Gi1/0/4 | disabled | Down | N/A |
| Gi1/0/5 | disabled | Down | N/A |

.....

**Switch(config-if)#end**

**Switch#copy running-config startup-config**

# 5 Konfiguracja Auto VoIP

## Wskazówki dotyczące konfiguracji

- Przed konfiguracją Auto VoIP konieczne jest włączenie LLDP-MED na portach i konfiguracja odpowiednich parametrów. Szczegółowe informacje o konfiguracji LLDP-MED znajdują się w rozdziale *Konfiguracja LLDP*.
- Funkcja Auto VoIP zapewnia elastyczne rozwiązania do optymalizacji transmisji głosowej. Może współpracować z innymi funkcjami, takimi jak VLAN i Class of Service, aby odpowiednio przetwarzać pakiety voice. Wszystkie te funkcje możesz skonfigurować stosownie do swoich potrzeb.

## 5.1 Przez GUI

Wybierz z menu **QoS > Auto VoIP**, aby wyświetlić poniższą stronę.

Rys. 5-1 Konfiguracja Auto VoIP

Global Config

Auto VoIP:  Enable Apply

Port Config

UNIT1

| <input type="checkbox"/>            | Port   | Interface Mode | Value | CoS Override Mode | Operational Status | DSCP Value |
|-------------------------------------|--------|----------------|-------|-------------------|--------------------|------------|
| <input checked="" type="checkbox"/> | 1/0/1  | Disable        | 0     | Disabled          | Disabled           | 0          |
| <input type="checkbox"/>            | 1/0/2  | Disable        | 0     | Disabled          | Disabled           | 0          |
| <input type="checkbox"/>            | 1/0/3  | Disable        | 0     | Disabled          | Disabled           | 0          |
| <input type="checkbox"/>            | 1/0/4  | Disable        | 0     | Disabled          | Disabled           | 0          |
| <input type="checkbox"/>            | 1/0/5  | Disable        | 0     | Disabled          | Disabled           | 0          |
| <input type="checkbox"/>            | 1/0/6  | Disable        | 0     | Disabled          | Disabled           | 0          |
| <input type="checkbox"/>            | 1/0/7  | Disable        | 0     | Disabled          | Disabled           | 0          |
| <input type="checkbox"/>            | 1/0/8  | Disable        | 0     | Disabled          | Disabled           | 0          |
| <input type="checkbox"/>            | 1/0/9  | Disable        | 0     | Disabled          | Disabled           | 0          |
| <input type="checkbox"/>            | 1/0/10 | Disable        | 0     | Disabled          | Disabled           | 0          |

Total: 10 1 entry selected. Cancel Apply

Wykonaj poniższe kroki, aby skonfigurować adresy OUI:

- 1) W sekcji **Global Config** włącz globalnie funkcję Auto VoIP.
- 2) W sekcji **Port Config** wybierz porty i skonfiguruj ich parametry.

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Interface Mode     | <p>Wybierz tryb interfejsu dla portu.</p> <p><b>Disable:</b> Wyłącz funkcję Auto VoIP na danym porcie.</p> <p><b>None:</b> Zezwól urządzeniom głosowym na korzystanie z własnych ustawień do transmisji głosowej.</p> <p><b>VLAN ID:</b> Urządzenia głosowe będą wysyłać pakiety voice z wybranym tagiem VLAN. Jeżeli wybierzesz ten tryb, uzupełnij pole VLAN ID.</p> <p>Ponadto, musisz także skonfigurować 802.1Q VLAN, aby odpowiednie porty mogły normalnie przesyłać pakiety.</p> <p><b>Dot1p:</b> Urządzenia głosowe będą wysyłać pakiety voice z wybranym priorytetem 802.1p. Jeżeli wybierzesz ten tryb, ustaw priorytet 802.1p w polu Value.</p> <p>Ponadto, musisz także skonfigurować usługę Class of Service, aby przełącznik przetwarzał pakiety zgodnie z priorytetem 802.1p.</p> <p><b>Untagged:</b> Urządzenia głosowe będą wysyłać nietagowane pakiety voice.</p> |
| Value              | Uzupełnij wartość ID VLAN lub priorytetu 802.1p dla portu, zgodnie z ustawieniami trybu interfejsu.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| CoS Override Mode  | <p>Włącz lub wyłącz tryb zastępowania usługi Class of Service.</p> <p><b>Enabled:</b> Włącz zastępowanie CoS. Przełącznik będzie ignorować priorytety 802.1p w pakietach voice, bezpośrednio umieszczając je w kolejce TC-5.</p> <p><b>Disabled:</b> Wyłącz zastępowanie CoS. Przełącznik będzie umieszczać pakiety voice w kolejkach TC zgodnie z priorytetami 802.1p pakietów.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Operational Status | Stan działania funkcji Voice VLAN na poziomie interfejsu. Aby funkcja działała poprawnie, włącz Voice VLAN zarówno globalnie, jak i na poziomie interfejsu.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| DSCP Value         | <p>Podaj wartość priorytetu DSCP. Urządzenie głosowe będzie przysyłać pakiety z odpowiednią wartością DSCP.</p> <p>Ponadto, możesz także skonfigurować Class of Service, aby przełącznik przetwarzał pakiety zgodnie z priorytetami DSCP.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |

3) Kliknij **Apply**.

## 5.2 Przez CLI

Wykonaj poniższe kroki, aby skonfigurować Auto VoIP:

|        |                                                                     |
|--------|---------------------------------------------------------------------|
| Krok 1 | <p><b>configure</b></p> <p>Uruchom tryb konfiguracji globalnej.</p> |
| Krok 2 | <p><b>auto-voip</b></p> <p>Uruchom globalnie Auto VoIP.</p>         |

- 
- Krok 3 **interface {fastEthernet *port* | range fastEthernet *port-list* | gigabitEthernet *port* | range gigabitEthernet *port-list* | ten-gigabitEthernet *port* | range ten-gigabitEthernet *port-list* | port-channel *port-channel-id* | range port-channel *port-channel-list*}**
- Uruchom tryb konfiguracji interfejsu.
- 
- Krok 4 Wybierz tryb interfejsu dla portu.
- no auto-voip**
- Gdy ustawisz tryb interfejsu jako disabled, funkcja Auto VoIP będzie wyłączona na danym porcie.
- auto-voip none**
- Gdy ustawisz tryb interfejsu jako none, przełącznik zezwoli urządzeniom głosowym na korzystanie z własnych ustawień do transmisji głosowej.
- auto-voip *vlan-id***
- Gdy ustawisz tryb interfejsu jako VLAN ID, urządzenia głosowe będą wysyłać pakiety voice z wybranym tagiem VLAN. Jeżeli wybierzesz ten tryb, uzupełnij pole VLAN ID. Prawidłowe wartości wahają się od 1 do 4093.
- Ponadto, musisz także skonfigurować 802.1Q VLAN, aby odpowiednie porty mogły normalnie przesyłać pakiety
- auto-voip dot1p *dot1p***
- Gdy ustawisz tryb interfejsu jako dot1p, urządzenia głosowe będą wysyłać pakiety voice z wybranym priorytetem 802.1p. Jeżeli wybierzesz ten tryb, ustaw priorytet 802.1p w polu Value. Prawidłowe wartości wahają się od 0 do 7.
- Ponadto, musisz także skonfigurować usługę Class of Service, aby przełącznik przetwarzał pakiety zgodnie z priorytetem 802.1p.
- auto-voip untagged**
- Gdy ustawisz tryb interfejsu jako untagged, urządzenia głosowe będą wysyłać nietagowane pakiety voice.
- 
- Krok 5 **auto-voip data priority {trust | untrust}**
- Włącz lub wyłącz tryb zastępowania usługi Class of Service. Domyślnie ustawioną opcją jest trust, co oznacza, że zastępowanie Class of Service jest wyłączone.
- trust:** W tym trybie przełącznik będzie umieszczać pakiety voice w kolejkach TC zgodnie z priorytetami 802.1p pakietów.
- untrust:** W tym trybie przełącznik będzie ignorować priorytety 802.1p w pakietach voice, bezpośrednio umieszczając je w kolejce TC-5.
- 
- Krok 6 **auto-voip dscp *value***
- Podaj wartość priorytetu DSCP. Urządzenie głosowe będzie przysyłać pakiety z odpowiednią wartością DSCP.
- Ponadto, możesz także skonfigurować Class of Service, aby przełącznik przetwarzał pakiety zgodnie z priorytetami DSCP.
- value:** Uzupełnij wartość priorytetu DSCP. Prawidłowe wartości wahają się od 0 do 63, a wartością domyślną jest 0.
-

- 
- Krok 7     **show auto-voip**  
Sprawdź globalny stan Auto VoIP.
- 
- Krok 8     **show auto-voip interface**  
Przejrzyj konfigurację Auto VoIP dla portów.
- 
- Krok 8     **end**  
Powróć do trybu privileged EXEC.
- 
- Krok 9     **copy running-config startup-config**  
Zapisz ustawienia w pliku konfiguracyjnym.
- 

Poniższy schemat przedstawia przykładowy sposób ustawiania trybu interfejsu jako dot1p, priorytetu 802.1p jako 4, priorytetu DSCP jako 10 i włączania trybu zastępowania CoS dla portu 1/0/3:

**Switch#configure**

**Switch(config)#auto-voip**

**Switch(config)#interface gigabitEthernet 1/0/3**

**Switch(config-if)#auto-voip dot1p 4**

**Switch(config-if)#auto-voip dscp 10**

**Switch(config-if)#auto-voip data priority untrust**

**Switch(config-if)#show auto-voip**

Administrative Mode: Enabled

**Switch(config-if)#show auto-voip interface**

Interface.Gi1/0/1

Auto-VoIP Interface Mode.       Disabled

Auto-VoIP COS Override.       False

Auto-VoIP DSCP Value.       0

Auto-VoIP Port Status.       Disabled

Interface.Gi1/0/2

Auto-VoIP Interface Mode.       Disabled

Auto-VoIP COS Override.       False

Auto-VoIP DSCP Value.       0

Auto-VoIP Port Status.       Disabled

```
Interface.Gi1/0/3
Auto-VoIP Interface Mode. Enabled
Auto-VoIP Priority. 4
Auto-VoIP COS Override. True
Auto-VoIP DSCP Value. 10
Auto-VoIP Port Status. Enabled
```

```
.....
```

```
Switch(config-if)#end
```

```
Switch#copy running-config startup-config
```

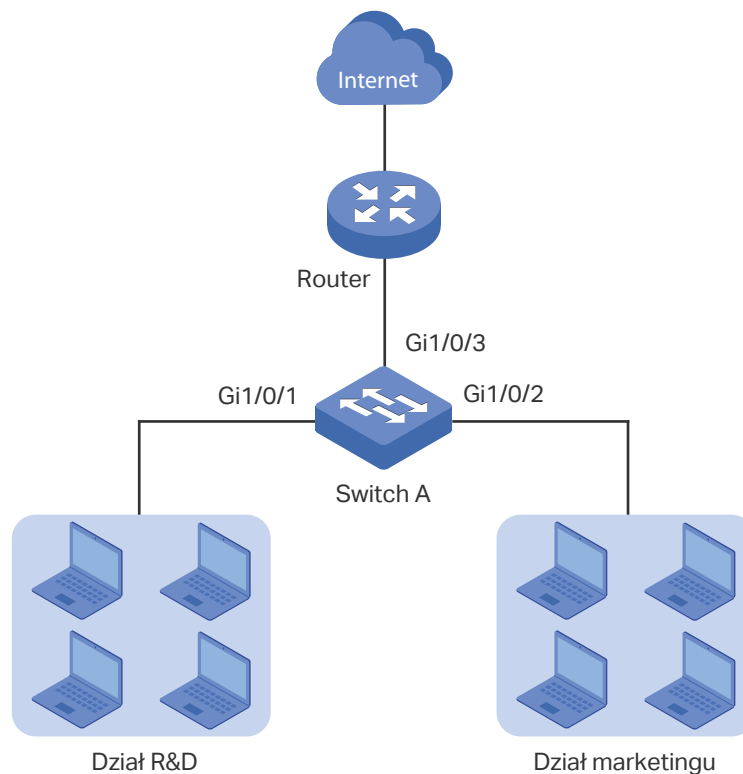
# 6 Przykłady konfiguracji

## 6.1 Przykład dla usług Class of Service

### 6.1.1 Wymagania sieciowe

Jak pokazano poniżej, zarówno dział R&D, jak i dział marketingu mają dostęp do Internetu. Wymaga się, aby w sytuacji, gdy wystąpi zator, przysłany mógł być ruch z obydwu działów, ale ruch z działu marketingu powinien mieć pierwszeństwo.

Rys. 6-1 Topologia zastosowania QoS



### 6.1.2 Schemat konfiguracji

Aby spełnić przedstawiony wymóg, należy skonfigurować funkcję Port Priority, aby pakiety z działu marketingu należały do kolejki o wyższym priorytecie niż pakiety z działu R&D.

- 1) Ustaw tryb zaufania portu 1/0/1 i 1/0/2 jako untrusted i ustaw mapowanie portów do różnych kolejek.
- 2) Ustaw typ harmonogramu kolejek jako weighted dla portu 1/0/3 i podaj wartość wagi kolejki, aby ruch z działu marketingu mógł mieć pierwszeństwo.

W poniższych podrozdziałach opisano dwa sposoby przeprowadzenia procedury konfiguracji: przez GUI oraz przez CLI.

### 6.1.3 Przez GUI

- 1) Wybierz z menu **QoS > Class of Service > Port Priority**, aby wyświetlić poniższą stronę. Ustaw trust mode portu 1/0/1 i 1/0/2 jako untrusted. Ustaw 802.1p priority portu 1/0/1 jako 1 i 802.1p priority portu 1/0/2 jako 0. Kliknij **Apply**.

Rys. 6-2 Konfiguracja Port Priority

Port Priority Config

| UNIT1                               |        | LAGS            |            |     |
|-------------------------------------|--------|-----------------|------------|-----|
| <input type="checkbox"/>            | Port   | 802.1p Priority | Trust Mode | LAG |
| <input checked="" type="checkbox"/> | 1/0/1  | 1               | Untrusted  | --  |
| <input type="checkbox"/>            | 1/0/2  | 0               | Untrusted  | --  |
| <input type="checkbox"/>            | 1/0/3  | 0               | Untrusted  | --  |
| <input type="checkbox"/>            | 1/0/4  | 0               | Untrusted  | --  |
| <input type="checkbox"/>            | 1/0/5  | 0               | Untrusted  | --  |
| <input type="checkbox"/>            | 1/0/6  | 0               | Untrusted  | --  |
| <input type="checkbox"/>            | 1/0/7  | 0               | Untrusted  | --  |
| <input type="checkbox"/>            | 1/0/8  | 0               | Untrusted  | --  |
| <input type="checkbox"/>            | 1/0/9  | 0               | Untrusted  | --  |
| <input type="checkbox"/>            | 1/0/10 | 0               | Untrusted  | --  |

Total: 10      1 entry selected.           

- 2) Wybierz z menu **QoS > Class of Service > 802.1p Priority**, aby wyświetlić poniższą stronę. Mapuj 802.1p priority 0 do TC-1 oraz 802.1p priority 1 do TC-0. Kliknij **Apply**.



Rys. 6-3 Konfiguracja mapowania 802.1p do kolejki

| 802.1p Priority | Queue |
|-----------------|-------|
| 0:              | TC-1  |
| 1:              | TC-0  |
| 2:              | TC-2  |
| 3:              | TC-3  |
| 4:              | TC-4  |
| 5:              | TC-5  |
| 6:              | TC-6  |
| 7:              | TC-7  |

Apply

| 802.1p Priority | Remap |
|-----------------|-------|
| 0:              | 0     |
| 1:              | 1     |
| 2:              | 2     |
| 3:              | 3     |
| 4:              | 4     |
| 5:              | 5     |
| 6:              | 6     |
| 7:              | 7     |

Apply

- Wybierz z menu **QoS > Class of Service > Scheduler Settings**, aby wyświetlić poniższą stronę. Wybierz port 1/0/3 i ustaw scheduler type TC-0 i TC-1 jako Weighted. Ustaw queue weight TC-0 jako 1, a TC-1 jako 5. Kliknij **Apply**.

Rys. 6-4 Konfiguracja kolejki ruchu wychodzącego

Scheduler Config

UNIT1 LAGS


1 2 3 4 5 6 7 8 9 10

Selected Unselected Not Available

Port 1/0/3

| <input type="checkbox"/>            | Queue TC-id | Scheduler Type | Queue Weight | Management Type |
|-------------------------------------|-------------|----------------|--------------|-----------------|
| <input type="checkbox"/>            | 0           | Weighted       | 1            | Taildrop        |
| <input checked="" type="checkbox"/> | 1           | Weighted       | 5            | Taildrop        |
| <input type="checkbox"/>            | 2           | Weighted       | 1            | Taildrop        |
| <input type="checkbox"/>            | 3           | Weighted       | 1            | Taildrop        |
| <input type="checkbox"/>            | 4           | Weighted       | 1            | Taildrop        |
| <input type="checkbox"/>            | 5           | Weighted       | 1            | Taildrop        |
| <input type="checkbox"/>            | 6           | Weighted       | 1            | Taildrop        |
| <input type="checkbox"/>            | 7           | Weighted       | 1            | Taildrop        |

Total: 8 1 entry selected. Cancel Apply

- 4) Kliknij  Save, aby zapisać ustawienia.

## 6.1.4 Przez CLI

- 1) Ustaw trust mode portu 1/0/1 jako untrusted oraz 802.1p priority jako 1.

```
Switch_A#configure
```

```
Switch_A(config)#interface gigabitEthernet 1/0/1
```

```
Switch_A(config-if)#qos trust mode untrust
```

```
Switch_A(config-if)#qos port-priority 1
```

```
Switch_A(config-if)#exit
```

- 2) Ustaw trust mode portu 1/0/2 jako untrusted oraz 802.1p priority jako 0.

```
Switch_A(config)#interface gigabitEthernet 1/0/2
```

```
Switch_A(config-if)#qos trust mode untrust
```

```
Switch_A(config-if)#qos port-priority 0
```

```
Switch_A(config-if)#exit
```

- 3) Mapuj 802.1p priority 0 do TC-1 oraz 802.1p priority 1 do TC-0.

```
Switch_A(config)#qos cos-map 0 1
```

```
Switch_A(config)#qos cos-map 1 0
```

- 4) Ustaw scheduler type TC-0 i TC-1 jako Weighted dla portu 1/0/3 ruchu wychodzącego. Ustaw queue weight TC-0 jako 1, a TC-1 jako 5.

```
Switch_A(config)#interface gigabitEthernet 1/0/3
Switch_A(config-if)#qos queue 0 mode wrr weight 1
Switch_A(config-if)#qos queue 1 mode wrr weight 5
Switch_A(config-if)#end
Switch_A#copy running-config startup-config
```

### Sprawdzanie konfiguracji

Sprawdzanie trybu trust portu:

```
Switch_A#show qos trust interface
```

| Port    | Trust Mode | LAG   |
|---------|------------|-------|
| -----   | -----      | ----- |
| Gi1/0/1 | untrust    | N/A   |
| Gi1/0/2 | untrust    | N/A   |
| Gi1/0/3 | untrust    | N/A   |
| Gi1/0/4 | untrust    | N/A   |
| ...     |            |       |

Sprawdzanie mapowania portu do 802.1p:

```
Switch_A#show qos port-priority interface
```

| Port    | CoS Value | LAG   |
|---------|-----------|-------|
| -----   | -----     | ----- |
| Gi1/0/1 | CoS 1     | N/A   |
| Gi1/0/2 | CoS 0     | N/A   |
| Gi1/0/3 | CoS 0     | N/A   |
| Gi1/0/4 | CoS 0     | N/A   |
| ...     |           |       |

Sprawdzanie mapowania 802.1p do kolejki:

```
Switch_A#show qos cos-map
```

```
-----+-----+-----+-----+-----+-----+-----+-----+-----
Dot1p Value |0 |1 |2 |3 |4 |5 |6 |7
-----+-----+-----+-----+-----+-----+-----+-----+-----
TC |TC1 |TC0 |TC2 |TC4 |TC4 |TC5 |TC6 |TC7
-----+-----+-----+-----+-----+-----+-----+-----+-----
```

Verify the scheduler mode of the egress port:

```
Switch_A#show qos queue interface gigabitEthernet 1/0/3
```

```
Gi1/0/3----LAG: N/A
```

```
Queue Schedule Mode Weight
```

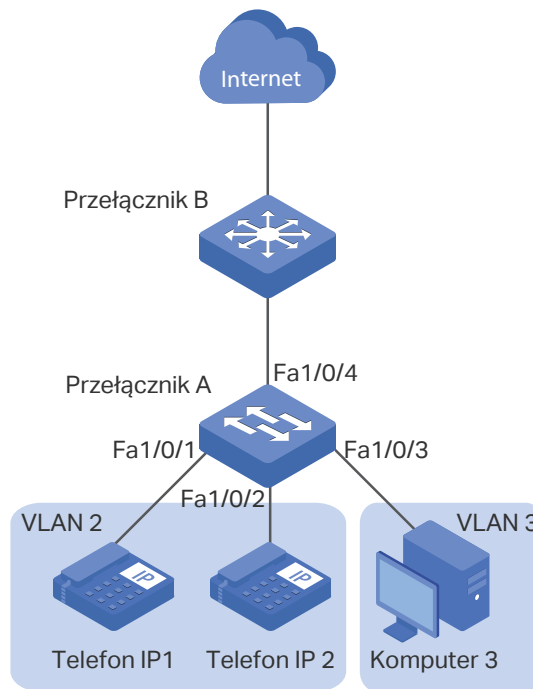
```
----- ----- -----
TC0 WRR 1
TC1 WRR 5
TC2 WRR 1
TC3 WRR 1
TC4 WRR 1
TC5 WRR 1
TC6 WRR 1
TC7 WRR 1
```

## 6.2 Przykład dla usługi Voice VLAN

### 6.2.1 Wymagania sieciowe

Jak pokazano poniżej, firma planuje instalację telefonów IP na powierzchni biura. W celu zapewnienia dobrej jakości transmisji głosu, telefony IP i komputery muszą być podłączone do innych portów przełącznika, a ruch głosowy wymaga wyższego priorytetu niż ruch danych.

Rys. 6-5 Topologia zastosowania Voice VLAN



## 6.2.2 Schemat konfiguracji

Aby spełnić przedstawiony wymóg, należy skonfigurować Voice VLAN, aby mieć pewność, że ruch głosowy może być przesyłany w tym samym VLAN-ie, natomiast ruch danych w innym VLAN-ie. Ponadto konieczne jest ustalenie priorytetu, aby ruch głosowy mógł mieć pierwszeństwo w razie natężonego ruchu w sieci.

- 1) Skonfiguruj 802.1Q VLAN dla portu 1/0/1, 1/0/2, 1/0/3 oraz 1/0/4.
- 2) Skonfiguruj funkcję Voice VLAN na porcie 1/0/1 oraz 1/0/2.

W poniższych podrozdziałach opisano dwa sposoby przeprowadzenia procedury konfiguracji: przez GUI oraz przez CLI.

## 6.2.3 Przez GUI

- 1) Wybierz z menu **L2 FEATURES > VLAN > 802.1Q VLAN > VLAN Config** i kliknij  **Add** aby wyświetlić poniższą stronę. Utwórz VLAN 2 i dodaj nietagowane porty 1/0/1, 1/0/2 i 1/0/4 do VLAN 2. Kliknij **Create**.

Rys. 6-6 Konfiguracja VLAN 2

### VLAN Config

VLAN ID:  (2-4094, format: 2,4-5,8)

VLAN Name:  (1-16 characters)

#### Untagged Ports

Port:  (Format: 1/0/1, input or choose below)

Select All

**UNIT1**      **LAGS**

1    2    3    4    5    6    7    8    9    10

Selected    Unselected    Not Available


#### Tagged Ports

Port:  (Format: 1/0/1, input or choose below)

Select All

**UNIT1**      **LAGS**

1    2    3    4    5    6    7    8    9    10

- 2) Kliknij  **Add**, aby wyświetlić poniższą stronę. Utwórz VLAN 3 i dodaj nietagowane porty 1/0/3 i 1/0/4 do VLAN 3. Kliknij **Create**.

Rys. 6-7 Konfiguracja VLAN 3

### VLAN Config

VLAN ID:  (2-4094, format: 2,4-5,8)

VLAN Name:  (1-16 characters)

#### Untagged Ports

Port:  (Format: 1/0/1, input or choose below)

Select All

UNIT1      LAGS

1    2    3    4    5    6    7    8    9    10

Selected    Unselected    Not Available

#### Tagged Ports

Port:  (Format: 1/0/1, input or choose below)

Select All

UNIT1      LAGS

1    2    3    4    5    6    7    8    9    10

- Wybierz z menu **L2 FEATURES > VLAN > 802.1Q VLAN > Port Config**, aby wyświetlić poniższą stronę. Wyłącz funkcję Ingress Checking na portach 1/0/1 i 1/0/2 oraz ustaw PVID jako 2. Kliknij **Apply**.

Rys. 6-8 Ustawianie parametrów portu

Port Config

UNIT1 LAGS

| <input type="checkbox"/>            | Port   | PVID | Ingress Checking | Acceptable Frame Types | LAG | Details |
|-------------------------------------|--------|------|------------------|------------------------|-----|---------|
| <input checked="" type="checkbox"/> | 1/0/1  | 2    | Disable          | Admit All              | --- | Details |
| <input checked="" type="checkbox"/> | 1/0/2  | 2    | Disable          | Admit All              | --- | Details |
| <input type="checkbox"/>            | 1/0/3  | 1    | Enabled          | Admit All              | --- | Details |
| <input type="checkbox"/>            | 1/0/4  | 1    | Enabled          | Admit All              | --- | Details |
| <input type="checkbox"/>            | 1/0/5  | 1    | Enabled          | Admit All              | --- | Details |
| <input type="checkbox"/>            | 1/0/6  | 1    | Enabled          | Admit All              | --- | Details |
| <input type="checkbox"/>            | 1/0/7  | 1    | Enabled          | Admit All              | --- | Details |
| <input type="checkbox"/>            | 1/0/8  | 1    | Enabled          | Admit All              | --- | Details |
| <input type="checkbox"/>            | 1/0/9  | 1    | Enabled          | Admit All              | --- | Details |
| <input type="checkbox"/>            | 1/0/10 | 1    | Enabled          | Admit All              | --- | Details |

Total: 10 2 entries selected. Cancel Apply

- 4) Wybierz z menu **QoS > Voice VLAN > OUI Config**, aby wyświetlić poniższą stronę. Sprawdź tabelę OUI.

Rys. 6-9 Sprawdzanie tabeli OUI

OUI Config

UNIT1 + Add - Delete

| <input type="checkbox"/> | OUI      | Status  | Description |
|--------------------------|----------|---------|-------------|
| <input type="checkbox"/> | 00:01:E3 | Default | SIEMENS     |
| <input type="checkbox"/> | 00:03:6B | Default | CISCO1      |
| <input type="checkbox"/> | 00:12:43 | Default | CISCO2      |
| <input type="checkbox"/> | 00:0F:E2 | Default | H3C         |
| <input type="checkbox"/> | 00:60:B9 | Default | NITSUKO     |
| <input type="checkbox"/> | 00:D0:1E | Default | PINTEL      |
| <input type="checkbox"/> | 00:E0:75 | Default | VERILINK    |
| <input type="checkbox"/> | 00:E0:BB | Default | 3COM        |
| <input type="checkbox"/> | 00:04:0D | Default | AVAYA1      |
| <input type="checkbox"/> | 00:1B:4F | Default | AVAYA2      |

Total: 11

- 5) Wybierz z menu **QoS > Voice VLAN > Global Config**, aby wyświetlić poniższą stronę. Włącz globalnie Voice VLAN. Ustaw VLAN ID jako 2, a priorytet jako 7. Kliknij **Apply**.



Rys. 6-10 Konfiguracja globalna Voice VLAN

Global Config

Voice VLAN:  Enable

VLAN ID:  (2-4094)

Priority:

- 6) Wybierz z menu **QoS > Voice VLAN > Port Config**, aby wyświetlić poniższą stronę. Włącz Voice VLAN na portach 1/0/1 i 1/0/2. Kliknij **Apply**.


Rys. 6-11 Włączanie Voice VLAN na portach

Port Config

UNIT1 LAGS

| <input type="checkbox"/>            | Port   | Voice VLAN | Operational Status |
|-------------------------------------|--------|------------|--------------------|
| <input checked="" type="checkbox"/> | 1/0/1  | Enabled    | Inactive           |
| <input checked="" type="checkbox"/> | 1/0/2  | Enabled    | Inactive           |
| <input type="checkbox"/>            | 1/0/3  | Disabled   | Inactive           |
| <input type="checkbox"/>            | 1/0/4  | Disabled   | Inactive           |
| <input type="checkbox"/>            | 1/0/5  | Disabled   | Inactive           |
| <input type="checkbox"/>            | 1/0/6  | Disabled   | Inactive           |
| <input type="checkbox"/>            | 1/0/7  | Disabled   | Inactive           |
| <input type="checkbox"/>            | 1/0/8  | Disabled   | Inactive           |
| <input type="checkbox"/>            | 1/0/9  | Disabled   | Inactive           |
| <input type="checkbox"/>            | 1/0/10 | Disabled   | Inactive           |

Total: 10 2 entries selected.

- 7) Kliknij  **Save**, aby zapisać ustawienia.

## 6.2.4 Przez CLI

- 1) Utwórz VLAN 2 i dodaj nietagowane porty 1/0/1, 1/0/2 i 1/0/4 do VLAN 2.

```
Switch_A#configure
```

```
Switch_A(config)#vlan 2
```

```
Switch_A(config-vlan)#name VoiceVLAN
```

```
Switch_A(config-vlan)#exit
```

```
Switch_A(config)#interface gigabitEthernet 1/0/1
```

```
Switch_A(config-if)#switchport general allowed vlan 2 untagged
```

```
Switch_A(config-if)#exit
```

```
Switch_A(config)#interface gigabitEthernet 1/0/2
```

```
Switch_A(config-if)#switchport general allowed vlan 2 untagged
Switch_A(config-if)#exit
```

```
Switch_A(config)#interface gigabitEthernet 1/0/4
```

```
Switch_A(config-if)#switchport general allowed vlan 2 untagged
Switch_A(config-if)#exit
```

- 2) Utwórz VLAN 3 i dodaj nietagowane porty 1/0/3 i 1/0/4 do VLAN 3.

```
Switch_A(config)#vlan 3
```

```
Switch_A(config-vlan)#name VLAN3
```

```
Switch_A(config-vlan)#exit
```

```
Switch_A(config)#interface gigabitEthernet 1/0/3
```

```
Switch_A(config-if)#switchport general allowed vlan 3 untagged
Switch_A(config-if)#exit
```

```
Switch_A(config)#interface gigabitEthernet 1/0/4
```

```
Switch_A(config-if)#switchport general allowed vlan 3 untagged
Switch_A(config-if)#exit
```

- 3) Wyłącz funkcję Ingress Checking na portach 1/0/1 i 1/0/2 oraz ustaw PVID jako 2.

```
Switch_A(config)#interface gigabitEthernet 1/0/1
```

```
Switch_A(config-if)#no switchport check ingress
```

```
Switch_A(config-if)#switchport pvid 2
```

```
Switch_A(config-if)#exit
```

```
Switch_A(config)#interface gigabitEthernet 1/0/2
```

```
Switch_A(config-if)#no switchport check ingress
```

```
Switch_A(config-if)#switchport pvid 2
```

```
Switch_A(config-if)#exit
```

- 4) Sprawdź tabelę OUI.

```
Switch(config)#show voice vlan oui
```

```
00:01:E3 Default SIEMENS
```

```
00:03:6B Default CISCO1
```

```
00:12:43 Default CISCO2
```

```
00:0F:E2 Default H3C
```

```
00:60:B9 Default NITSUKO
```

```

00:D0:1E Default PINTEL
00:E0:75 Default VERILINK
00:E0:BB Default 3COM
00:04:0D Default AVAYA1
00:1B:4F Default AVAYA2
00:04:13 Default SNOM

```

- 5) Włącz globalnie Voice VLAN. Ustaw VLAN ID jako 2 i ustaw priority jako 7.

```

Switch_A(config)#voice vlan 2
Switch_A(config)#voice vlan priority 7

```

- 6) Włącz Voice VLAN na portach 1/0/1 i 1/0/2.

```

Switch_A(config)#interface gigabitEthernet 1/0/1
Switch_A(config-if)#voice vlan
Switch_A(config-if)#exit
Switch_A(config)#interface gigabitEthernet 1/0/2
Switch_A(config-if)#voice vlan
Switch_A(config-if)#end
Switch_A#copy running-config startup-config

```

## Sprawdzanie konfiguracji

Sprawdzanie podstawowej konfiguracji VLAN:

```
Switch_A(config)#show vlan brief
```

| VLAN | Name        | Status | Ports                                                                                           |
|------|-------------|--------|-------------------------------------------------------------------------------------------------|
| 1    | System-VLAN | active | Gi1/0/1, Gi1/0/2, Gi1/0/3, Gi1/0/4,<br>Gi1/0/5, Gi1/0/6, Gi1/0/7, Gi1/0/8,<br>Gi1/0/9, Gi1/0/10 |
| 2    | VoiceVLAN   | active | Gi1/0/1, Gi1/0/2, Gi1/0/4                                                                       |
| 3    | VLAN3       | active | Gi1/0/3, Gi1/0/4                                                                                |

Sprawdzanie konfiguracji Voice VLAN:

```
Switch_A(config)#show voice vlan interface
```

Voice VLAN ID        2  
 Priority                7

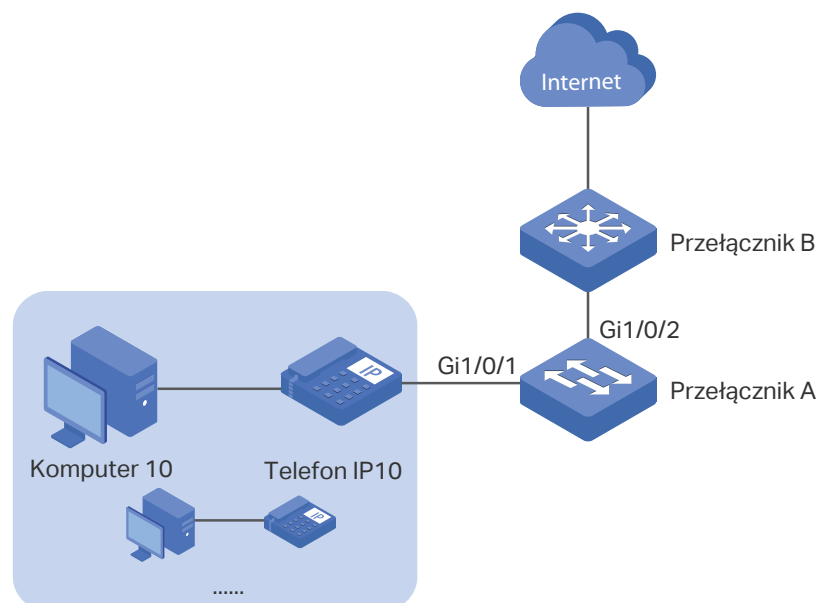
| Interface | Voice VLAN Mode | Operational Status | LAG |
|-----------|-----------------|--------------------|-----|
| -----     | -----           | -----              | --- |
| Gi1/0/1   | enabled         | Up                 | N/A |
| Gi1/0/2   | enabled         | Up                 | N/A |
| Gi1/0/3   | disabled        | Down               | N/A |
| Gi1/0/4   | disabled        | Down               | N/A |
| Gi1/0/5   | disabled        | Down               | N/A |
| ...       |                 |                    |     |
| Gi1/0/10  | disabled        | Down               | N/A |

## 6.3 Przykład dla usługi Auto VoIP

### 6.3.1 Wymagania sieciowe

Jak pokazano poniżej, firma planuje zainstalowanie telefonów IP na powierzchni biurowej. Telefony IP muszą korzystać z tych samych portów co komputery, ponieważ nie ma dostępnych innych portów dla telefonów IP. W celu zapewnienia dobrej jakości transmisji głosu, ruch głosowy musi mieć wyższy priorytet niż ruch danych.

Rys. 6-12 Topologia zastosowania Auto VoIP



## 6.3.2 Schemat konfiguracji

Aby umożliwić optymalizację ruchu głosowego, skonfiguruj Auto VoIP i LLDP-MED w taki sposób, aby telefony IP musiały przysyłać ruch z określonym priorytetem DSCP. Ruch głosowy może być w ten sposób kierowany do wybranej kolejki, a ruch danych do innej kolejki, zgodnie z konfiguracją Class of Service. Upewnij się, że ruch głosowy ma pierwszeństwo w razie natężonego ruchu w sieci.

- 1) Włącz funkcję Auto VoIP i skonfiguruj wartość DSCP portów.
- 2) Skonfiguruj Class of Service.
- 3) Włącz LLDP-MED i skonfiguruj odpowiednie parametry.

W poniższych podrozdziałach opisano dwa sposoby przeprowadzenia procedury konfiguracji: przez GUI oraz przez CLI.

### 6.3.3 Przez GUI

Konfiguracja Auto VoIP dla portu 1/0/1 i dla innych portów podłączonych do telefonu IP jest taka sama. Poniższą procedurę konfiguracji omówimy na przykładzie portu 1/0/1.

- 1) Wybierz z menu **QoS > Auto VoIP**, aby wyświetlić poniższą stronę. Włącz globalnie Auto VoIP i ustaw wartość DSCP portu 1/0/1 jako 63. Kliknij **Apply**.

Rys. 6-13 Konfiguracja Auto VoIP

Global Config

Auto VoIP:  Enable Apply

Port Config

| UNIT1                               |        |                |       |                   |                    |            |  |
|-------------------------------------|--------|----------------|-------|-------------------|--------------------|------------|--|
| <input type="checkbox"/>            | Port   | Interface Mode | Value | CoS Override Mode | Operational Status | DSCP Value |  |
| <input checked="" type="checkbox"/> | 1/0/1  | Disable        | 0     | Disabled          | Disabled           | 63         |  |
| <input type="checkbox"/>            | 1/0/2  | Disable        | 0     | Disabled          | Disabled           | 0          |  |
| <input type="checkbox"/>            | 1/0/3  | Disable        | 0     | Disabled          | Disabled           | 0          |  |
| <input type="checkbox"/>            | 1/0/4  | Disable        | 0     | Disabled          | Disabled           | 0          |  |
| <input type="checkbox"/>            | 1/0/5  | Disable        | 0     | Disabled          | Disabled           | 0          |  |
| <input type="checkbox"/>            | 1/0/6  | Disable        | 0     | Disabled          | Disabled           | 0          |  |
| <input type="checkbox"/>            | 1/0/7  | Disable        | 0     | Disabled          | Disabled           | 0          |  |
| <input type="checkbox"/>            | 1/0/8  | Disable        | 0     | Disabled          | Disabled           | 0          |  |
| <input type="checkbox"/>            | 1/0/9  | Disable        | 0     | Disabled          | Disabled           | 0          |  |
| <input type="checkbox"/>            | 1/0/10 | Disable        | 0     | Disabled          | Disabled           | 0          |  |

Total: 10 1 entry selected. Cancel Apply

- 2) Wybierz z menu **QoS > Class of Service > Port Priority**, aby wyświetlić poniższą stronę. Ustaw tryb trust portu 1/0/1 jako trust DSCP. Kliknij **Apply**.

Rys. 6-14 Konfiguracja Port Priority

Port Priority Config

UNIT1 LAGS

| <input type="checkbox"/>            | Port   | 802.1p Priority | Trust Mode | LAG |
|-------------------------------------|--------|-----------------|------------|-----|
| <input checked="" type="checkbox"/> | 1/0/1  | 0               | Trust DSCP | --  |
| <input type="checkbox"/>            | 1/0/2  | 0               | Untrusted  | --  |
| <input type="checkbox"/>            | 1/0/3  | 0               | Untrusted  | --  |
| <input type="checkbox"/>            | 1/0/4  | 0               | Untrusted  | --  |
| <input type="checkbox"/>            | 1/0/5  | 0               | Untrusted  | --  |
| <input type="checkbox"/>            | 1/0/6  | 0               | Untrusted  | --  |
| <input type="checkbox"/>            | 1/0/7  | 0               | Untrusted  | --  |
| <input type="checkbox"/>            | 1/0/8  | 0               | Untrusted  | --  |
| <input type="checkbox"/>            | 1/0/9  | 0               | Untrusted  | --  |
| <input type="checkbox"/>            | 1/0/10 | 0               | Untrusted  | --  |

Total: 10 1 entry selected. Cancel Apply

- 2) Wybierz z menu **QoS > Class of Service > DSCP Priority**, aby wyświetlić poniższą stronę. Ustaw 802.1p priority jako 7 dla priorytetu 63 DSCP. Kliknij **Apply**.

Rys. 6-15 Ustawianie 802.1p priority dla priorytetu 63 DSCP

DSCP Priority Config

| <input type="checkbox"/>            | DSCP Priority | 802.1p Priority | DSCP Remap      |
|-------------------------------------|---------------|-----------------|-----------------|
| <input type="checkbox"/>            | 54            | 6               | 54              |
| <input type="checkbox"/>            | 55            | 6               | 55              |
| <input type="checkbox"/>            | 56            | 7               | 56 cs7 (111000) |
| <input type="checkbox"/>            | 57            | 7               | 57              |
| <input type="checkbox"/>            | 58            | 7               | 58              |
| <input type="checkbox"/>            | 59            | 7               | 59              |
| <input type="checkbox"/>            | 60            | 7               | 60              |
| <input type="checkbox"/>            | 61            | 7               | 61              |
| <input type="checkbox"/>            | 62            | 7               | 62              |
| <input checked="" type="checkbox"/> | 63            | 7               | 63              |

Total: 64 1 entry selected. Cancel Apply

- 3) Ustaw 802.1p priority jako 5 dla innych priorytetów DSCP. Kliknij **Apply**.

Rys. 6-16 Ustawianie 802.1p priority dla innych priorytetów DSCP

DSCP Priority Config

| <input type="checkbox"/>            | DSCP Priority | 802.1p Priority | DSCP Remap      |
|-------------------------------------|---------------|-----------------|-----------------|
|                                     |               | 5               |                 |
| <input checked="" type="checkbox"/> | 54            | 5               | 54              |
| <input checked="" type="checkbox"/> | 55            | 5               | 55              |
| <input checked="" type="checkbox"/> | 56            | 5               | 56 cs7 (111000) |
| <input checked="" type="checkbox"/> | 57            | 5               | 57              |
| <input checked="" type="checkbox"/> | 58            | 5               | 58              |
| <input checked="" type="checkbox"/> | 59            | 5               | 59              |
| <input checked="" type="checkbox"/> | 60            | 5               | 60              |
| <input checked="" type="checkbox"/> | 61            | 5               | 61              |
| <input checked="" type="checkbox"/> | 62            | 5               | 62              |
| <input type="checkbox"/>            | 63            | 7               | 63              |

Total: 64      63 entries selected.     

- 4) Wybierz z menu **QoS > Class of Service > Scheduler Settings**, aby wyświetlić poniższą stronę. Zaznacz port 1/0/2. Ustaw tryb scheduler jako weighted, a queue weight jako 1 dla TC-5. Kliknij **Apply**.

Rys. 6-17 Konfiguracja TC-5 dla portu

Scheduler Config

UNIT1      LAGS

1 2 3 4 5 6 7 8 9 10

Selected       Unselected       Not Available

Port 1/0/2

| <input type="checkbox"/>            | Queue TC-id | Scheduler Type | Queue Weight | Management Type |
|-------------------------------------|-------------|----------------|--------------|-----------------|
|                                     |             | Weighted       | 1            |                 |
| <input type="checkbox"/>            | 0           | Weighted       | 1            | Taildrop        |
| <input type="checkbox"/>            | 1           | Weighted       | 1            | Taildrop        |
| <input type="checkbox"/>            | 2           | Weighted       | 1            | Taildrop        |
| <input type="checkbox"/>            | 3           | Weighted       | 1            | Taildrop        |
| <input type="checkbox"/>            | 4           | Weighted       | 1            | Taildrop        |
| <input checked="" type="checkbox"/> | 5           | Weighted       | 1            | Taildrop        |
| <input type="checkbox"/>            | 6           | Weighted       | 1            | Taildrop        |
| <input type="checkbox"/>            | 7           | Weighted       | 1            | Taildrop        |

Total: 8      1 entry selected.     

- 5) Zaznacz port 1/0/2. Ustaw tryb scheduler jako weighted, a queue weight jako 10 dla TC-7. Kliknij **Apply**.

Rys. 6-18 Konfiguracja TC-7 dla portu

Scheduler Config

UNIT1 LAGS

1 2 3 4 5 6 7 8 9 10

Selected Unselected Not Available

Port 1/0/2

| <input type="checkbox"/>            | Queue TC-id | Scheduler Type | Queue Weight | Management Type |
|-------------------------------------|-------------|----------------|--------------|-----------------|
| <input type="checkbox"/>            |             | Weighted       | 10           |                 |
| <input type="checkbox"/>            | 0           | Weighted       | 1            | Taildrop        |
| <input type="checkbox"/>            | 1           | Weighted       | 1            | Taildrop        |
| <input type="checkbox"/>            | 2           | Weighted       | 1            | Taildrop        |
| <input type="checkbox"/>            | 3           | Weighted       | 1            | Taildrop        |
| <input type="checkbox"/>            | 4           | Weighted       | 1            | Taildrop        |
| <input type="checkbox"/>            | 5           | Weighted       | 1            | Taildrop        |
| <input type="checkbox"/>            | 6           | Weighted       | 1            | Taildrop        |
| <input checked="" type="checkbox"/> | 7           | Weighted       | 10           | Taildrop        |

Total: 8 1 entry selected. Cancel Apply

- 6) Wybierz z menu **L2 FEATURES > LLDP > LLDP-MED Config > Port Config** i kliknij Detail przy porcie 1/0/1, aby wyświetlić poniższą stronę. Zaznacz wszystkie pola wyboru dla TLV. Kliknij **Save**.



Rys. 6-19 Konfiguracja TLV

Included TLVs Detail(Port: 1/0/1)

Included TLVs

All  
 Network Policy     Location Identification     Extended Power-Via-MDI     Inventory

Location Identification Parameters

Emergency Number     Civic Address

What:  ▼

Country Code:  ▼

Language:  Chars. (0-255)

Province/State:  Chars. (0-255)

City/Township:  Chars. (0-255)

County/Parish/District:  Chars. (0-255)

Street:  Chars. (0-255)

House Number:  Chars. (0-255)

Name:  Chars. (0-255)

Postal/Zip Code:  Chars. (0-255)

Room Number:  Chars. (0-255)

- 7) Wybierz z menu **L2 FEATURES > LLDP > LLDP-MED Config > Port Config**, aby wyświetlić poniższą stronę. Włącz LLDP-MED na porcie 1/0/1. Kliknij **Apply**.


Rys. 6-20 Włączanie LLDP-MED na porcie

Port Config

UNIT1

| <input type="checkbox"/>            | Port   | LLDP-MED Status         | Included TLVs          |
|-------------------------------------|--------|-------------------------|------------------------|
| <input checked="" type="checkbox"/> | 1/0/1  | Enable <small>▼</small> | <a href="#">Detail</a> |
| <input type="checkbox"/>            | 1/0/2  | Disabled                | <a href="#">Detail</a> |
| <input type="checkbox"/>            | 1/0/3  | Disabled                | <a href="#">Detail</a> |
| <input type="checkbox"/>            | 1/0/4  | Disabled                | <a href="#">Detail</a> |
| <input type="checkbox"/>            | 1/0/5  | Disabled                | <a href="#">Detail</a> |
| <input type="checkbox"/>            | 1/0/6  | Disabled                | <a href="#">Detail</a> |
| <input type="checkbox"/>            | 1/0/7  | Disabled                | <a href="#">Detail</a> |
| <input type="checkbox"/>            | 1/0/8  | Disabled                | <a href="#">Detail</a> |
| <input type="checkbox"/>            | 1/0/9  | Disabled                | <a href="#">Detail</a> |
| <input type="checkbox"/>            | 1/0/10 | Disabled                | <a href="#">Detail</a> |

Total: 28      1 entry selected.     

- 8) Kliknij  **Save**, aby zapisać ustawienia.

## 6.3.4 Przez CLI

- 1) Włącz globalnie Auto VoIP i ustaw wartość DSCP portu 1/0/1 jako 63.

```
Switch_A#configure
Switch_A(config)#auto-voip
Switch_A(config)#interface gigabitEthernet 1/0/1
Switch_A(config-if)#auto-voip dscp 63
Switch_A(config-if)#exit
```

- 2) Ustaw trust mode portu 1/0/1 jako trust DSCP. Ustaw 802.1p priority jako 7 dla DSCP priority 63, a 802.1p priority jako 5 dla innych priorytetów DSCP.

```
Switch_A(config)#interface gigabitEthernet 1/0/1
Switch_A(config-if)#qos trust mode dscp
Switch_A(config-if)#exit
Switch_A(config)#qos dscp-map 63 7
Switch_A(config)#qos dscp-map 0-62 5
```

- 3) Na porcie 1/0/1 ustaw scheduler mode jako weighted, a queue weight jako 1 dla TC-5. Ustaw scheduler mode jako weighted, a queue weight jako 10 dla TC-7.

```
Switch_A(config)#interface gigabitEthernet 1/0/1
Switch_A(config-if)#qos queue 5 mode wrr weight 1
Switch_A(config-if)#qos queue 7 mode wrr weight 10
Switch_A(config-if)#exit
```

- 4) Włącz LLDP-MED na porcie 1/0/1 i zaznacz wszystkie TLVs, aby były dołączane do wychodzących jednostek LLDPDU.

```
Switch_A(config)#interface gigabitEthernet 1/0/1
Switch_A(config-if)#lldp med-status
Switch_A(config-if)#lldp med-tlv-select all
Switch_A(config-if)#end
Switch_A#copy running-config startup-config
```

## Sprawdzanie konfiguracji

Sprawdzanie konfiguracji Auto VoIP:

```
Switch_A(config)#show auto-voip
```

Administrative Mode: Enabled

Verify the Auto VoIP configuration of ports:

```
Switch_A(config)#show auto-voip interface
```

```
Interface.Fa1/0/1
```

```
Auto-VoIP Interface Mode. Disabled
```

```
Auto-VoIP COS Override. False
```

```
Auto-VoIP DSCP Value. 63
```

```
Auto-VoIP Port Status. Disabled
```

```
Interface.Fa1/0/2
```

```
Auto-VoIP Interface Mode. Disabled
```

```
Auto-VoIP COS Override. False
```

```
Auto-VoIP DSCP Value. 0
```

```
Auto-VoIP Port Status. Disabled
```

```
Interface.Fa1/0/3
```

```
Auto-VoIP Interface Mode. Disabled
```

```
Auto-VoIP COS Override. False
```

```
Auto-VoIP DSCP Value. 0
```

```
Auto-VoIP Port Status. Disabled
```

...

Sprawdzanie konfiguracji Class of Service:

```
Switch_A(config)#show qos trust interface gigabitEthernet 1/0/1
```

```
Port Trust Mode LAG
```

```

```

```
Gi1/0/1 trust DSCP N/A
```

```
Switch_A(config)#show qos cos-map
```

```
-----+-----+-----+-----+-----+-----+-----+-----+-----+-----
Dot1p Value |0 |1 |2 |3 |4 |5 |6 |7
-----+-----+-----+-----+-----+-----+-----+-----+-----+-----
TC |TC1 |TC0 |TC2 |TC3 |TC4 |TC5 |TC6 |TC7
-----+-----+-----+-----+-----+-----+-----+-----+-----+-----
```

```
Switch_A(config)#show qos dscp-map
```

```
DSCP: 0 1 2 3 4 5 6 7
DSCP to 802.1P 5 5 5 5 5 5 5 5

DSCP: 8 9 10 11 12 13 14 15
DSCP to 802.1P 5 5 5 5 5 5 5 5

DSCP: 16 17 18 19 20 21 22 23
DSCP to 802.1P 5 5 5 5 5 5 5 5

DSCP: 24 25 26 27 28 29 30 31
DSCP to 802.1P 5 5 5 5 5 5 5 5

DSCP: 32 33 34 35 36 37 38 39
DSCP to 802.1P 5 5 5 5 5 5 5 5

DSCP: 40 41 42 43 44 45 46 47
DSCP to 802.1P 5 5 5 5 5 5 5 5

DSCP: 48 49 50 51 52 53 54 55
DSCP to 802.1P 5 5 5 5 5 5 5 5

```

```

DSCP: 56 57 58 59 60 61 62 63
DSCP to 802.1P 5 5 5 5 5 5 5 7
 ---- ---- ---- ---- ---- ---- ----

```

Sprawdzanie konfiguracji LLDP-MED:

```
Switch_A(config)#show lldp interface
```

Konfiguracja interfejsu LLDP:

```
gigabitEthernet 1/0/1:
```

```

Admin Status: TxRx
SNMP Trap: Disabled
TLV Status
--- -----
Port-Description Yes
System-Capability Yes
System-Description Yes
System-Name Yes
Management-Address Yes
Port-VLAN-ID Yes
Protocol-VLAN-ID Yes
VLAN-Name Yes
Link-Aggregation Yes
MAC-Physic Yes
Max-Frame-Size Yes
Power Yes
LLDP-MED Status: Enabled
TLV Status
--- -----
Network Policy Yes

```

---

|                         |     |
|-------------------------|-----|
| Location Identification | Yes |
| Extended Power Via MDI  | Yes |
| Inventory Management    | Yes |
| ...                     |     |

# Część 19

## Konfiguracja Access Security

### ROZDZIAŁY

1. Access Security
2. Konfiguracja Access Security

# 1 Access Security

## 1.1 Informacje ogólne

Access Security zapewnia dodatkowe środki ochrony zdalnego dostępu do przełącznika, zwiększając tym samym bezpieczeństwo zarządzania konfiguracją.

## 1.2 Obsługiwane funkcje

### Access Control

Funkcja ta służy do kontrolowania dostępu użytkowników do przełącznika w oparciu o adres IP, adres MAC lub port.

### HTTP

Funkcja opiera się na protokole HTTP. Może udzielić użytkownikom dostęp lub odmówić dostępu do przełącznika przez przeglądarkę sieciową.

### HTTPS

Funkcja opiera się na protokołach SSL lub TLS, pracujących w warstwie transportowej. Wspiera security access (zabezpieczenie dostępu) przez przeglądarkę sieciową.

### SSH

Funkcja opiera się na protokole SSH, protokole zabezpieczeń ustawionym w warstwie aplikacji i w warstwach transportowych. Funkcja z SSH jest podobna do połączenia telnet, może jednak zapewnić bezpieczeństwo informacji i silne uwierzytelnianie.

### Telnet

Funkcja opiera się na protokole Telnet, objętym protokołem TCP/IP. Wykorzystując Telnet, użytkownicy mogą zdalnie logować się do przełącznika..

### Serial Port

Dostępna jest możliwość konfiguracji parametrów portu szeregowego.



# 2 Konfiguracja Access Security

Z konfiguracją zabezpieczeń dostępu (Access Security) możliwa jest:

- konfiguracja funkcji Access Control;
- konfiguracja funkcji HTTP;
- konfiguracja funkcji HTTPS;
- konfiguracja funkcji SSH;
- konfiguracja funkcji Telnet

## 2.1 Przez GUI

### 2.1.1 Konfiguracja funkcji Access Control

Wybierz z menu **SECURITY > Access Security > Access Control**, aby wyświetlić poniższą stronę.

Rys. 2-1 Konfiguracja funkcji Access Control

Global Config

Access Control:  Enable

Control Mode: IP-based ▼

Apply

Entry Table

+ Add - Delete

| <input type="checkbox"/>  | Index | Port/IP/MAC | Access Interface | Operation |
|---------------------------|-------|-------------|------------------|-----------|
| No Entries in this table. |       |             |                  |           |
| Total: 0                  |       |             |                  |           |


1) W sekcji **Global Config** włącz Access Control, wybierz jeden tryb kontroli i kliknij **Apply**.

**Control Mode** Wybierz tryb kontroli dla użytkowników, by mogli logować się do strony zarządzania.

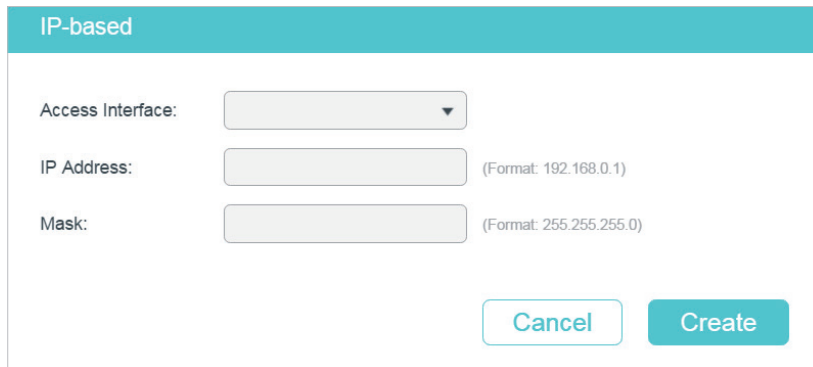
**IP-based:** Dostęp do przełącznika mają jedynie użytkownicy z IP mieszczącym się w ustawionym tu zakresie.

**MAC-based:** Dostęp do przełącznika mają jedynie użytkownicy z ustawionym tu adresem MAC.

**Port-based:** Dostęp do przełącznika mają jedynie użytkownicy podłączeni do wyznaczonych w tym miejscu portów.

- 2) W sekcji **Entry Table** kliknij  **Add**, aby dodać wpis dla funkcji Access Control.  
W przypadku wybrania trybu **IP-based** pojawi się następujące okno.

Rys. 2-2 Konfiguracja wpisu Access Control - tryb IP Based



**Access Interface**

Wybierz interfejs, aby kontrolować sposoby dostępu użytkowników do przełącznika.

**SNMP:** Funkcja służąca do zarządzania urządzeniami sieciowymi przez NMS.

**Telnet:** Typ połączenia umożliwiający użytkownikom logowanie zdalne.

**SSH:** Typ połączenia bazujący na protokole SSH.

**HTTP:** Typ połączenia bazujący na protokole HTTP.

**HTTPS:** Typ połączenia bazujący na protokole SSL.

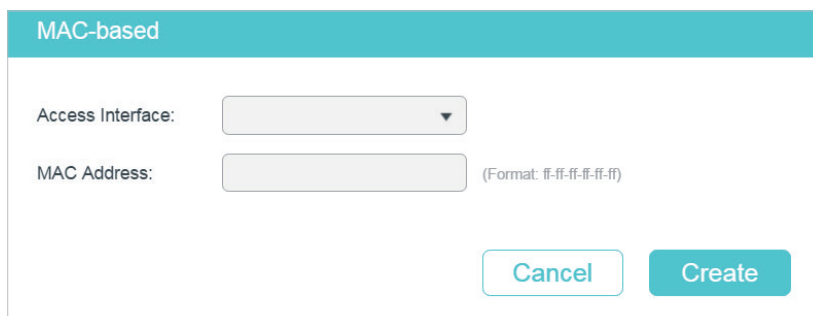
**Ping:** Protokół komunikacyjny służący do testowania połączenia sieci.

**IP Address/  
Mask**

Wprowadź adres IP i maskę, aby określić zakres IP. Jedynie użytkownicy z IP w tym zakresie mają dostęp do przełącznika.

- W przypadku wybrania trybu **MAC-based** pojawi się następujące okno.

Rys. 2-3 Konfiguracja wpisu Access Control - tryb MAC Based



|                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Access Interface | <p>Wybierz interfejs, aby kontrolować sposoby dostępu użytkowników do przełącznika.</p> <p><b>SNMP:</b> Funkcja służąca do zarządzania urządzeniami sieciowymi przez NMS.</p> <p><b>Telnet:</b> Typ połączenia umożliwiający użytkownikom logowanie zdalne.</p> <p><b>SSH:</b> Typ połączenia bazujący na protokole SSH.</p> <p><b>HTTP:</b> Typ połączenia bazujący na protokole HTTP.</p> <p><b>HTTPS:</b> Typ połączenia bazujący na protokole SSL.</p> <p><b>Ping:</b> Protokół komunikacyjny służący do testowania połączenia sieci.</p> |
| MAC Address      | Określ adres MAC. Tylko użytkownicy z poprawnym adresem MAC mają dostęp do przełącznika.                                                                                                                                                                                                                                                                                                                                                                                                                                                      |

W przypadku wybrania trybu **Port-based** pojawi się następujące okno.

Rys. 2-4 Konfiguracja wpisu Access Control Entry - tryb Port Based

The screenshot displays the 'Port-based' configuration interface. At the top, there is a teal header with the text 'Port-based'. Below this, there are two input fields: 'Access Interface:' with a dropdown arrow and 'Port:' with a text box and the note '(Format: 1/0/1)'. Underneath, the text 'UNIT1' is centered above a row of ten port icons numbered 1 through 10. Port 8 is highlighted with a blue border and a small blue dot, indicating it is selected. To the left of the port icons is a checkbox labeled 'Select All'. Below the port icons is a legend: a blue icon labeled 'Selected', a white icon labeled 'Unselected', and a grey icon labeled 'Not Available'. At the bottom right of the window are two buttons: 'Cancel' and 'Create'.

|                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Access Interface | <p>Wybierz interfejs, aby kontrolować sposoby dostępu użytkowników do przełącznika.</p> <p><b>SNMP:</b> Funkcja służąca do zarządzania urządzeniami sieciowymi przez NMS.</p> <p><b>Telnet:</b> Typ połączenia umożliwiający użytkownikom logowanie zdalne.</p> <p><b>SSH:</b> Typ połączenia bazujący na protokole SSH.</p> <p><b>HTTP:</b> Typ połączenia bazujący na protokole HTTP.</p> <p><b>HTTPS:</b> Typ połączenia bazujący na protokole SSL.</p> <p><b>Ping:</b> Protokół komunikacyjny służący do testowania połączenia sieci.</p> |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

|      |                                                                                                                          |
|------|--------------------------------------------------------------------------------------------------------------------------|
| Port | Wybierz co najmniej jeden port do konfiguracji. Tylko użytkownicy podłączeni do tych portów mają dostęp do przełącznika. |
|------|--------------------------------------------------------------------------------------------------------------------------|

- 3) Kliknij **Create**. Wyświetlą się utworzone wpisy w **Entry Table**.

## 2.1.2 Konfiguracja funkcji HTTP

Wybierz z menu **SECURITY > Access Security > HTTP Config**, aby wyświetlić poniższą stronę.

Rys. 2-5 Konfiguracja funkcji HTTP

**Global Config**

---

HTTP:  Enable

Port:  (1-65535)

[Apply](#)

**Session Config**

---

Session Timeout:  minutes (5-30)

[Apply](#)

**Number of Access Users**

---

Number Control:  Enable

Number of Admins:  (1-16)

Number of Operators:  (0-15)

Number of Power Users:  (0-15)

Number of Users:  (0-15)

[Apply](#)

- 1) W sekcji **Global Control** włącz funkcję HTTP, wyznacz port wykorzystywany w HTTP i kliknij **Apply**, aby włączyć funkcję HTTP.

|      |                                                                                                                                   |
|------|-----------------------------------------------------------------------------------------------------------------------------------|
| HTTP | Funkcja HTTP opiera się na protokole HTTP. Funkcja umożliwia użytkownikom zarządzanie przełącznikiem przez przeglądarkę sieciową. |
|------|-----------------------------------------------------------------------------------------------------------------------------------|

|      |                                     |
|------|-------------------------------------|
| Port | Określ numer portu dla usługi HTTP. |
|------|-------------------------------------|

- 2) W sekcji **Session Config** określ Session Timeout i kliknij **Apply**.

|                 |                                                                                                                       |
|-----------------|-----------------------------------------------------------------------------------------------------------------------|
| Session Timeout | Jeżeli użytkownicy nie wykonają żadnych działań w czasie Session Timeout, nastąpi automatyczne wylogowanie z systemu. |
|-----------------|-----------------------------------------------------------------------------------------------------------------------|

- 3) W sekcji **Number of Access Users** włącz funkcję Number Control, określ następujące parametry i kliknij **Apply**.

---

|                       |                                                                                                                                                                                                                      |
|-----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Number Control        | Włącz lub wyłącz Number Control. Włączona funkcja umożliwi ci kontrolowanie liczby użytkowników logujących się w tym samym czasie do strony zarządzającej. Całkowita liczba użytkowników nie powinna przekraczać 16. |
| Number of Admins      | Określ maks. liczbę użytkowników z poziomem dostępu Admin.                                                                                                                                                           |
| Number of Operators   | Określ maks. liczbę użytkowników z poziomem dostępu Operator.                                                                                                                                                        |
| Number of Power Users | Określ maks. liczbę użytkowników z poziomem dostępu Power User.                                                                                                                                                      |
| Number of Users       | Określ maks. liczbę użytkowników z poziomem dostępu User.                                                                                                                                                            |

---

## 2.1.3 Konfiguracja funkcji HTTPS

Wybierz z menu **SECURITY > Access Security > HTTPS Config**, aby wyświetlić poniższą stronę.

Rys. 2-6 Konfiguracja funkcji HTTPS

### Global Config

HTTPS:  Enable

SSL Version 3:  Enable

TLS Version 1:  Enable

Port:  (1-65535)

[Apply](#)

### CipherSuite Config

RSA\_WITH\_RC4\_128\_MD5:  Enable

RSA\_WITH\_RC4\_128\_SHA:  Enable

RSA\_WITH\_DES\_CBC\_SHA:  Enable

RSA\_WITH\_3DES\_EDE\_CBC\_SHA:  Enable

[Apply](#)

### Session Config

Session Timeout:  minutes (5-30)

[Apply](#)

### Number of Access Users

Number Control:  Enable

Number of Admins:  (1-16)

Number of Operators:  (0-15)

Number of Power Users:  (0-15)

Number of Users:  (0-15)

[Apply](#)

### Load Certificate

Certificate File:  [Browse](#)

[Load](#)

### Load Key

Key File:  [Browse](#)

[Load](#)

- 1) W sekcji **Global Config** włącz funkcję HTTPS, wybierz obsługiwany przez przełącznik protokół i wyznacz port do HTTPS. Kliknij **Apply**.

|               |                                                                                                                                                                                                                                                                        |
|---------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| HTTPS         | <p>Włącz lub wyłącz funkcję HTTPS.</p> <p>Funkcja HTTPS opiera się na protokole SSL lub TLS. Funkcja zapewnia bezpieczne połączenie między klientem a przełącznikiem.</p>                                                                                              |
| SSL Version 3 | <p>Włącz lub wyłącz na przełączniku protokół SSL Version 3.</p> <p>SSL to protokół transportowy. Może dostarczyć uwierzytelnianie serwera, szyfrowanie i integralność komunikatów, zapewniając bezpieczne połączenie HTTP.</p>                                         |
| TLS Version 1 | <p>Włącz lub wyłącz na przełączniku protokół TLS Version 1.</p> <p>TLS to protokół transportowy, będący uaktualnieniem SSL. TLS obsługuje inny algorytm szyfrowania niż SSL, nie jest więc z nim kompatybilny. TLS może obsługiwać bardziej bezpieczne połączenie.</p> |

2) W sekcji **CipherSuite Config** wybierz algorytm, który chcesz włączyć i kliknij **Apply**.

|                           |                                                                                              |
|---------------------------|----------------------------------------------------------------------------------------------|
| RSA_WITH_RC4_128_MD5      | Wymiana kluczy z szyfrowaniem 1-bitowym RC4 i algorytmem MD5 dla skrótu wiadomości.          |
| RSA_WITH_RC4_128_SHA      | Wymiana kluczy z szyfrowaniem 128-bitowym RC4 i SHA dla skrótu wiadomości.                   |
| RSA_WITH_DES_CBC_SHA      | Wymiana kluczy z DES-CBC dla szyfrowania wiadomości i SHA dla skrótu wiadomości.             |
| RSA_WITH_3DES_EDE_CBC_SHA | Wymiana kluczy z 3DES i DES-EDE3-CBC dla szyfrowania wiadomości i SHA dla skrótu wiadomości. |

3) W sekcji **Session Config** określ Session Timeout i kliknij **Apply**.

|                 |                                                                                                                      |
|-----------------|----------------------------------------------------------------------------------------------------------------------|
| Session Timeout | Jeżeli użytkownicy nie wykonają żadnych działań w czasie Session Timeout, nastąpi automatyczne wylogowanie z systemu |
|-----------------|----------------------------------------------------------------------------------------------------------------------|

4) W sekcji **Number of Access Users** włącz funkcję Number Control, określ następujące parametry i kliknij **Apply**.

|                       |                                                                                                                                                                                                                      |
|-----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Number Control        | Włącz lub wyłącz Number Control. Włączona funkcja umożliwi ci kontrolowanie liczby użytkowników logujących się w tym samym czasie do strony zarządzającej. Całkowita liczba użytkowników nie powinna przekraczać 16. |
| Number of Admins      | Określ maks. liczbę użytkowników z poziomem dostępu Admin.                                                                                                                                                           |
| Number of Operators   | Określ maks. liczbę użytkowników z poziomem dostępu Operator.                                                                                                                                                        |
| Number of Power Users | Określ maks. liczbę użytkowników z poziomem dostępu Power User.                                                                                                                                                      |
| Number of Users       | Określ maks. liczbę użytkowników z poziomem dostępu User.                                                                                                                                                            |

5) W sekcji **Load Certificate** i **Load Key** pobierz certyfikat i klucz.

---

|                  |                                                                                                                                                                                                          |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Certificate File | Wybierz certyfikat, który chcesz pobrać na przełącznik. Certyfikat musi mieć kodowanie BASE64. Pobrane certyfikat i klucz SSL muszą do siebie pasować, w przeciwnym razie połączenie HTTPS nie zadziała. |
| Key File         | Wybierz klucz, który chcesz pobrać na przełącznik. Klucz musi mieć kodowanie BASE64. Pobrane certyfikat i klucz SSL muszą do siebie pasować, w przeciwnym razie połączenie HTTPS nie zadziała.           |

---



## 2.1.4 Konfiguracja funkcji SSH

Wybierz z menu **SECURITY > Access Security > SSH Config**, aby wyświetlić poniższą stronę.

Rys. 2-7 Konfiguracja funkcji SSH

**Global Config**

SSH:  Enable

Protocol V1:  Enable

Protocol V2:  Enable

Idle Timeout:  seconds(1-120)

Maximum Connections:  (1-5)

Port:  (1-65535)

[Apply](#)

**Encryption Algorithm**

AES128-CBC:  Enable

AES192-CBC:  Enable

AES256-CBC:  Enable

Blowfish-CBC:  Enable

CAST128-CBC:  Enable

3DES-CBC:  Enable

[Apply](#)

**Data Integrity Algorithm**

HMAC-SHA1:  Enable

HMAC-MD5:  Enable

[Apply](#)

**Load Key**

Choose the SSH public key file to download into the switch.

Key Type:  ▼

Key File:  [Browse](#)

[Load](#)

- 1) W sekcji **Global Config** wybierz **Enable**, aby włączyć funkcję SSH i określ następujące parametry.

### SSH

Wybierz **Enable**, aby włączyć funkcję SSH.

SSH to protokół pracujący w warstwie aplikacji i w warstwie transportowej. Może zapewnić bezpieczne zdalne połączenie z urządzeniem. SSH jest lepszą gwarancją bezpieczeństwa niż protokół Telnet, ponieważ posiada silne szyfrowanie.

|                     |                                                                                                                             |
|---------------------|-----------------------------------------------------------------------------------------------------------------------------|
| Protocol V1         | Wybierz <b>Enable</b> aby włączyć SSH w wersji 1.                                                                           |
| Protocol V2         | Wybierz <b>Enable</b> aby włączyć SSH w wersji 2.                                                                           |
| Idle Timeout        | Określ okres czasu bezczynności. Po wygaśnięciu czasu bezczynności system automatycznie zwolni połączenie.                  |
| Maximum Connections | Określ maks. liczbę połączeń z serwerem SSH. Jeżeli liczba połączeń osiągnie określony limit, nie powstaną nowe połączenia. |
| Port                | Wyznacz port wykorzystywany do SSH.                                                                                         |

- 2) W sekcji **Encryption Algorithm** włącz algorytm szyfrowania, który ma być obsługiwany przez przełącznik i kliknij **Apply**.
- 3) W sekcji **Data Integrity Algorithm** włącz algorytm integralności, który ma być obsługiwany przez przełącznik i kliknij **Apply**.
- 4) W sekcji **Import Key File** z rozwijanej listy wybierz typ klucza i kliknij **Browse**, aby pobrać plik wybranego klucza.

|          |                                                                                                                               |
|----------|-------------------------------------------------------------------------------------------------------------------------------|
| Key Type | Wybierz typ klucza. Algorytm odpowiedniego typu wykorzystywany jest zarówno do generowania klucza, jak i do uwierzytelniania. |
| Key File | Wybierz klucz publiczny do pobrania na przełącznik. Długość klucza pobranego pliku wynosi od 512 do 3072 bitów.               |



Uwaga:

Pobieranie pliku klucza zajmuje wiele czasu. Czekaj, nie wykonując żadnych działań.

## 2.1.5 Konfiguracja funkcji Telnet

Wybierz z menu **SECURITY > Access Security > Telnet Config**, aby wyświetlić poniższą stronę.

Rys. 2-8 Konfiguracja funkcji Telnet

Telnet Config

---

Telnet:  Enable

Port:  (1-65535)

[Apply](#)

Włącz Telnet i kliknij **Apply**.

|        |                                                                                                                                                                                          |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Telnet | Wybierz <b>Enable</b> , aby włączyć funkcję Telnet. Funkcja opiera się na protokole Telnet, objętym protokołem TCP/IP. Dzięki niej użytkownicy mogą zdalnie logować się do przełącznika. |
| Port   | Wyznacz port wykorzystywany przez Telnet.                                                                                                                                                |

## 2.1.6 Konfiguracja parametrów portu szeregowego

Wybierz z menu **SECURITY > Access Security > Serial Port Config**, aby wyświetlić poniższą stronę.

Rys. 2-9 Konfiguracja parametrów portu szeregowego

Serial Port Settings

---

Baud Rate:

Data Bits: 8

Parity Bits: none

Stop Bits: 1

Skonfiguruj parametr Baud Rate i kliknij **Apply**.

|             |                                                                                                   |
|-------------|---------------------------------------------------------------------------------------------------|
| Baud Rate   | Skonfiguruj szybkość transmisji danych połączenia konsolowego. Domyślną wartością jest 38400 b/s. |
| Data Bits   | Wyświetla bity danych.                                                                            |
| Parity Bits | Wyświetla bity parzystości.                                                                       |
| Stop Bits   | Wyświetla bity stopu.                                                                             |

## 2.2 Przez CLI

### 2.2.1 Konfiguracja Access Control

Wykonaj poniższe kroki, aby skonfigurować funkcję kontroli dostępu:

|        |                                                                     |
|--------|---------------------------------------------------------------------|
| Krok 1 | <p><b>configure</b></p> <p>Uruchom tryb konfiguracji globalnej.</p> |
|--------|---------------------------------------------------------------------|

Krok 2 Użyj poniższej komendy do kontrolowania dostępu użytkowników przez ograniczenie dopuszczanych adresów IP.

**user access-control ip-based enable**

Skonfiguruj tryb kontroli jako IP-based.

**user access-control ip-based { ip-addr ip-mask } [ snmp ] [ telnet ] [ ssh ] [ http ] [ https ] [ ping ] [ all ]**

Dostęp do przełącznika mają jedynie użytkownicy z IP mieszczącym się w ustawionym tu zakresie.

*ip-addr*: Wyznacz adres IP dla użytkownika.

*ip-mask*: Wyznacz maskę podsieci użytkownika.

[ snmp ] [ telnet ] [ ssh ] [ http ] [ https ] [ ping ] [ all ]: Wybierz jaki typ dostępu do przełącznika mają użytkownicy. Domyślnie, wszystkie typy dostępu są włączone.

Użyj poniższej komendy do kontrolowania dostępu użytkowników przez ograniczenie dopuszczanych adresów MAC:

**user access-control mac-based enable**

Skonfiguruj tryb kontroli jako MAC-based.

**user access-control mac-based { mac-addr } [ snmp ] [ telnet ] [ ssh ] [ http ] [ https ] [ ping ] [ all ]**

Tylko użytkownicy z wyznaczonymi tu adresami MAC mają dostęp do przełącznika.

*mac-addr*: Wyznacz adres MAC użytkownika.

[ snmp ] [ telnet ] [ ssh ] [ http ] [ https ] [ ping ] [ all ]: Wybierz jaki typ dostępu do przełącznika mają użytkownicy. Domyślnie, wszystkie typy dostępu są włączone.

Użyj poniższej komendy do kontrolowania dostępu użytkowników przez ograniczenie dopuszczanych portów:

**user access-control port-based enable**

Skonfiguruj tryb kontroli jako Port-based.

**user access-control port-based interface { fastEthernet port-list | gigabitEthernet port-list | ten-gigabitEthernet port-list } [ snmp ] [ telnet ] [ ssh ] [ http ] [ https ] [ ping ] [ all ]**

Dostęp do przełącznika mają jedynie użytkownicy podłączeni do wyznaczonych w tym miejscu portów.

*port-list*: Sporządź listę portów Ethernet port w formacie 1/0/1-4. Możesz wyznaczyć maks. 5 portów.

Krok 3 **show user configuration**

Sprawdź dane ustawień bezpieczeństwa informacji uwierzytelniania użytkowników i interfejsu dostępu.

Krok 4 **end**

Powróć do trybu privileged EXEC.

**Krok 5**     **copy running-config startup-config**

Zapisz ustawienia w pliku konfiguracyjnym.

Poniższy przykład prezentuje ustawianie typu kontroli dostępu na IP-based. Ustaw adres IP jako 192.168.0.100, maskę podsieci jako 255.255.255.255 i włącz na przełączniku obsługę snmp, telnet, http i https.

**Switch#configure****Switch(config)#user access-control ip-based enable****Switch(config)#user access-control ip-based** 192.168.0.100 255.255.255.255 snmp  
telnet http https**Switch(config)#show user configuration**

User authentication mode: IP based

| Index | IP Address       | Access Interface       |
|-------|------------------|------------------------|
| ----- | -----            | -----                  |
| 1     | 192.168.0.100/32 | SNMP Telnet HTTP HTTPS |

**Switch(config)#end****Switch#copy running-config startup-config**

## 2.2.2 Konfiguracja funkcji HTTP

Wykonaj poniższe kroki, aby skonfigurować funkcję HTTP:

**Krok 1**     **configure**

Uruchom tryb konfiguracji globalnej.

**Krok 2**     **ip http server**

Włącz funkcję HTTP. Funkcja jest domyślnie włączona.

**Krok 3**     **ip http session timeout *minutes***

Określ czas Session Timeout (czas wygasania sesji). Jeżeli użytkownicy nie wykonają żadnych działań w czasie Session Timeout, nastąpi automatyczne wylogowanie z systemu.

*minutes*: Określ czas wygasania sesji, od 5 do 30 minut. Wartość domyślna to 10.

- 
- Krok 4    **ip http max-users admin-num operator-num poweruser-num user-num**
- Określ maks. liczbę użytkowników, którzy mogą łączyć się z serwerem HTTP. Całkowita liczba użytkowników nie powinna przekraczać 16.
- admin-num*: Wprowadź maks. liczbę użytkowników z poziomem dostępu Admin. Wartość powinna wynosić od 1 do 16.
- operator-num*: Wprowadź maks. liczbę użytkowników z poziomem dostępu Operator. Wartość powinna wynosić od 1 do 15.
- poweruser-num*: Wprowadź maks. liczbę użytkowników z poziomem dostępu Power User. Wartość powinna wynosić od 1 do 15.
- user-num*: Wprowadź maks. liczbę użytkowników z poziomem dostępu User. Wartość powinna wynosić od 1 do 15.
- 
- Krok 5    **show ip http configuration**
- Sprawdź dane konfiguracyjne serwera HTTP(status, session timeout, access-control, max-user number, idle-timeout itd.).
- 
- Krok 6    **end**
- Powróć do trybu privileged EXEC.
- 
- Krok 7    **copy running-config startup-config**
- Zapisz ustawienia w pliku konfiguracyjnym.
- 

Poniższy przykład prezentuje ustawianie czasu wygasania sesji na 9, maks. liczby adminów na 6, maks. liczby operatorów na 2, maks. liczby użytkowników zaawansowanych na 2 i maks. liczby użytkowników na 2.

**Switch#configure**

**Switch(config)#ip http server**

**Switch(config)#ip http session timeout 9**

**Switch(config)#ip http max-user 6 2 2 2**

**Switch(config)#show ip http configuration**

```

HTTP Status: Enabled
HTTP Port: 80
HTTP Session Timeout: 9
HTTP User Limitation: Enabled
HTTP Max Users as Admin: 6
HTTP Max Users as Operator: 2
HTTP Max Users as Power User: 2
HTTP Max Users as User: 2

```

**Switch(config)#end**

**Switch#copy running-config startup-config**

## 2.2.3 Konfiguracja funkcji HTTPS

Wykonaj poniższe kroki, aby skonfigurować funkcję HTTPS:

---

|        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Krok 1 | <b>configure</b><br>Uruchom tryb konfiguracji globalnej.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Krok 2 | <b>ip http secure-server</b><br>Włącz funkcję HTTPS. Funkcja jest domyślnie włączona.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Krok 3 | <b>ip http secure-protocol { [ ssl3 ] [ tls1 ] }</b><br>Skonfiguruj, aby włączyć na przełączniku obsługę odpowiedniego protokołu. Domyślnie przełącznik obsługuje SSLv3 i TLSv1.<br><br><b>ssl3:</b> Włącz protokół SSL w wersji 3. SSL to protokół transportowy. Może dostarczyć uwierzytelnianie serwera, szyfrowanie i integralność komunikatów, zapewniając bezpieczne połączenie HTTP.<br><br><b>tls1:</b> Włącz protokół TLS w wersji. TLS to protokół transportowy, będący uaktualnieniem SSL. TLS obsługuje inny algorytm szyfrowania niż SSL, nie jest więc z nim kompatybilny. TLS może obsługiwać bardziej bezpieczne połączenie.                |
| Krok 4 | <b>ip http secure-ciphersuite { [ 3des-ede-cbc-sha ] [ rc4-128-md5 ] [ rc4-128-sha ] [ des-cbc-sha ] }</b><br>Włącz odpowiedni mechanizm szyfrowania. Domyślnie, wszystkie typy są włączone.<br><br><b>3des-ede-cbc-sha:</b> Wymiana kluczy z 3DES i DES-EDE3-CBC dla szyfrowania wiadomości i SHA dla skrótu wiadomości.<br><br><b>rc4-128-md5:</b> Wymiana kluczy z szyfrowaniem 128-bitowym RC4 i algorytmem MD5 dla skrótu wiadomości.<br><br><b>rc4-128-sha:</b> Wymiana kluczy z szyfrowaniem 128-bitowym RC i SHA dla skrótu wiadomości.<br><br><b>des-cbc-sha:</b> Wymiana kluczy z DES-CBC dla szyfrowania wiadomości i SHA dla skrótu wiadomości. |
| Krok 5 | <b>ip http secure-session timeout <i>minutes</i></b><br>Określ czas Session Timeout (czas wygasania sesji). Jeżeli użytkownicy nie wykonają żadnych działań w czasie Session Timeout, nastąpi automatyczne wylogowanie z systemu.<br><br><b><i>minutes:</i></b> Określ czas wygasania sesji, od 5 do 30 minut. Wartość domyślna to 10.                                                                                                                                                                                                                                                                                                                      |

---

- 
- Krok 6    **ip http secure-max-users** *admin-num operator-num poweruser-num user-num*
- Określ maks. liczbę użytkowników, którzy mogą łączyć się z serwerem HTTP. Całkowita liczba użytkowników nie powinna przekraczać 16.
- admin-num*: Wprowadź maks. liczbę użytkowników z poziomem dostępu Admin. Wartość powinna wynosić od 1 do 16.
- operator-num*: Wprowadź maks. liczbę użytkowników z poziomem dostępu Operator. Wartość powinna wynosić od 1 do 15.
- poweruser-num*: Wprowadź maks. liczbę użytkowników z poziomem dostępu Power User. Wartość powinna wynosić od 1 do 15.
- user-num*: Wprowadź maks. liczbę użytkowników z poziomem dostępu User. Wartość powinna wynosić od 1 do 15.
- 
- Krok 7    **ip http secure-server download certificate** *ssl-cert ip-address ip-addr*
- Pobierz na przełącznik wybrany certyfikat z serwera TFTP.
- ssl-cert*: Ustaw nazwę certyfikatu SSL, od 1 do 25 znaków. Certyfikat musi mieć kodowanie BASE64. Pobrane certyfikat i klucz SSL muszą do siebie pasować.
- ip-addr*: Określ adres IP serwera TFTP. Obsługiwane są adresy IPv4 i IPv6.
- 
- Krok 8    **ip http secure-server download key** *ssl-key ip-address ip-addr*
- Pobierz na przełącznik wybrany klucz z serwera TFTP.
- ssl-key*: Ustaw nazwę pliku klucza zapisanego w serwerze TFTP. Klucz musi mieć kodowanie BASE64.
- ip-addr*: Ustaw adres IP serwera TFTP. Obsługiwane są adresy IPv4 i IPv6.
- 
- Krok 9    **show ip http secure-server**
- Sprawdź konfigurację globalną HTTPS.
- 
- Krok 10    **end**
- Powróć do trybu privileged EXEC.
- 
- Krok 11    **copy running-config startup-config**
- Zapisz ustawienia w pliku konfiguracyjnym.
- 

Poniższy przykład prezentuje konfigurację funkcji HTTPS. Włącz protokoły SSL3 i TLS1. Włącz mechanizm szyfrowania 3des-ede-cbc-sha. Ustaw czas wygasania sesji na 15, maks. liczbę adminów na 2, maks. liczbę operatorów na 2, maks. liczbę użytkowników zaawansowanych na 2, maks. liczbę użytkowników na 2. Pobierz certyfikat nazwany ca.crt i klucz z nazwą ca.key z serwera TFTP z adresem IP 192.168.0.100.

**Switch#configure**

**Switch(config)#ip http secure-server**

**Switch(config)#ip http secure-protocol** ssl3 tls1

**Switch(config)#ip http secure-ciphersuite** 3des-ede-cbc-sha

**Switch(config)#ip http secure-session timeout** 15



```
Switch(config)#ip http secure-max-users 2 2 2 2
```

```
Switch(config)#ip http secure-server download certificate ca.crt ip-address
192.168.0.100
```

Start to download SSL certificate.....

Download SSL certificate OK.

```
Switch(config)#ip http secure-server download key ca.key ip-address 192.168.0.100
```

Start to download SSL key.....

Download SSL key OK.

```
Switch(config)#show ip http secure-server
```

```
HTTPS Status: Enabled
HTTPS Port: 443
SSL Protocol Level(s): ssl3 tls1
SSL CipherSuite: 3des-edc-cbc-sha
HTTPS Session Timeout: 15
HTTPS User Limitation: Enabled
HTTPS Max Users as Admin: 2
HTTPS Max Users as Operator: 2
HTTPS Max Users as Power User: 2
HTTPS Max Users as User: 2
```

```
Switch(config)#end
```

```
Switch#copy running-config startup-config
```

## 2.2.4 Konfiguracja funkcji SSH

Wykonaj poniższe kroki, aby skonfigurować funkcję SSH:

---

Krok 1     **configure**

Uruchom tryb konfiguracji globalnej.

---

Krok 2     **ip ssh server**

Włącz funkcję SSH. Funkcja jest domyślnie wyłączona.

---

**Krok 3 ip ssh version { v1 | v2 }**

Skonfiguruj, aby włączyć na przełączniku obsługę odpowiedniego protokołu. Domyślnie przełącznik obsługuje SSHv1 i SSHv3.

*v1 | v2*: Wybierz, aby włączyć odpowiedni protokół.

**Krok 4 ip ssh timeout value**

Określ okres czasu bezczynności. Po wygaśnięciu czasu bezczynności system automatycznie zwolni połączenie.

*value*: Wprowadź wartość wygasania czasu, między 1 a 120 sekund. Wartość domyślna to 20 sekund.

**Krok 5 ip ssh max-client num**

Określ maks. liczbę połączeń z serwerem SSH. Jeżeli liczba połączeń osiągnie określony limit, nie powstaną nowe połączenia.

*num*: Wprowadź liczbę połączeń, od 1 do 5. Wartość domyślna to 5.

**Krok 6 ip ssh algorithm { AES128-CBC | AES192-CBC | AES256-CBC | Blowfish-CBC | Cast128-CBC | 3DES-CBC | HMAC-SHA1 | HMAC-MD5 }**

Włącz odpowiedni algorytm. Domyślnie wszystkie typy są włączone.

**AES128-CBC | AES192-CBC | AES256-CBC | Blowfish-CBC | Cast128-CBC | 3DES-CBC**: Określ algorytm szyfrowania, który ma być obsługiwany przez przełącznik.

**HMAC-SHA1 | HMAC-MD5**: Określ algorytm integralności danych, który ma być obsługiwany przez przełącznik.

**Krok 7 ip ssh download { v1 | v2 } key-file ip-address ip-addr**

Wybierz typ pliku klucza i pobierz na przełącznik wybrany plik z serwera TFTP.

*v1 | v2*: Wybierz typ klucza. Algorytm odpowiedniego typu wykorzystywany jest zarówno do generowania klucza, jak do uwierzytelniania.

*key-file*: Ustaw nazwę pliku klucza zapisanego w serwerze TFTP. Upewnij się, że długość klucza pobranego pliku wynosi od 512 do 3072 bitów.

*ip-addr*: Ustaw adres IP serwera TFTP. Obsługiwane są adresy IPv4 i IPv6.

**Krok 8 show ip ssh**

Sprawdź konfigurację globalną SSH.

**Krok 9 end**

Powróć do trybu privileged EXEC.

**Krok 10 copy running-config startup-config**

Zapisz ustawienia w pliku konfiguracyjnym.

**Uwaga:**

Pobieranie pliku klucza zajmuje wiele czasu. Czekać, nie wykonując żadnych działań.

Poniższy przykład prezentuje konfigurację funkcji SSH. Ustaw wersję 1 i 2 SSH. Włącz algorytm szyfrowania AES128-CBC i Cast128-CBC. Włącz algorytm integralności danych HMAC-MD5. Wybierz typ klucza SSH-2 RSA/DSA.

```
Switch(config)#ip ssh server
```

```
Switch(config)#ip ssh version v1
```

```
Switch(config)#ip ssh version v2
```

```
Switch(config)#ip ssh timeout 100
```

```
Switch(config)#ip ssh max-client 4
```

```
Switch(config)#ip ssh algorithm AES128-CBC
```

```
Switch(config)#ip ssh algorithm Cast128-CBC
```

```
Switch(config)#ip ssh algorithm HMAC-MD5
```

```
Switch(config)#ip ssh download v2 publickey ip-address 192.168.0.100
```

Start to download SSH key file.....

Download SSH key file OK.

```
Switch(config)#show ip ssh
```

Global Config:

SSH Server: Enabled

Protocol V1: Enabled

Protocol V2: Enabled

Idle Timeout: 100

MAX Clients: 4

Port: 22

Encryption Algorithm:

AES128-CBC: Enabled

AES192-CBC: Disabled

AES256-CBC: Disabled

Blowfish-CBC: Disabled

Cast128-CBC: Enabled

3DES-CBC: Disabled

Data Integrity Algorithm:

HMAC-SHA1: Disabled

```
HMAC-MD5: Enabled
Key Type: SSH-2 RSA/DSA
Key File:
----- BEGIN SSH2 PUBLIC KEY -----
Comment: "dsa-key-20160711"
```

```
Switch(config)#end
```

```
Switch#copy running-config startup-config
```

## 2.2.5 Konfiguracja funkcji Telnet

Wykonaj poniższe kroki, aby włączyć funkcję Telnet:

|        |                                           |                                                                     |
|--------|-------------------------------------------|---------------------------------------------------------------------|
| Krok 1 | <b>configure</b>                          | Uruchom tryb konfiguracji globalnej.                                |
| Krok 2 | <b>telnet enable</b>                      | Włącz funkcję telnet. Funkcja jest domyślnie włączona.              |
| Krok 3 | <b>telnet port port</b>                   | Wyznacz port wykorzystywany przez Telnet, w zakresie od 1 do 65535. |
| Krok 4 | <b>end</b>                                | Powróć do trybu privileged EXEC.                                    |
| Krok 4 | <b>copy running-config startup-config</b> | Zapisz ustawienia w pliku konfiguracyjnym.                          |

## 2.2.6 Konfiguracja parametrów portu szeregowego

Wykonaj poniższe kroki, aby skonfigurować parametry portu szeregowego:

|        |                                                                        |                                                                                                                                                                                                               |
|--------|------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Krok 1 | <b>configure</b>                                                       | Uruchom tryb konfiguracji globalnej.                                                                                                                                                                          |
| Krok 2 | <b>serial_port baud_rate { 9600   19200   38400   57600   115200 }</b> | Określ szybkość transmisji danych połączenia konsolowego.<br><br>9600   19200   38400   57600   115200: Określ komunikacyjną szybkość transmisji danych na porcie konsoli. Wartością domyślną jest 38400 b/s. |
| Krok 3 | <b>end</b>                                                             | Powróć do trybu privileged EXEC.                                                                                                                                                                              |

---

Krok 4    **copy running-config startup-config**

Zapisz ustawienia w pliku konfiguracyjnym.

---

# Część 20

## Konfiguracja AAA

### ROZDZIAŁY

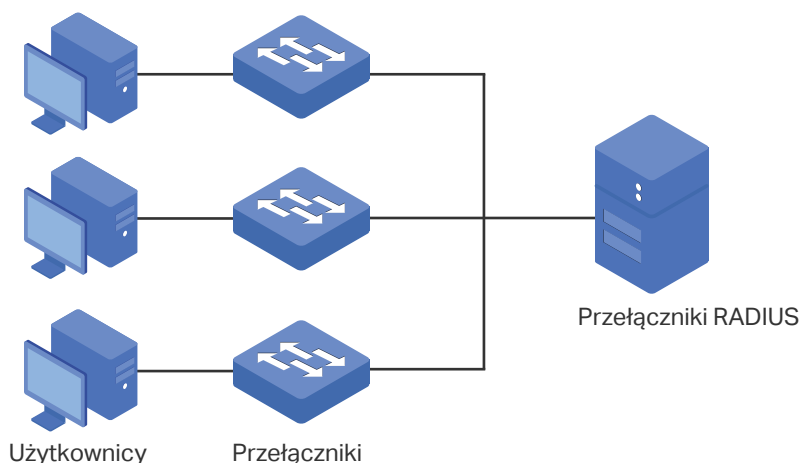
1. Informacje ogólne
2. Konfiguracja AAA
3. Przykład konfiguracji

# 1 Informacje ogólne

Skrót AAA oznacz authentication (uwierzytelnianie), authorization (autoryzacja) i accounting (kontrola dostępu). Na przełącznikach TP-Link funkcja ta służy przede wszystkim do uwierzytelniania użytkowników, którzy próbują zalogować się do przełącznika lub chcą uzyskać uprawnienia administracyjne. Administrator może tworzyć konta dla gości i ustawiać hasła dostępu dla innych użytkowników. Goście nie mają uprawnień administracyjnych bez znajomości ustawionego hasła dostępu.

AAA zapewnia dostęp do bezpiecznej i efektywnej metody uwierzytelniania. Proces uwierzytelniania może odbywać się lokalnie na przełączniku lub centralnie, na serwerze(-ach) RADIUS/TACACS+. Jak pokazano na poniższym schemacie, administrator sieci może centralnie konfigurować konta zarządzające przełączników na serwerze RADIUS i uwierzytelniać na nim użytkowników, którzy próbują uzyskać dostęp do przełącznika lub chcą uzyskać uprawnienia administracyjne.

Rys. 1-1 Topologia sieci AAA



## 2 Konfiguracja AAA

Funkcja AAA umożliwia przetwarzanie uwierzytelniania lokalnie na przełączniku lub centralnie na serwerach RADIUS/TACACS+. Aby zapewnić stabilność systemu uwierzytelniania, możesz równocześnie skonfigurować wiele serwerów i metod uwierzytelniania. W tym rozdziale dowiesz się jak skonfigurować kompleksowo procesy uwierzytelniania w AAA.

Wykonaj poniższe kroki, aby przeprowadzić proces konfiguracji:

- 1) Dodaj serwery.
- 2) Skonfiguruj grupy serwerów.
- 3) Skonfiguruj listę metod.
- 4) Skonfiguruj listę opcji AAA.
- 5) Skonfiguruj konto logowania i hasło dostępu.

### Wskazówki dotyczące konfiguracji

Poniżej wyjaśnione są podstawowe pojęcia i mechanizm działania AAA:

- Domyślne ustawienie AAA

Domyślnie funkcja AAA jest włączona i nie można jej wyłączyć.

- Grupa serwera

Serwery korzystające z tego samego protokołu mogą być dodane do jednej grupy serwerów. Serwery w tej grupie będą uwierzytelniać dostęp użytkowników w takiej kolejności, w jakiej zostały dodane. Serwer, który był dodany do grupy jako pierwszy ma najwyższy priorytet i odpowiada za uwierzytelnianie w normalnych okolicznościach. Jeżeli jednak ten pierwszy serwer przestanie działać lub nie będzie odpowiadać na żądanie uwierzytelnienia dostępu, funkcję uwierzytelniania przejmie drugi serwer, itd.

- Lista metod

Za metodę uznawana jest m.in. grupa serwerów, czy też uwierzytelnianie lokalne. Listę metod może tworzyć wiele metod. Do uwierzytelniania dostępu użytkownika przełącznik korzysta z pierwszej metody na liście, a jeżeli ta metoda zawiedzie, przełącznik korzysta z kolejnej metody. Proces ten trwa, dopóki dostęp użytkownika nie zostanie uwierzytelniony lub do wyczerpania zdefiniowanych metod. Jeżeli proces uwierzytelniania się powiedzie lub jeżeli serwer bezpieczeństwa lub przełącznik lokalny odmówi dostępu użytkownikowi, proces uwierzytelniania zatrzyma się i kolejne metody nie będą wykorzystane.

Dostępne są dwa typy listy metod: lista metod logowania dla wszystkich użytkowników, którzy chcą uzyskać dostęp do przełącznika oraz lista metod dostępu dla gości, którzy chcą uzyskać uprawnienia administratora.



- Lista opcji AAA


Przełącznik obsługuje następujące opcje dostępu: Telnet, SSH i HTTP. Dla każdej opcji można wybrać skonfigurowaną listę metod uwierzytelniania.

## 2.1 Przez GUI

### 2.1.1 Dodawanie serwerów

Na przełączniku możesz dodać jeden lub kilka serwerów RADIUS/TACACS+ do uwierzytelniania. Jeżeli dodasz kilka serwerów, serwer, który był dodany do grupy jako pierwszy ma najwyższy priorytet i odpowiada za uwierzytelnianie użytkowników starających się uzyskać dostęp do przełącznika. Kolejne serwery są serwerami zapasowymi, na wypadek awarii pierwszego serwera.

- Dodawanie serwera RADIUS

Wybierz z menu **SECURITY > AAA > RADIUS Config** i kliknij  **Add**, aby wyświetlić poniższą stronę.

Rys. 2-1 Konfiguracja serwera RADIUS

**RADIUS Server**

|                      |                                   |                                                                                                            |
|----------------------|-----------------------------------|------------------------------------------------------------------------------------------------------------|
| Server IP:           | <input type="text"/>              | <small>(Format: 192.168.0.1)</small>                                                                       |
| Shared Key:          | <input type="text"/>              | <small>1-32 characters. Only numbers, letters and the following symbols are allowed: - . / : @ _ .</small> |
| Authentication Port: | <input type="text" value="1812"/> | <small>(1-65535)</small>                                                                                   |
| Accounting Port:     | <input type="text" value="1813"/> | <small>(1-65535)</small>                                                                                   |
| Retransmit:          | <input type="text" value="2"/>    | <small>(1-3)</small>                                                                                       |
| Timeout:             | <input type="text" value="5"/>    | <small>seconds (1-9)</small>                                                                               |
| NAS Identifier:      | <input type="text"/>              | <small>(Optional)</small>                                                                                  |

Wykonaj poniższe kroki, aby dodać serwer RADIUS:

- 1) Skonfiguruj poniższe parametry.

|            |                                                                                                                                                                   |
|------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Server IP  | Podaj adres IP serwera z protokołem bezpieczeństwa RADIUS.                                                                                                        |
| Shared Key | Podaj wspólny klucz zabezpieczeń serwera RADIUS i przełącznika. Serwer RADIUS i przełącznik korzystają z ciągu klucza do szyfrowania haseł i wymiany komunikatów. |

|                     |                                                                                                                                                                                                                                                     |
|---------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Authentication Port | Podaj numer portu docelowego UDP na serwerze RADIUS dla żądań uwierzytelniania. Domyślnym ustawieniem jest 1812.                                                                                                                                    |
| Accounting Port     | Podaj numer portu docelowego UDP na serwerze RADIUS dla żądań rozliczania. Domyślną wartością jest 1813. Port ten zwykle stosuje się dla funkcji 802.1x.                                                                                            |
| Retransmit          | Określ ile razy żądanie ma być wysłane do serwera, gdy serwer nie odpowiada. Domyślnym ustawieniem jest 2.                                                                                                                                          |
| Timeout             | Podaj czas oczekiwania przełącznika na odpowiedź serwera przed ponownym wysłaniem żądania. Domyślnym ustawieniem jest 5 sekund.                                                                                                                     |
| NAS Identifier      | Podaj nazwę NAS (Network Access Server), która zostanie umieszczona w pakiecie RADIUS dla łatwiejszej identyfikacji. Nazwa musi zawierać od 1 do 31 znaków. Domyślną wartością jest adres MAC przełącznika. Zasadniczo NAS określa sam przełącznik. |

2) Kliknij **Create**, aby dodać serwer RADIUS na przełączniku.

#### ■ Dodawanie serwera TACACS+

Wybierz z menu **SECURITY > AAA > TACACS+ Config** i kliknij  **Add**, aby wyświetlić poniższą stronę.

Rys. 2-2 Konfiguracja serwera TACACS+

**TACACS+ Server**

Server IP:  (Format:192.168.0.1)

Timeout:  seconds (1-9)

Shared Key:  1-32 characters. Only numbers, letters and the following symbols are allowed: - . / : @ \_ .

Server Port:  (1-65535)

Wykonaj poniższe kroki, aby dodać serwer TACACS+:

1) Skonfiguruj poniższe parametry.

|            |                                                                                                                                                                     |
|------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Server IP  | Podaj adres IP serwera z protokołem bezpieczeństwa TACACS+.                                                                                                         |
| Timeout    | Podaj czas oczekiwania przełącznika na odpowiedź serwera przed ponownym wysłaniem żądania. Domyślnym ustawieniem jest 5 sekund.                                     |
| Shared Key | Podaj wspólny klucz zabezpieczeń serwera TACACS+ i przełącznika. Serwer TACACS+ i przełącznik korzystają z ciągu klucza do szyfrowania haseł i wymiany komunikatów. |

|             |                                                                                       |
|-------------|---------------------------------------------------------------------------------------|
| Server Port | Określ port TCP stosowany na serwerze TACACS+ dla AAA. Domyślnym ustawieniem jest 49. |
|-------------|---------------------------------------------------------------------------------------|

- 2) Kliknij **Create**, aby dodać serwer TACACS+ na przełączniku.

## 2.1.2 Konfiguracja grup serwerów

Przełącznik ma dwie wbudowane grupy serwerów, jeden dla serwerów RADIUS, a drugi dla serwerów TACACS+. Serwery korzystające z tego samego protokołu są automatycznie dodawane do domyślnej grupy serwerów. Możesz dodawać nowe grupy serwerów, jeżeli uznasz to za potrzebne.

Wybierz z menu **SECURITY > AAA > Server Group**, aby wyświetlić poniższą stronę.

Rys. 2-3 Dodawanie nowej grupy serwera

| Server Group List        |    |              |             |           |                |
|--------------------------|----|--------------|-------------|-----------|----------------|
|                          |    |              |             |           | + Add - Delete |
| <input type="checkbox"/> | ID | Server Group | Server Type | Server IP | Operation      |
| <input type="checkbox"/> | 1  | radius       | RADIUS      |           |                |
| <input type="checkbox"/> | 2  | tacacs       | TACACS+     |           |                |
| Total: 2                 |    |              |             |           |                |

Na liście są dwie domyślne grupy serwerów. Możesz je edytować lub wykonać poniższe kroki, aby skonfigurować nową grupę serwerów:

- 1) Kliknij **Add**, aby pojawiło się poniższe okno.

Rys. 2-4 Dodawanie grupy serwera

**Server Group**

Server Group:  (1-15 characters)

Server Type:

Server IP:

Skonfiguruj poniższe parametry:

|              |                                                                          |
|--------------|--------------------------------------------------------------------------|
| Server Group | Podaj nazwę grupy serwerów.                                              |
| Server Type  | Wybierz typ serwera dla grupy. Dostępne są dwie opcje: RADIUS i TACACS+. |
| Server IP    | Wybierz adres IP serwera, który zostanie dodany do grupy serwerów.       |

- 2) Kliknij **Create**.

## 2.1.3 Konfiguracja listy metod

Lista metod opisuje metody uwierzytelniania i kolejność, w jakiej są używane do uwierzytelniania dostępu użytkowników. Przełącznik obsługuje listę metod logowania dla wszystkich użytkowników, którzy chcą uzyskać dostęp do przełącznika i oraz listę metod dostępu dla gości, którzy chcą uzyskać uprawnienia administratora.

Wybierz z menu **SECURITY > AAA > Method List**, aby wyświetlić poniższą stronę.

Rys. 2-5 Lista metod

| Authentication Login Method List |    |         |       |      |      |      |           |
|----------------------------------|----|---------|-------|------|------|------|-----------|
| + Add - Delete                   |    |         |       |      |      |      |           |
| <input type="checkbox"/>         | ID | Name    | Pri1  | Pri2 | Pri3 | Pri4 | Operation |
| <input type="checkbox"/>         | 1  | default | local | --   | --   | --   |           |
| Total: 1                         |    |         |       |      |      |      |           |

| Authentication Enable Method List |    |         |      |      |      |      |           |
|-----------------------------------|----|---------|------|------|------|------|-----------|
| + Add - Delete                    |    |         |      |      |      |      |           |
| <input type="checkbox"/>          | ID | Name    | Pri1 | Pri2 | Pri3 | Pri4 | Operation |
| <input type="checkbox"/>          | 1  | default | none | --   | --   | --   |           |
| Total: 1                          |    |         |      |      |      |      |           |

Dostępne są odpowiednio dwie domyślne metody dla uwierzytelniania logowania i uwierzytelniania dostępu.

Możesz edytować domyślne metody lub wykonać poniższe kroki, aby dodać nową metodę:

- 1) Kliknij **Add** w sekcji **Authentication Login Method List** lub **Authentication Enable Method List**, aby dodać odpowiedni typ list metod. Pojawi się poniższe okno.

Rys. 2-6 Dodawanie nowej metody

**Authentication Login Method**

Method List Name:  (1-15 characters)

Pri1:

Pri2:

Pri3:

Pri4:

Skonfiguruj parametry dla metody, którą chcesz dodać.

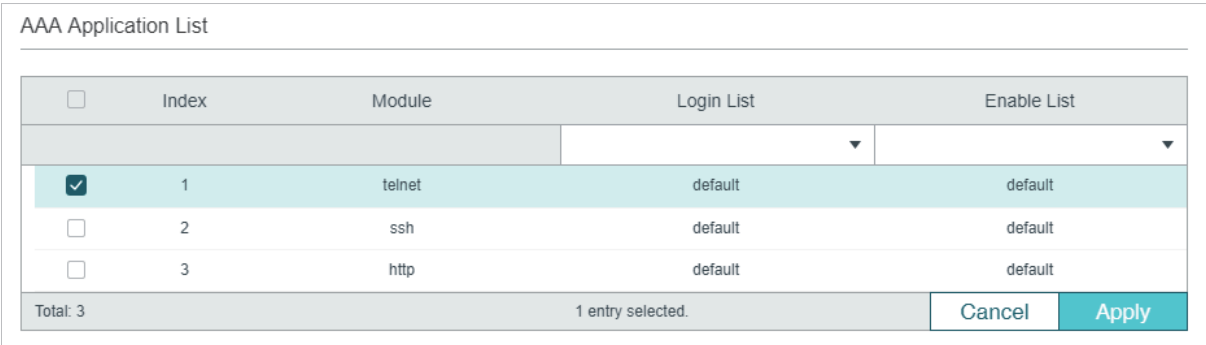
| Method List Name | Podaj nazwę metody.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Pri1- Pri4       | <p>Ustal kolejność metod uwierzytelniania. Metoda o priorytecie 1 posłuży do uwierzytelniania dostępu użytkownika jako pierwsza, metoda o priorytecie 2 jako kolejna, gdy poprzednia metoda zawiedzie, itd.</p> <p><b>local:</b> Skorzystaj z lokalnej bazy danych przełącznika do uwierzytelniania.</p> <p><b>none:</b> Brak uwierzytelniania.</p> <p><b>radius:</b> Skorzystaj ze zdalnego serwera/grup serwerów RADIUS.</p> <p><b>tacacs:</b> Skorzystaj ze zdalnego serwera/grup serwerów TACACS+.</p> <p><b>Other user-defined server groups:</b> Skorzystaj z grup serwerów zdefiniowanych przez użytkownika.</p> |

2) Kliknij **Create**, aby dodać nową metodę.

## 2.1.4 Konfiguracja listy aplikacji AAA

Wybierz z menu **SECURITY > AAA > Global Config**, aby wyświetlić poniższą stronę.

Rys. 2-7 Konfiguracja listy aplikacji



| <input type="checkbox"/>            | Index | Module | Login List | Enable List |
|-------------------------------------|-------|--------|------------|-------------|
| <input checked="" type="checkbox"/> | 1     | telnet | default    | default     |
| <input type="checkbox"/>            | 2     | ssh    | default    | default     |
| <input type="checkbox"/>            | 3     | http   | default    | default     |

Total: 3      1 entry selected.     

Wykonaj poniższe kroki, aby skonfigurować listę aplikacji AAA.

1) W sekcji **AAA Application List** wybierz opcję dostępu i skonfiguruj listę logowania i listę dostępu.

|             |                                                                                                                                                |
|-------------|------------------------------------------------------------------------------------------------------------------------------------------------|
| Module      | Konfigurowalne protokoły na przełączniku: telnet, ssh i http.                                                                                  |
| Login List  | Wybierz skonfigurowaną uprzednio listę metod logowania. Pozwoli ona uwierzytelniać użytkowników, którzy starają się zalogować na przełącznik.  |
| Enable List | Wybierz skonfigurowaną uprzednio listę metod dostępu. Pozwoli ona uwierzytelniać użytkowników, którzy chcą uzyskać uprawnienia administratora. |

2) Kliknij **Apply**.

## 2.1.5 Konfiguracja konta logowania i hasła dostępu

Konto logowania i hasło dostępu można skonfigurować lokalnie na przełączniku lub centralnie na serwerach RADIUS/TACACS+.

### ■ Na przełączniku

Lokalną nazwę użytkownika i hasło logowania można skonfigurować na stronie zarządzania kontami użytkowników. Szczegółowe informacje znajdziesz w rozdziale [Zarządzanie systemem](#).

Aby skonfigurować lokalne hasło dostępu do uzyskania uprawnień administratora, wybierz z menu **SECURITY > AAA > Global Config**, aby wyświetlić poniższą stronę.

Rys. 2-8 Konfiguracja hasła dostępu

Enable Admin

---

Enable Admin:  Clear Password  Set Password

Password:  (1-31 characters)

[Apply](#)

Dostępne są dwie opcje: **Clear Password** i **Set Password**. Możesz zdecydować czy hasło dostępu będzie wymagane od gości starających się uzyskać uprawnienia administratora. Kliknij **Apply**.

*Wskazówka:* Zalogowani goście mogą wpisać lokalne hasło dostępu, aby uzyskać uprawnienia administratora.

### ■ Na serwerze

Użytkownicy konta utworzonych poprzez serwer RADIUS/TACACS+ mogą tylko przeglądać ustawienia i informacje sieciowe bez hasła dostępu.

Zasady konfiguracji na serwerze są następujące:

- W przypadku konfiguracji uwierzytelniania logowaniem, na serwerze można utworzyć więcej niż jedno konto logowania. Ponadto, można także dostosować nazwę użytkownika i hasło.
- W przypadku konfiguracji hasła dostępu:

Na serwerze RADIUS nazwą użytkownika musi być **\$enable\$**, ale hasło dostępu jest konfigurowalne. Wszyscy użytkownicy, którzy chcą uzyskać uprawnienia administratora korzystają z tego hasła.

Na serwerze TACACS+ ustaw hasło logowania w pliku konfiguracyjnym, wpisując wartość "enable 15". Wszyscy użytkownicy, którzy chcą uzyskać uprawnienia administratora korzystają z tego hasła.

## 2.2 Przez CLI

### 2.2.1 Dodawanie serwerów

Na przełączniku możesz dodać jeden lub kilka serwerów RADIUS/TACACS+ do uwierzytelniania. Jeżeli dodasz kilka serwerów, serwer, który był dodany do grupy jako pierwszy ma najwyższy priorytet i odpowiada za uwierzytelnianie użytkowników starających się uzyskać dostęp do przełącznika. Kolejne serwery są serwerami zapasowymi, na wypadek awarii pierwszego serwera.

- Dodawania serwera RADIUS

Wykonaj poniższe kroki, aby dodać serwer RADIUS na przełączniku:

|        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Krok 1 | <p><b>configure</b></p> <p>Uruchom tryb konfiguracji globalnej.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Krok 2 | <p><b>radius-server host</b> <i>ip-address</i> [<b>auth-port</b> <i>port-id</i>] [<b>acct-port</b> <i>port-id</i>] [<b>timeout</b> <i>time</i>] [<b>retransmit</b> <i>number</i>] [<b>nas-id</b> <i>nas-id</i>] <b>key</b> {[ 0 ] <i>string</i>   7 <i>encrypted-string</i>}</p> <p>Dodaj serwer RADIUS i skonfiguruj odpowiednie parametry.</p> <p><b>host</b> <i>ip-address</i>: Podaj adres IP serwera z protokołem RADIUS.</p> <p><b>auth-port</b> <i>port-id</i>: Podaj numer portu docelowego UDP na serwerze RADIUS dla żądań uwierzytelniania. Domyślnym ustawieniem jest 1812.</p> <p><b>acct-port</b> <i>port-id</i>: Podaj numer portu docelowego UDP na serwerze RADIUS dla żądań rozliczania. Domyślną wartością jest 1813. Port ten zwykle stosuje się dla funkcji 802.1x.</p> <p><b>timeout</b> <i>time</i>: Podaj czas oczekiwania przełącznika na odpowiedź serwera przed ponownym wysłaniem żądania. Prawidłowe wartości wahają się od 1 do 9 sekund, a domyślnym ustawieniem jest 5 sekund.</p> <p><b>retransmit</b> <i>number</i>: Określ ile razy żądanie ma być wysłane do serwera, gdy serwer nie odpowiada. Prawidłowe wartości wahają się od 1 do 3, a domyślnym ustawieniem jest 2.</p> <p><b>nas-id</b> <i>nas-id</i>: Podaj nazwę NAS (Network Access Server), która zostanie umieszczona w pakiecie RADIUS dla łatwiejszej identyfikacji. Nazwa musi zawierać od 1 do 31 znaków. Domyślną wartością jest adres MAC przełącznika. Zasadniczo NAS określa sam przełącznik.</p> <p><b>key</b> {[ 0 ] <i>string</i>   7 <i>encrypted-string</i>}: Podaj wspólny klucz zabezpieczeń. 0 i 7 to dostępne typy szyfrowań. 0 oznacza klucz nieszyfrujący. 7 oznacza klucz szyfrowania symetrycznego, o stałej długości. Domyślnym ustawieniem jest 0. <i>string</i> jest wspólnym kluczem przełącznika i serwera, składającym się maksymalnie z 32 znaków. <i>encrypted-string</i> to klucz szyfrowania symetrycznego, o stałej długości, który można skopiować z pliku konfiguracyjnego innego przełącznika. Skonfigurowane klucze lub klucze szyfrowania wyświetlą się tutaj w postaci zaszyfrowanej.</p> |
| Krok 3 | <p><b>show radius-server</b></p> <p>Przejrzyj ustawienia serwera RADIUS.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Krok 4 | <p><b>end</b></p> <p>Powróć do trybu privileged EXEC.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |

---

Krok 5      **copy running-config startup-config**  
Zapisz ustawienia w pliku konfiguracyjnym.

---

Poniższy schemat przedstawia przykładowy sposób dodawania serwera RADIUS na przełączniku. Ustawionym adresem IP serwera będzie 192.168.0.10, portem uwierzytelniania 1812, wspólnym kluczem 123456, czasem oczekiwania 8 sekund, a liczbą ponownych wysłań żądania 3.

### Switch#configure

```
Switch(config)#radius-server host 192.168.0.10 auth-port 1812 timeout 8 retransmit 3
key 123456
```

### Switch(config)#show radius-server

| Server Ip    | Auth Port | Acct Port | Timeout | Retransmit | NAS Identifier | Shared key |
|--------------|-----------|-----------|---------|------------|----------------|------------|
| 192.168.0.10 | 1812      | 1813      | 5       | 2          | 000AEB132397   | 123456     |

### Switch(config)#end

### Switch#copy running-config startup-config

#### ■ Dodawanie serwera TACACS+

Wykonaj poniższe kroki, aby dodać serwer TACACS+ na przełączniku:

---

Krok 1      **configure**  
Uruchom tryb konfiguracji globalnej.

---

Krok 2      **tacacs-server host ip-address [ port port-id ] [ timeout time ] [ key { [ 0 ] string | 7 encrypted-string } ]**

Dodaj serwer RADIUS i skonfiguruj odpowiednie parametry.

**host ip-address:** Podaj adres IP serwera z protokołem TACACS+.

**port port-id:** Podaj numer portu docelowego UDP na serwerze TACAS+ dla żądań uwierzytelniania. Domyślnym ustawieniem jest 49.

**timeout time:** Podaj czas oczekiwania przełącznika na odpowiedź serwera przed ponownym wysłaniem żądania. Prawidłowe wartości wahają się od 1 do 9 sekund, a domyślnym ustawieniem jest 5 sekund.

**key { [ 0 ] string | 7 encrypted-string }:** Podaj wspólny klucz zabezpieczeń. 0 i 7 to dostępne typy szyfrowań. 0 oznacza klucz nieszyfrujący. 7 oznacza klucz szyfrowania symetrycznego, o stałej długości. Domyślnym ustawieniem jest 0. *string* jest wspólnym kluczem przełącznika i serwera, składającym się maksymalnie z 32 znaków. *encrypted-string* to klucz szyfrowania symetrycznego, o stałej długości, który można skopiować z pliku konfiguracyjnego innego przełącznika. Skonfigurowane klucze lub klucze szyfrowania wyświetlą się tutaj w postaci zaszyfrowanej.

---

Krok 3      **show tacacs-server**  
Przejrzyj ustawienia serwera TACACS+.

---



---

Krok 4      **end**  
Powróć do trybu privileged EXEC.

---

Krok 5      **copy running-config startup-config**  
Zapisz ustawienia w pliku konfiguracyjnym.

---

Poniższy schemat przedstawia przykładowy sposób dodawania serwera TACACS+ na przełączniku. Ustawionym adresem IP serwera będzie 192.168.0.20, portem uwierzytelniania 49, wspólnym kluczem 123456, a czasem oczekiwania 8 sekund.

### Switch#configure

**Switch(config)#tacacs-server host 192.168.0.20 auth-port 49 timeout 8 key 123456**

### Switch(config)#show tacacs-server

| Server Ip    | Port | Timeout | Shared key |
|--------------|------|---------|------------|
| 192.168.0.20 | 49   | 8       | 123456     |

### Switch(config)#end

**Switch#copy running-config startup-config**

## 2.2.2 Konfiguracja grup serwerów

Przełącznik ma dwie wbudowane grupy serwerów, jeden dla serwerów RADIUS, a drugi dla serwerów TACACS+. Serwery korzystające z tego samego protokołu są automatycznie dodawane do domyślnej grupy serwerów. Możesz dodawać nowe grupy serwerów, jeżeli uznasz to za potrzebne.

Dwie domyślne grupy serwerów nie mogą być usunięte, ani edytowane. Wykonaj poniższe kroki, aby dodać grupę serwerów:

---

Krok 1      **configure**  
Uruchom tryb konfiguracji globalnej.

---

Krok 2      **aaa group { radius | tacacs } group-name**  
Utwórz grupę serwerów.  
  
*radius | tacacs:* Podaj typ grupy.  
  
*group-name:* Podaj nazwę grupy.

---

Krok 3      **server ip-address**  
Dodaj istniejące serwery do grup serwerów.  
  
*ip-address:* Podaj adres IP serwera, który ma być dodany do grupy.

---

|        |                                                                                         |
|--------|-----------------------------------------------------------------------------------------|
| Krok 4 | <b>show aaa group [ group-name ]</b><br>Przejrzyj ustawienia grup serwerów.             |
| Krok 5 | <b>end</b><br>Powróć do trybu privileged EXEC.                                          |
| Step 6 | <b>copy running-config startup-config</b><br>Zapisz ustawienia w pliku konfiguracyjnym. |

Poniższy schemat przedstawia przykładowy sposób tworzenia grupy serwera RADIUS o nazwie RADIUS1 i dodawania do grupy dwóch istniejących serwerów RADIUS, których adresami IP są odpowiednio 192.168.0.10 i 192.168.0.20.

**Switch#configure**

**Switch(config)#aaa group radius RADIUS1**

**Switch(aaa-group)#server 192.168.0.10**

**Switch(aaa-group)#server 192.168.0.20**

**Switch(aaa-group)#show aaa group RADIUS1**

192.168.0.10

192.168.0.20

**Switch(aaa-group)#end**

**Switch#copy running-config startup-config**

### 2.2.3 Konfiguracja listy metod

Lista metod opisuje metody uwierzytelniania i kolejność, w jakiej są używane do uwierzytelniania dostępu użytkowników. Przełącznik obsługuje listę metod logowania dla wszystkich użytkowników, którzy chcą uzyskać dostęp do przełącznika i oraz listę metod dostępu dla gości, którzy chcą uzyskać uprawnienia administratora.

Wykonaj poniższe kroki, aby skonfigurować listę metod:

|        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Krok 1 | <b>configure</b><br>Uruchom tryb konfiguracji globalnej.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Krok 2 | <b>aaa authentication login { method-list } { method1 } [ method2 ] [ method3 ] [ method4 ]</b><br>Skonfiguruj listę metod logowania.<br><br><i>method-list</i> : Podaj nazwę listy metod.<br><br><i>method1/method2/method3/method4</i> : Ustal kolejność metod uwierzytelniania. Metoda o priorytecie 1 posłuży do uwierzytelniania dostępu użytkownika jako pierwsza, metoda o priorytecie 2 jako kolejna, gdy poprzednia metoda zawiedzie, itd. Metodami domyślnymi są radius, tacacs, local i none. None oznacza brak uwierzytelniania logowania użytkowników. |

|        |                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Krok 3 | <b>aaa authentication enable { method-list } { method1 } [ method2 ] [ method3 ] [ method4 ]</b><br>Skonfiguruj listę metod hasła dostępu.<br><br><i>method-list</i> : Podaj nazwę listy metod.<br><br><i>method1/method2/method3/method4</i> : Ustal kolejność metod uwierzytelniania. Metodami domyślnymi są radius, tacacs, local i none. None oznacza brak uwierzytelniania dla użytkowników, którzy chcą uzyskać uprawnienia administratora. |
| Krok 4 | <b>show aaa authentication [ login   enable ]</b><br>Przejrzyj ustawienia listy metod.                                                                                                                                                                                                                                                                                                                                                            |
| Krok 5 | <b>end</b><br>Powróć do trybu privileged EXEC.                                                                                                                                                                                                                                                                                                                                                                                                    |
| Krok 6 | <b>copy running-config startup-config</b><br>Zapisz ustawienia w pliku konfiguracyjnym.                                                                                                                                                                                                                                                                                                                                                           |

Poniższy schemat przedstawia przykładowy sposób tworzenia listy metod logowania o nazwie Login1 i ustawiania method 1 jako domyślnej grupy serwerów RADIUS i method 2 jako local.

#### Switch#configure

**Switch(config)##aaa authentication login Login1 radius local**

**Switch(config)#show aaa authentication login**

| Methodlist | pri1   | pri2  | pri3 | pri4 |
|------------|--------|-------|------|------|
| default    | local  | --    | --   | --   |
| Login1     | radius | local | --   | --   |

**Switch(config)#end**

**Switch#copy running-config startup-config**

Poniższy schemat przedstawia przykładowy sposób tworzenia listy metod hasła dostępu o nazwie Enable1 i ustawiania method 1 jako domyślnej grupy serwerów RADIUS i method 2 jako local.

#### Switch#configure

**Switch(config)##aaa authentication enable Enable1 radius local**

**Switch(config)#show aaa authentication enable**

| Methodlist | pri1  | pri2 | pri3 | pri4 |
|------------|-------|------|------|------|
| default    | local | --   | --   | --   |

```
Enable1 radius local -- --
```

```
Switch(config)#end
```

```
Switch#copy running-config startup-config
```

## 2.2.4 Konfiguracja listy aplikacji AAA

Możesz skonfigurować listy metod uwierzytelniania poprzez następujące aplikacje dostępu: Telnet, SSH i HTTP.

### ■ Telnet

Wykonaj poniższe kroki, aby powiązać listy metod logowania i hasła dostępu z Telnet:

|        |                                              |                                                                                                               |
|--------|----------------------------------------------|---------------------------------------------------------------------------------------------------------------|
| Krok 1 | <b>configure</b>                             | Uruchom tryb konfiguracji globalnej.                                                                          |
| Krok 2 | <b>line telnet</b>                           | Uruchom tryb konfiguracji łącza.                                                                              |
| Krok 3 | <b>login authentication { method-list }</b>  | Powiąz listę metod logowania z Telnet.<br><br><i>method-list</i> : Podaj nazwę listy metod logowania.         |
| Krok 4 | <b>enable authentication { method-list }</b> | Powiąz listę metod hasła dostępu z Telnet.<br><br><i>method-list</i> : Podaj nazwę listy metod hasła dostępu. |
| Krok 5 | <b>show aaa global</b>                       | Przejrzyj ustawienia list aplikacji.                                                                          |
| Krok 6 | <b>end</b>                                   | Powróć do trybu privileged EXEC.                                                                              |
| Krok 7 | <b>copy running-config startup-config</b>    | Zapisz ustawienia w pliku konfiguracyjnym.                                                                    |

Poniższy schemat przedstawia przykładowy sposób wiązania istniejącej listy metod logowania o nazwie Login1 i listy metod hasła dostępu o nazwie Enable1 z Telnet.

```
Switch#configure
```

```
Switch(config)#line telnet
```

```
Switch(config-line)#login authentication Login1
```

```
Switch(config-line)#enable authentication Enable1
```

**Switch(config-line)#show aaa global**

|        |            |             |
|--------|------------|-------------|
| Module | Login List | Enable List |
| Telnet | Login1     | Enable1     |
| Ssh    | default    | default     |
| Http   | default    | default     |

**Switch(config-line)#end****Switch#copy running-config startup-config**

- SSH

Wykonaj poniższe kroki, aby powiązać listy metod logowania i hasła dostępu z SSH:

|        |                                                                                                                                                                   |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Krok 1 | <b>configure</b><br>Uruchom tryb konfiguracji globalnej.                                                                                                          |
| Krok 2 | <b>line ssh</b><br>Uruchom tryb konfiguracji łącza.                                                                                                               |
| Krok 3 | <b>login authentication { <i>method-list</i> }</b><br>Powiąż listę metod logowania z SSH.<br><br><i>method-list</i> : Podaj nazwę listy metod logowania.          |
| Krok 4 | <b>enable authentication { <i>method-list</i> }</b><br>Powiąż listę metod hasła dostępu z SSH.<br><br><i>method-list</i> : Podaj nazwę listy metod hasła dostępu. |
| Krok 5 | <b>show aaa global</b><br>Przejrzyj ustawienia list aplikacji.                                                                                                    |
| Krok 6 | <b>end</b><br>Powróć do trybu privileged EXEC.                                                                                                                    |
| Krok 7 | <b>copy running-config startup-config</b><br>Zapisz ustawienia w pliku konfiguracyjnym.                                                                           |

Poniższy schemat przedstawia przykładowy sposób wiązania istniejącej listy metod logowania o nazwie Login1 i listy metod hasła dostępu o nazwie Enable1 z SSH.

**Switch#configure****Switch(config)#line ssh****Switch(config-line)#login authentication Login1****Switch(config-line)#enable authentication Enable1**

**Switch(config-line)#show aaa global**

|        |            |             |
|--------|------------|-------------|
| Module | Login List | Enable List |
| Telnet | default    | default     |
| Ssh    | Login1     | Enable1     |
| Http   | default    | default     |

**Switch(config-line)#end****Switch#copy running-config startup-config**

## ■ HTTP

Wykonaj poniższe kroki, aby powiązać listy metod logowania i hasła dostępu z HTTP:

|        |                                                                                                                                                                     |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Krok 1 | <b>configure</b><br>Uruchom tryb konfiguracji globalnej.                                                                                                            |
| Krok 2 | <b>ip http login authentication { method-list }</b><br>Powiąż listę metod logowania z HTTP.<br><br><i>method-list</i> : Podaj nazwę listy metod logowania.          |
| Krok 3 | <b>ip http enable authentication { method-list }</b><br>Powiąż listę metod hasła dostępu z HTTP.<br><br><i>method-list</i> : Podaj nazwę listy metod hasła dostępu. |
| Krok 4 | <b>show aaa global</b><br>Przejrzyj ustawienia list aplikacji.                                                                                                      |
| Krok 5 | <b>end</b><br>Powróć do trybu privileged EXEC.                                                                                                                      |
| Krok 6 | <b>copy running-config startup-config</b><br>Zapisz ustawienia w pliku konfiguracyjnym.                                                                             |

Poniższy schemat przedstawia przykładowy sposób wiązania istniejącej listy metod logowania o nazwie Login1 i listy metod hasła dostępu o nazwie Enable1 z HTTP:

**Switch#configure**

```
Switch(config)#ip http login authentication Login1
```

```
Switch(config)#ip http enable authentication Enable1
```

**Switch(config)#show aaa global**

|        |            |             |
|--------|------------|-------------|
| Module | Login List | Enable List |
| Telnet | default    | default     |

|      |         |         |
|------|---------|---------|
| Ssh  | default | default |
| Http | Login1  | Enable1 |

**Switch(config)#end**

**Switch#copy running-config startup-config**

## 2.2.5 Konfiguracja konta logowania i hasła dostępu

Konto logowania i hasło dostępu można skonfigurować lokalnie na przełączniku lub centralnie na serwerach RADIUS/TACACS+.

### ■ Na przełączniku

Lokalną nazwę użytkownika i hasło logowania można skonfigurować na stronie zarządzania kontami użytkowników. Szczegółowe informacje znajdziesz w rozdziale [Zarządzanie systemem](#).

Wykonaj poniższe kroki, aby skonfigurować lokalne hasło dostępu do uzyskania uprawnień administratora:

|        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Krok 1 | <b>configure</b><br>Uruchom tryb konfiguracji globalnej.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Krok 2 | <b>enable admin password { [0] password   7 encrypted-password }</b><br>Ustaw hasło dostępu. To polecenia korzysta z szyfrowania symetrycznego.<br><br>0 i 7 to dostępne typy szyfrowań. 0 oznacza klucz nieszyfrujący. 7 oznacza klucz szyfrowania symetrycznego o stałej długości. Domyślnym ustawieniem jest 0. <i>password</i> jest wspólnym kluczem przełącznika i serwera, składającym się maksymalnie z 32 znaków. <i>encrypted-password</i> to klucz szyfrowania symetrycznego o stałej długości, który można skopiować z pliku konfiguracyjnego innego przełącznika. Skonfigurowane klucze lub klucze szyfrowania wyświetlą się tutaj w postaci zaszyfrowanej.<br><br><b>enable admin secret { [0] password   5 encrypted-password }</b><br>Ustaw hasło dostępu. To polecenia korzysta z szyfrowania MD5.<br><br>0 i 5 to dostępne typy szyfrowań. 0 oznacza klucz nieszyfrujący. 5 oznacza szyfrowanie MD5 o stałej długości. Domyślnym ustawieniem jest 0. <i>password</i> jest ciągiem 1 - 31 znaków alfanumerycznych lub symboli. <i>encrypted-password</i> jest hasłem szyfrowanym MD5 o stałej długości, które można skopiować z pliku konfiguracyjnego innego przełącznika. |
| Krok 3 | <b>end</b><br>Powróć do trybu uprzywilejowanego (privileged EXEC mode).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Krok 4 | <b>copy running-config startup-config</b><br>Zapisz ustawienia w pliku konfiguracyjnym.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |

### ■ Na serwerze

Użytkownicy konta utworzonych poprzez serwer RADIUS/TACACS+ mogą tylko przeglądać ustawienia i informacje sieciowe bez hasła dostępu.

Zasady konfiguracji na serwerze są następujące:

- W przypadku konfiguracji uwierzytelniania logowaniem, na serwerze można utworzyć więcej niż jedno konto logowania. Ponadto, można także dostosować nazwę użytkownika i hasło.
- W przypadku konfiguracji hasła dostępu:

Na serwerze RADIUS nazwą użytkownika musi być **\$enable\$**, ale hasło dostępu jest konfigurowalne. Wszyscy użytkownicy, którzy chcą uzyskać uprawnienia administratora korzystają z tego hasła.

Na serwerze TACACS+ ustaw hasło logowania w pliku konfiguracyjnym, wpisując wartość "enable 15". Wszyscy użytkownicy, którzy chcą uzyskać uprawnienia administratora korzystają z tego hasła.

*Wskazówka:* Korzystając z polecenia **enable-admin** zalogowani goście mogą podać hasło dostępu i uzyskać uprawnienia administratora.



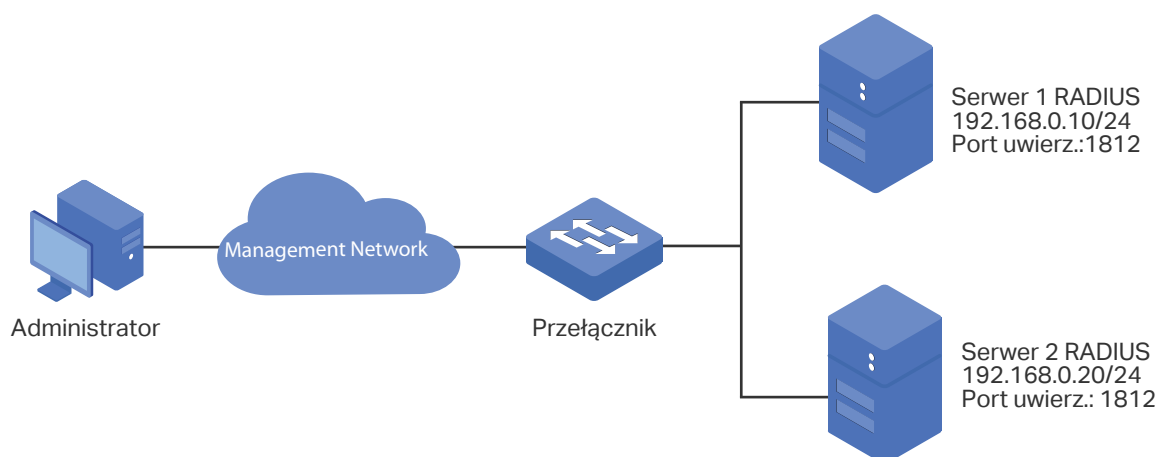
# 3 Przykład konfiguracji

## 3.1 Wymagania sieciowe

Jak pokazano poniżej, przełącznik ma być zarządzany zdalnie poprzez Telnet. Ponadto starszy administrator w firmie chce utworzyć konto dla młodszych administratorów, aby zapewnić im dostęp tylko do informacji konfiguracyjnych i wybranych informacji sieciowych bez podawania hasła dostępu.

W sieci są dwa serwery RADIUS, aby zapewnić wyższe bezpieczeństwo uwierzytelniania administratorów, którzy próbują się zalogować lub uzyskać uprawnienia administracyjne. Jeśli serwer 1 RADIUS ulegnie awarii i nie będzie odpowiadać na żądania uwierzytelnienia, serwer 2 RADIUS przejmie jego rolę, aby zapewnić stabilność systemu uwierzytelniania.

Rys. 3-1 Topologia sieci



## 3.2 Schemat konfiguracji

Aby spełnić ten warunek, starszy administrator może utworzyć konto logowania i hasło dostępu do dwóch serwerów RADIUS oraz skonfigurować na przełączniku funkcję AAA. Adresy IP serwerów RADIUS to odpowiednio 192.168.0.10/24 i 192.168.0.20/24; numer portu uwierzytelniającego to 1812; klucz dzielony to 123456.

Kroki konfiguracji przełącznika są następujące:

- 1) Dodaj na przełączniku dwa serwery RADIUS.
- 2) Utwórz nową grupę serwera RADIUS i dodaj do tej grupy dwa serwery. Upewnij się, że serwer 1 RADIUS ma pierwszeństwo uwierzytelniania.
- 3) Skonfiguruj listę metod.
- 4) Skonfiguruj listę aplikacji AAA.

W poniższych podrozdziałach opisano dwa sposoby przeprowadzenia procedury konfiguracji: przez GUI oraz przez CLI.

### 3.3 Przez GUI

- 1) Wybierz z menu **SECURITY > AAA > RADIUS Config** i kliknij **+ Add**, aby wyświetlić poniższą stronę. Ustaw adres IP serwera jako 192.168.0.10, klucz dzielony jako 123456, port uwierzytelniania jako 1812, a inne parametry pozostaw domyślne. Kliknij **Create**, aby dodać Serwer 1 RADIUS na przełączniku.

Rys. 3-2 Dodawanie serwera 1 RADIUS

**RADIUS Server**

|                      |                                           |                                                                                             |
|----------------------|-------------------------------------------|---------------------------------------------------------------------------------------------|
| Server IP:           | <input type="text" value="192.168.0.10"/> | (Format:192.168.0.1)                                                                        |
| Shared Key:          | <input type="text" value="123456"/>       | 1-32 characters. Only numbers, letters and the following symbols are allowed: - . / : @ _ . |
| Authentication Port: | <input type="text" value="1812"/>         | (1-65535)                                                                                   |
| Accounting Port:     | <input type="text" value="1813"/>         | (1-65535)                                                                                   |
| Retransmit:          | <input type="text" value="2"/>            | (1-3)                                                                                       |
| Timeout:             | <input type="text" value="5"/>            | seconds (1-9)                                                                               |
| NAS Identifier:      | <input type="text"/>                      | (Optional)                                                                                  |

- 2) Kliknij **+ Add**, aby wyświetlić poniższą stronę. Ustaw IP serwera jako 192.168.0.20, klucz dzielony jako 123456, port uwierzytelniania jako 1812, a inne parametry pozostaw domyślne. Kliknij **Create**, aby dodać Serwer 2 RADIUS na przełączniku

Rys. 3-3 Dodawanie serwer 2 RADIUS

**RADIUS Server**

|                      |                                           |                                                                                             |
|----------------------|-------------------------------------------|---------------------------------------------------------------------------------------------|
| Server IP:           | <input type="text" value="192.168.0.20"/> | (Format:192.168.0.1)                                                                        |
| Shared Key:          | <input type="text" value="123456"/>       | 1-32 characters. Only numbers, letters and the following symbols are allowed: - . / : @ _ . |
| Authentication Port: | <input type="text" value="1812"/>         | (1-65535)                                                                                   |
| Accounting Port:     | <input type="text" value="1813"/>         | (1-65535)                                                                                   |
| Retransmit:          | <input type="text" value="2"/>            | (1-3)                                                                                       |
| Timeout:             | <input type="text" value="5"/>            | seconds (1-9)                                                                               |
| NAS Identifier:      | <input type="text"/>                      | (Optional)                                                                                  |

- 3) Wybierz z menu **SECURITY > AAA > Server Group**, aby wyświetlić poniższą stronę. Kliknij **+ Add**. Ustaw nazwę grupy jako RADIUS1, a typ serwera jako RADIUS. Wybierz z listy adres 192.168.0.10 i 192.168.0.20. Kliknij **Create**, aby utworzyć grupę serwera.

Rys. 3-4 Tworzenie grupy serwera

The screenshot shows the 'Server Group' configuration interface. It features a teal header with the title 'Server Group'. Below the header, there are three input fields: 'Server Group' (text input with value 'RADIUS1' and a '(1-15 characters)' label), 'Server Type' (dropdown menu with value 'RADIUS'), and 'Server IP' (dropdown menu with value '192.168.0.10,192.168.0.20'). At the bottom right, there are two buttons: 'Cancel' and 'Create'.

- 4) Wybierz z menu **SECURITY > AAA > Method List** i kliknij **+ Add** w sekcji **Authentication Login Method List**. Ustaw nazwę listy metod jako MethodLogin, a Pri1 jako RADIUS1. Kliknij **Create**, aby ustawić listę metod uwierzytelniania logowania.

Rys. 3-5 Konfiguracja listy metod logowania

The screenshot shows the 'Authentication Login Method' configuration interface. It features a teal header with the title 'Authentication Login Method'. Below the header, there are five input fields: 'Method List Name' (text input with value 'MethodLogin' and a '(1-15 characters)' label), 'Pri1' (dropdown menu with value 'RADIUS1'), 'Pri2' (dropdown menu with value '--'), 'Pri3' (dropdown menu with value '--'), and 'Pri4' (dropdown menu with value '--'). At the bottom right, there are two buttons: 'Cancel' and 'Create'.

- 5) Na tej samej stronie kliknij **+ Add** w sekcji **Authentication Enable Method List**. Ustaw nazwę listy metod jako MethodEnable, a Pri1 jako RADIUS1. Kliknij **Create**, aby ustawić listę metod do uwierzytelniania hasła dostępu.

Rys. 3-6 Konfiguracja listy metod hasła dostępu

**Authentication Enable Method**

Method List Name:  (1-15 characters)

Pri1:

Pri2:

Pri3:

Pri4:

- 6) Wybierz z menu **SECURITY > AAA > Global Config**, aby wyświetlić poniższą stronę. W sekcji **AAA Application List** wybierz telnet i ustaw listę logowania jako Method-Login, a listę dostępu jako Method-Enable. Następnie kliknij **Apply**.

Rys. 3-6 Konfiguracja listy aplikacji AAA

**AAA Application List**

| <input type="checkbox"/>            | Index | Module | Login List  | Enable List  |
|-------------------------------------|-------|--------|-------------|--------------|
| <input checked="" type="checkbox"/> | 1     | telnet | MethodLogin | MethodEnable |
| <input type="checkbox"/>            | 2     | ssh    | default     | default      |
| <input type="checkbox"/>            | 3     | http   | default     | default      |

Total: 3      1 entry selected.     

- 7) Kliknij  **Save**, aby zapisać ustawienia.

## 3.4 Przez CLI

- 1) Dodaj Serwer 1 RADIUS i Serwer 2 RADIUS na przełączniku.

```
Switch(config)#radius-server host 192.168.0.10 auth-port 1812 key 123456
```

```
Switch(config)#radius-server host 192.168.0.20 auth-port 1812 key 123456
```

- 2) Utwórz nową grupę serwera o nazwie RADIUS1 i dodaj dwa serwery RADIUS do grupy serwera.

```
Switch(config)#aaa group radius RADIUS1
```

```
Switch(aaa-group)#server 192.168.0.10
```

```
Switch(aaa-group)#server 192.168.0.20
```

```
Switch(aaa-group)#exit
```

- 3) Utwórz dwie listy metod: Method-Login oraz Method-Enable i ustaw grupę serwera RADIUS1 jako metodę uwierzytelniania dla tych dwóch list metod.

```
Switch(config)#aaa authentication login Method-Login RADIUS1
```

```
Switch(config)#aaa authentication enable Method-Enable RADIUS1
```

- 4) Ustaw Method-Login oraz Method-Enable jako metody uwierzytelniania dla aplikacji Telnet.

```
Switch(config)#line telnet
```

```
Switch(config-line)#login authentication Method-Login
```

```
Switch(config-line)#enable authentication Method-Enable
```

```
Switch(config-line)#end
```

```
Switch#copy running-config startup-config
```

### Sprawdzanie konfiguracji

Sprawdzanie konfiguracji serwerów RADIUS:

```
Switch#show radius-server
```

| Server Ip    | Auth Port | Acct Port | Timeout | Retransmit | NAS Identifier | Shared key |
|--------------|-----------|-----------|---------|------------|----------------|------------|
| 192.168.0.10 | 1812      | 1813      | 5       | 2          | 000AEB132397   | 123456     |
| 192.168.0.20 | 1812      | 1813      | 5       | 2          | 000AEB132397   | 123456     |

Sprawdzanie konfiguracji grupy serwera RADIUS1:

```
Switch#show aaa group RADIUS1
```

```
192.168.0.10
```

```
192.168.0.20
```

Sprawdzanie konfiguracji listy metod:

```
Switch#show aaa authentication
```

Authentication Login Methodlist:

| Methodlist   | pri1    | pri2 | pri3 | pri4 |
|--------------|---------|------|------|------|
| default      | local   | --   | --   | --   |
| Method-Login | RADIUS1 | --   | --   | --   |

Authentication Enable Methodlist:

| Methodlist | pri1 | pri2 | pri3 | pri4 |
|------------|------|------|------|------|
|            |      |      |      |      |

```
default none -- -- --
Method-Enable RADIUS1 -- -- --
...
```

Sprawdzanie stanu funkcji AAA i konfiguracji listy aplikacji AAA:

```
Switch#show aaa global
```

| Module | Login List   | Enable List   |
|--------|--------------|---------------|
| Telnet | Method-Login | Method-Enable |
| SSH    | default      | default       |
| Http   | default      | default       |

# Część 21

## Konfiguracja 802.1x

### ROZDZIAŁY

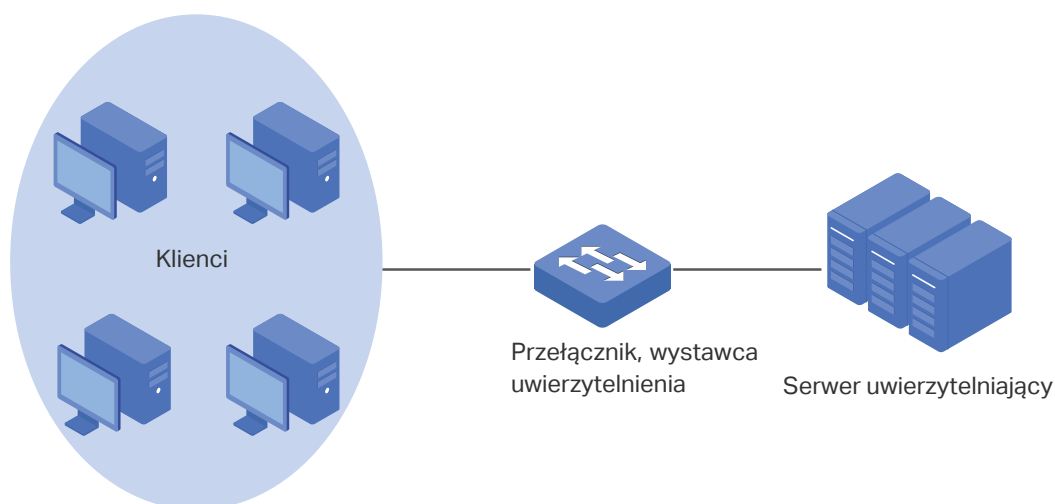
1. Informacje ogólne
2. Konfiguracja 802.1x
3. Przykład konfiguracji

# 1 Informacje ogólne

802.1x to protokół opartej na portach kontroli dostępu do sieci. Stosowany jest do uwierzytelniania i kontroli dostępu urządzeń podłączonych do portów. Jeśli urządzenie podłączone do portu zostanie uwierzytelnione przez serwer uwierzytelniający, jego żądanie dostępu do sieci LAN zostanie zaakceptowane; jeśli nie zostanie uwierzytelnione, żądanie zostanie odrzucone.

Uwierzytelnianie 802.1x jest oparte na modelu klient-serwer, w którym urządzenia przyjmują trzy typy ról: client/supplicant, authenticator i authentication server. Przedstawiono to na poniższym schemacie:

Rys. 1-1 Model uwierzytelniania 802.1x



## ■ Client

Klient, zwykle komputer podłączony jest do urządzenia authenticator poprzez port fizyczny. Zaleca się zainstalować oprogramowanie klienckie TP-Link 802.1x authentication na hostach klienckich, gdyż umożliwi im to wysyłanie żądań uwierzytelnienia 802.1x dostępu do sieci LAN.

## ■ Authenticator

Wystawcą uwierzytelnienia jest zwykle urządzenie sieciowe z obsługą protokołu 802.1x. Jak pokazano na poniższym schemacie, wystawcą uwierzytelnienia jest przełącznik.

Wystawca uwierzytelnienia pełni rolę serwera pośredniczącego pomiędzy klientem a serwerem uwierzytelniającym. Wystawca uwierzytelnienia żąda informacji o użytkowniku od klienta i wysyła go do serwera uwierzytelniającego; odbiera on także odpowiedzi od serwera uwierzytelniającego i wysyła je z powrotem do klienta. Wystawca uwierzytelnienia zezwala na dostęp do sieci LAN uwierzytelnionym klientom poprzez podłączone porty, natomiast do klientów niewierzytelnionych wysyła odmowę dostępu.



- Authentication Server

Serwer uwierzytelniający to zwykle host, który obsługuje program serwera RADIUS. Gromadzi informacje o klientach, potwierdza legalność klienta i informuje wystawcę uwierzytelnienia o stanie uwierzytelnienia danego klienta.

## 2 Konfiguracja 802.1x

Aby przeprowadzić konfigurację 802.1x, wykonaj poniższe kroki:

- 1) Skonfiguruj serwer RADIUS.
- 2) Skonfiguruj globalnie 802.1x.
- 3) Skonfiguruj 802.1x na portach.

Dodatkowo możesz sprawdzić stan wystawcy uwierzytelnienia.

### Wytyczne konfiguracyjne


Uwierzytelnianie 802.1x i funkcja Port Security nie mogą być jednocześnie włączone. Przed włączeniem uwierzytelniania 802.1x upewnij się, że funkcja Port Security jest wyłączona.

## 2.1 Przez GUI

### 2.1.1 Konfiguracja serwera RADIUS

Skonfiguruj parametry i grupę serwera RADIUS.

- Dodawanie serwera RADIUS

Wybierz z menu **SECURITY > AAA > RADIUS Config** i kliknij  **Add**, aby wyświetlić poniższą stronę.

Rys. 2-1 Dodawanie serwera RADIUS

**RADIUS Server**

|                      |                                   |                                                                                             |
|----------------------|-----------------------------------|---------------------------------------------------------------------------------------------|
| Server IP:           | <input type="text"/>              | (Format:192.168.0.1)                                                                        |
| Shared Key:          | <input type="text"/>              | 1-32 characters. Only numbers, letters and the following symbols are allowed: - . / : @ _ . |
| Authentication Port: | <input type="text" value="1812"/> | (1-65535)                                                                                   |
| Accounting Port:     | <input type="text" value="1813"/> | (1-65535)                                                                                   |
| Retransmit:          | <input type="text" value="2"/>    | (1-3)                                                                                       |
| Timeout:             | <input type="text" value="5"/>    | seconds (1-9)                                                                               |
| NAS Identifier:      | <input type="text"/>              | (Optional)                                                                                  |

Wykonaj poniższe kroki, aby dodać serwer RADIUS:

## 1) Skonfiguruj parametry serwera RADIUS.

|                     |                                                                                                                                                                                                                                                              |
|---------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Server IP           | Wprowadź adres IP serwera obsługującego protokół RADIUS.                                                                                                                                                                                                     |
| Shared Key          | Wprowadź klucz wspólny dla serwera RADIUS i przełącznika. Serwer RADIUS i przełącznik wykorzystują ciąg klucza do szyfrowania haseł i wymiany odpowiedzi.                                                                                                    |
| Authentication Port | Wyznacz na serwerze RADIUS port docelowy UDP do żądań uwierzytelniania. Ustawienie domyślne to 1812.                                                                                                                                                         |
| Accounting Port     | Wyznacz na serwerze RADIUS port docelowy UDP do żądań rozliczania. Ustawienie domyślne to 1813.                                                                                                                                                              |
| Retransmit          | Wyznacz, ile razy ponawiane będzie wysyłanie żądania na serwer w przypadku braku odpowiedzi serwera. Ustawienie domyślne to 2.                                                                                                                               |
| Timeout             | Wyznacz, ile czasu przełącznik będzie czekał na odpowiedź serwera przed ponownym wysłaniem żądania. Ustawienie domyślne to 5 s.                                                                                                                              |
| NAS Identifier      | Ustaw nazwę NAS (Network Access Server), która będzie zawarta w pakietach RADIUS w celu identyfikacji. Nazwa powinna zawierać od 1 do 31 znaków. Domyślnie jako nazwa ustawiony jest adres MAC przełącznika. Zwykle serwer NAS sam identyfikuje przełącznik. |

2) Kliknij **Apply**.

- Konfiguracja grupy serwera RADIUS

Wybierz z menu **SECURITY > AAA > Server Group**, aby wyświetlić poniższą stronę.

Rys. 2-2 Dodawanie grupy serwera

| Server Group List        |    |              |             |           |           |
|--------------------------|----|--------------|-------------|-----------|-----------|
| <input type="checkbox"/> | ID | Server Group | Server Type | Server IP | Operation |
| <input type="checkbox"/> | 1  | radius       | RADIUS      |           |           |
| <input type="checkbox"/> | 2  | tacacs       | TACACS+     |           |           |
| Total: 2                 |    |              |             |           |           |

Wykonaj poniższe kroki, aby dodać serwer RADIUS do grupy serwera:

- 1) Kliknij aby edytować domyślną grupę serwera RADIUS lub kliknij **Add**, aby dodać nową grupę serwera.

W przypadku kliknięcia , pojawi się poniższe okno. Wybierz serwer RADIUS i kliknij **Save**.

Rys. 2-3 Edytowanie grupy serwera

W przypadku kliknięcia **+** **Add** pojawi się następujące okno. Ustaw nazwę grupy serwera, wybierz typ serwera jako RADIUS i wybierz adres IP serwera RADIUS. Kliknij **Save**.

Rys. 2-4 Dodawanie grupy serwera

### ■ Konfiguracja listy Dot1x

Wybierz z menu **SECURITY > AAA > Dot1x List**, aby wyświetlić poniższą stronę.

Rys. 2-5 Konfiguracja listy Dot1x

Wykonaj poniższe kroki, aby skonfigurować grupy serwera RADIUS do uwierzytelniania 802.1x i kontroli dostępu:

- 1) W sekcji **Authentication Dot1x Method** z rozwijanej listy Pri1 wybierz grupę serwera RADIUS do uwierzytelniania i kliknij **Apply**.

- 2) W sekcji **Accounting Dot1x Method** z rozwijanej listy Pri1 wybierz grupę serwera RADIUS do kontroli dostępu i kliknij **Apply**.

## 2.1.2 Konfiguracja globalna 802.1x

Wybierz z menu **SECURITY > 802.1x > Global Config**, aby wyświetlić poniższą stronę.

Rys. 2-6 Konfiguracja globalna

Global Config

---

802.1x:  Enable

Authentication Protocol: EAP ▼

Accounting:  Enable

Handshake:  Enable

VLAN Assignment:  Enable

Apply

Wykonaj poniższe kroki, aby skonfigurować globalne parametry 802.1x:

- 1) W sekcji **Global Config** skonfiguruj następujące parametry.

|               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|---------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 802.1x        | Włącz lub wyłącz 802.1x globalnie.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Auth Protocol | <p>Wybierz protokół uwierzytelniania 802.1x.</p> <p><b>PAP:</b> System uwierzytelniania 802.1x wykorzystuje pakiety EAP do wymiany informacji między przełącznikiem i klientem. Przekazywanie pakietów EAP (Extensible Authentication Protocol) jest zakończone na przełączniku, a pakiety EAP konwertowane są do innych pakietów protokołu (takich jak RADIUS) i przekazywane do serwera uwierzytelniania.</p> <p><b>EAP:</b> System uwierzytelniania 802.1x wykorzystuje pakiety EAP do wymiany informacji między przełącznikiem i klientem. Pakiety EAP z danymi uwierzytelniania są kondensowane w pakietach zaawansowanego protokołu (takich jak RADIUS) i przekazywane do serwera uwierzytelniania.</p> |
| Accounting    | Włącz lub wyłącz funkcję kontroli dostępu 802.1x.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Handshake     | Włącz lub wyłącz funkcję Handshake. Funkcja służy do wykrywania stanu połączenia między TP-Link 802.1x Client i przełącznikiem. Wyłącz funkcję Handshake, jeżeli korzystasz z innych oprogramowań niż TP-Link 802.1x Client.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |

## VLAN Assignment

Włącz lub wyłącz funkcję przydziału VLAN 802.1x. Przydział VLAN 802.1x to technologia umożliwiająca serwerowi RADIUS wysłanie przydziału VLAN do portu po jego uwierzytelnieniu.

Jeżeli przypisanego VLAN nie ma na przełączniku, przełącznik automatycznie utworzy powiązany VLAN, doda do niego port uwierzytelniania i zmieni PVID oparty na przydzielonym VLAN.

Jeżeli przydzielony VLAN istnieje na przełączniku, zamiast tworzyć nowy VLAN, przełącznik bezpośrednio doda port uwierzytelniania do powiązanego VLAN i zmieni PVID.

Jeżeli serwer RADIUS nie dostarczy żadnego VLAN lub jeżeli uwierzytelnianie 802.1x jest wyłączone, port po pomyślnym uwierzytelnieniu pozostanie w swojej sieci VLAN.

2) Kliknij **Apply**.

## 2.1.3 Konfiguracja 802.1x na portach

Wybierz z menu **SECURITY > 802.1x > Port Config**, aby wyświetlić poniższą stronę.

Rys. 2-7 Konfiguracja portów

| Port Config              |        |         |         |                     |              |             |                       |                      |                          |
|--------------------------|--------|---------|---------|---------------------|--------------|-------------|-----------------------|----------------------|--------------------------|
| UNIT1                    |        |         |         |                     |              |             |                       |                      |                          |
| <input type="checkbox"/> | Port   | Status  | MAB     | Guest VLAN (0-4094) | Port Control | Port Method | Maximum Request (1-9) | Quiet Period (0-999) | Supplicant Timeout (1-9) |
| <input type="checkbox"/> | 1/0/1  | Disable | Disable | 0                   | Auto         | MAC Based   | 3                     | 10                   | 3                        |
| <input type="checkbox"/> | 1/0/2  | Disable | Disable | 0                   | Auto         | MAC Based   | 3                     | 10                   | 3                        |
| <input type="checkbox"/> | 1/0/3  | Disable | Disable | 0                   | Auto         | MAC Based   | 3                     | 10                   | 3                        |
| <input type="checkbox"/> | 1/0/4  | Disable | Disable | 0                   | Auto         | MAC Based   | 3                     | 10                   | 3                        |
| <input type="checkbox"/> | 1/0/5  | Disable | Disable | 0                   | Auto         | MAC Based   | 3                     | 10                   | 3                        |
| <input type="checkbox"/> | 1/0/6  | Disable | Disable | 0                   | Auto         | MAC Based   | 3                     | 10                   | 3                        |
| <input type="checkbox"/> | 1/0/7  | Disable | Disable | 0                   | Auto         | MAC Based   | 3                     | 10                   | 3                        |
| <input type="checkbox"/> | 1/0/8  | Disable | Disable | 0                   | Auto         | MAC Based   | 3                     | 10                   | 3                        |
| <input type="checkbox"/> | 1/0/9  | Disable | Disable | 0                   | Auto         | MAC Based   | 3                     | 10                   | 3                        |
| <input type="checkbox"/> | 1/0/10 | Disable | Disable | 0                   | Auto         | MAC Based   | 3                     | 10                   | 3                        |
| Total: 10                |        |         |         |                     |              |             |                       |                      |                          |

Wykonaj poniższe kroki, aby skonfigurować uwierzytelnianie 802.1x na wybranym porcie:

1) Wybierz co najmniej jeden port i skonfiguruj następujące parametry:

|        |                                          |
|--------|------------------------------------------|
| Status | Włącz uwierzytelnianie 802.1x na porcie. |
|--------|------------------------------------------|

|                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|--------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| MAB                      | <p>Zaznacz, czy chcesz połączyć na porcie funkcję MAB (MAC-Based Authentication Bypass).</p> <p>Przy włączonej funkcji MAB przełącznik automatycznie wysyła do serwera uwierzytelniania ramkę żądania dostępu RADIUS z adresem MAC klienta ustawionym jako nazwa użytkownika i hasło. Konieczna jest konfiguracja serwera RADIUS z danymi do uwierzytelniania klienta. Możesz włączyć tę funkcję na portach IEEE 802.1x podłączonych do urządzenia bez obsługi 802.1x. Dla przykładu, większość drukarek, telefonów IP i faksów nie obsługuje 802.1x.</p> <p><i>Note:</i> MAB nie zadziała, jeżeli włączony jest Guest VLAN.</p> |
| Guest VLAN               | <p>Ustaw ID dla Guest VLAN. 0 oznacza, że Guest VLAN jest wyłączony. Skonfigurowany VLAN musi być istniejącym VLAN 802.1Q.</p> <p>Przy włączonej funkcji Guest VLAN port ma dostęp do zasobów w sieci VLAN dla gości, nawet jeżeli port nie został jeszcze uwierzytelniony. Jeżeli guest VLAN jest wyłączony, a port nie został uwierzytelniony, port nie ma dostępu do zasobów LAN.</p>                                                                                                                                                                                                                                         |
| Port Control             | <p>Wybierz tryb ochrony portu. Domyślnie ustawiony jest tryb Auto.</p> <p><b>Auto:</b> Jeżeli wybierzesz tę opcję, port będzie miał dostęp do sieci tylko po uwierzytelnieniu.</p> <p><b>Force-Authorized:</b> Jeżeli wybierzesz tę opcję, port nie będzie musiał być uwierzytelniony, żeby mieć dostęp do sieci.</p> <p><b>Force-Unauthenticated:</b> Jeżeli wybierzesz tę opcję, port nie będzie mógł zostać uwierzytelniony.</p>                                                                                                                                                                                              |
| Port Method              | <p>Wybierz strategię portu. Domyślnie ustawiona jest opcja MAC Based.</p> <p><b>MAC Based:</b> Wszyscy klienci podłączeni do portu muszą być uwierzytelnieni.</p> <p><b>Port Based:</b> Jeżeli jeden klient podłączony do portu jest uwierzytelniony, inni klienci mogą łączyć się z LAN bez uwierzytelniania.</p>                                                                                                                                                                                                                                                                                                               |
| Maximum Request (1-9)    | <p>Wyznacz maks. liczbę prób wysłania pakietu uwierzytelniania. Wartość powinna wynosić od 1 do 9. Wartość domyślna to 3 razy.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Quiet Period (1-999)     | <p>Wyznacz czas trwania Quiet Period. Wartość powinna wynosić od 1 do 999 sekund. Czas domyślny to 10 sekund.</p> <p>Quiet Period rozpoczyna się po błędzie uwierzytelniania. Jest to czas, w którym przełącznik nie przetwarza żądań uwierzytelniania od tego samego klienta.</p>                                                                                                                                                                                                                                                                                                                                               |
| Supplicant Timeout (1-9) | <p>Wyznacz maks. czas, przez który przełącznik czeka na odpowiedź klienta. Wartość powinna wynosić od 1 do 9 sekund. Wartość domyślna to 3 sekundy.</p> <p>Jeżeli w wyznaczonym czasie przełącznik nie otrzyma od klienta żadnej odpowiedzi, ponownie wyśle żądanie.</p>                                                                                                                                                                                                                                                                                                                                                         |
| Authorized               | <p>Informacja o tym, czy port jest uwierzytelniony, czy nie.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| LAG                      | <p>Informacja do której grupy LAG należy port.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |

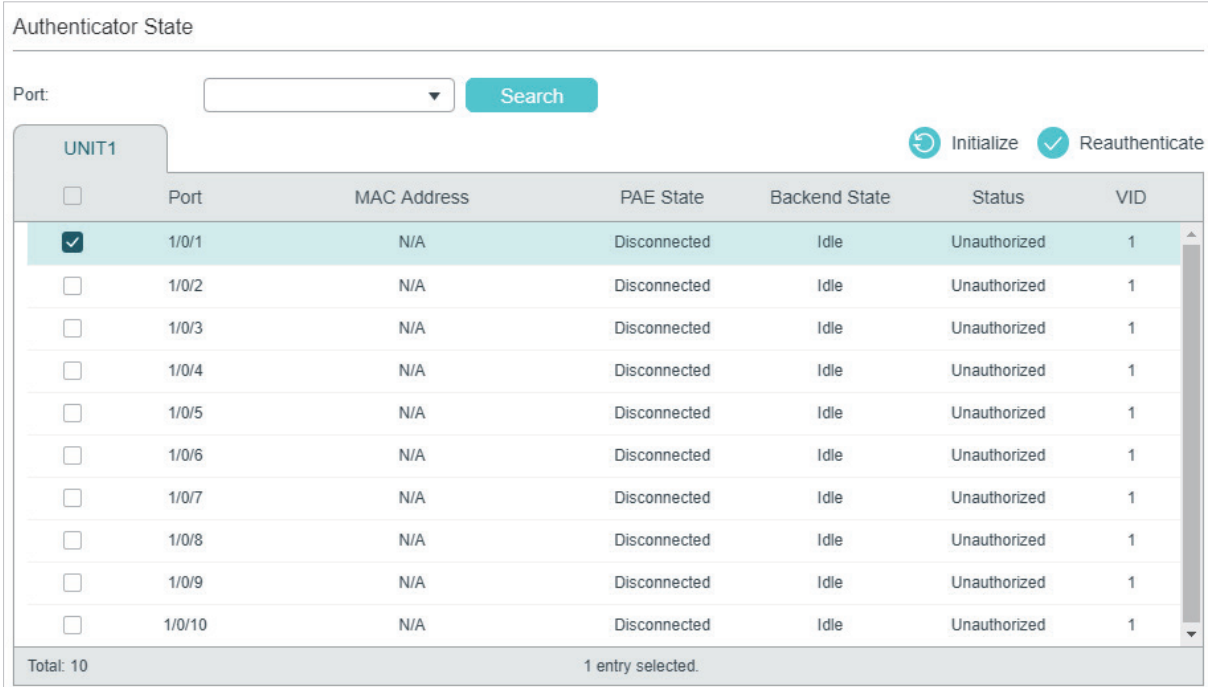
2) Kliknij **Apply**. Uwaga:

Jeżeli port należy do grupy LAG, nie można włączyć jego funkcji uwierzytelniania 802.1x. Analogicznie, port z włączonym uwierzytelnianiem 802.1x nie może być dodany do grupy LAG.

## 2.1.4 Sprawdzanie stanu wystawcy uwierzytelnienia



Wybierz z menu **SECURITY > 802.1x > Authenticator State**, aby wyświetlić poniższą stronę.

Rys. 2-8 Sprawdzanie stanu wystawcy uwierzytelnienia



Authenticator State

Port:

UNIT1  Initialize  Reauthenticate

| <input type="checkbox"/>            | Port   | MAC Address | PAE State    | Backend State | Status       | VID |
|-------------------------------------|--------|-------------|--------------|---------------|--------------|-----|
| <input checked="" type="checkbox"/> | 1/0/1  | N/A         | Disconnected | Idle          | Unauthorized | 1   |
| <input type="checkbox"/>            | 1/0/2  | N/A         | Disconnected | Idle          | Unauthorized | 1   |
| <input type="checkbox"/>            | 1/0/3  | N/A         | Disconnected | Idle          | Unauthorized | 1   |
| <input type="checkbox"/>            | 1/0/4  | N/A         | Disconnected | Idle          | Unauthorized | 1   |
| <input type="checkbox"/>            | 1/0/5  | N/A         | Disconnected | Idle          | Unauthorized | 1   |
| <input type="checkbox"/>            | 1/0/6  | N/A         | Disconnected | Idle          | Unauthorized | 1   |
| <input type="checkbox"/>            | 1/0/7  | N/A         | Disconnected | Idle          | Unauthorized | 1   |
| <input type="checkbox"/>            | 1/0/8  | N/A         | Disconnected | Idle          | Unauthorized | 1   |
| <input type="checkbox"/>            | 1/0/9  | N/A         | Disconnected | Idle          | Unauthorized | 1   |
| <input type="checkbox"/>            | 1/0/10 | N/A         | Disconnected | Idle          | Unauthorized | 1   |

Total: 10 1 entry selected.

Na tej stronie możesz sprawdzić stan uwierzytelnienia każdego portu:

|                      |                                                                                                                                                                                                                                                                                                                     |
|----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Port</b>          | Informacja o numerze portu.                                                                                                                                                                                                                                                                                         |
| <b>MAC Address</b>   | Informacja o adresie MAC uwierzytelnionego urządzenia. Jeżeli wybraną strategią portu jest Port Based (w oparciu o port), adres MAC pierwszego uwierzytelnionego urządzenia będzie wyświetlał się z sufiksem „p”.                                                                                                   |
| <b>PAE State</b>     | Informacja o aktualnym stanie maszyny stanów uwierzytelniania PAE. Dostępne wartości to: Initialize (Inicjuj), Disconnected (Rozłączony), Connecting (Łączenie), Authenticating (Uwierzytelnianie), Authenticated (Uwierzytelniony), Aborting (Przerywanie), Held (Utrzymany), ForceAuthorized i ForceUnauthorized. |
| <b>Backend State</b> | Informacja o bieżącym stanie maszyny stanów backendu uwierzytelniania. Dostępne wartości to: Request (żądanie), Response (odpowiedź), Success (powodzenie), Fail (niepowodzenie), Timeout (koniec czasu), Initialize (inicjowanie) i Idle (bezczynność).                                                            |
| <b>Status</b>        | Informacja o tym, czy port jest uwierzytelniony, czy nie.                                                                                                                                                                                                                                                           |



---

|         |                                                                                                                                                                                                                                                             |
|---------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| VLAN ID | Informacja o VLAN ID przypisanym przez wystawcę uwierzytelnienia do urządzenia suplikującego, jeżeli powiązany port jest uwierzytelniony. Jeżeli powiązany port nie jest uwierzytelniony i dostępny jest Guest VLAN ID, wyświetlony zostanie Guest VLAN ID. |
|---------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

---

## 2.2 Przez CLI

### 2.2.1 Konfiguracja serwera RADIUS

Wykonaj poniższe kroki, aby skonfigurować serwer RADIUS:

---

|        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Krok 1 | <p><b>configure</b></p> <p>Uruchom tryb konfiguracji globalnej.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Krok 2 | <p><b>radius-server host <i>ip-address</i> [ <i>auth-port port-id</i> ] [ <i>acct-port port-id</i> ] [ <i>timeout time</i> ] [ <i>retransmit number</i> ] [ <i>nas-id nas-id</i> ] key { [ 0 ] <i>string</i>   7 <i>encrypted-string</i> }</b></p> <p>Dodaj serwer RADIUS i odpowiednio skonfiguruj powiązane parametry.</p> <p><b>host <i>ip-address</i>:</b> Wpisz adres IP serwera obsługującego protokół RADIUS.</p> <p><b>auth-port <i>port-id</i>:</b> Wyznacz port docelowy UDP na serwerze RADIUS do żądań uwierzytelniania. Port domyślny to 1812.</p> <p><b>acct-port <i>port-id</i>:</b> Wyznacz port docelowy UDP na serwerze RADIUS do żądań rozliczania. Port domyślny to 1813. Z reguły funkcja rozliczania nie jest wykorzystywana w zarządzaniu kontem uwierzytelniania.</p> <p><b>timeout <i>time</i>:</b> Wyznacz, ile czasu przełącznik będzie czekał na odpowiedź serwera przed ponownym wysłaniem żądania. Wartość powinna wynosić od 1 do 9 sekund. Ustawienie domyślne to 5 s.</p> <p><b>retransmit <i>number</i>:</b> Wyznacz, ile razy ponawiane będzie wysyłanie żądania na serwer w przypadku braku odpowiedzi serwera. Wartość powinna wynosić od 1 do 3. Ustawienie domyślne to 2.</p> <p><b>nas-id <i>nas-id</i>:</b> Określ nazwę NAS (Network Access Server), która będzie zawarta w pakietach RADIUS w celu identyfikacji. Nazwa powinna zawierać od 1 do 31 znaków. Domyślnie jako nazwa ustawiony jest adres MAC przełącznika. Z reguły NAS sam wskazuje na przełącznik.</p> <p><b>key { [ 0 ] <i>string</i>   7 <i>encrypted-string</i> }:</b> Wprowadź klucz wspólny. 0 i 7 wykuczają wybieranie trybu szyfrowania. 0 oznacza, że wybrany zostanie klucz nieszyfrowany. 7 oznacza, że zastosowany zostanie klucz szyfrowany symetrycznie o stałej długości. Domyślny typ szyfrowania to 0. <i>string</i> jest to klucz wspólny dla przełącznika i serwera, składający się z maks. 32 znaków. <i>encrypted-string</i> to klucz szyfrowany symetrycznie o stałej długości, który można skopiować z pliku konfiguracyjnego innego przełącznika. Klucz lub klucz zaszyfrowany skonfigurowany w tym miejscu zostanie wyświetlony w formie zaszyfrowanej.</p> |
| Krok 3 | <p><b>aaa group radius <i>group-name</i></b></p> <p>Utwórz grupę serwera RADIUS.</p> <p><b>radius:</b> Ustaw typ grypy na radius.</p> <p><b><i>group-name</i>:</b> Ustaw nazwę grupy.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |

---

---

|         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|---------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Krok 4  | <b>server ip-address</b><br>Dodaj istniejące serwery do grupy serwera.<br><i>ip-address</i> : Ustaw adres IP serwera, który będzie dodany do grupy.                                                                                                                                                                                                                                                                                                                                                                   |
| Krok 5  | <b>exit</b><br>Wróć do trybu konfiguracji globalnej.                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Krok 6  | <b>aaa authentication dot1x default { method }</b><br>Wybierz grupę RADIUS do uwierzytelniania 802.1x.<br><i>method</i> : Wyznacz grupę RADIUS do uwierzytelniania 802.1x.<br><b>aaa accounting dot1x default { method }</b><br>Wybierz grupę RADIUS do kontroli dostępu 802.1x.<br><i>method</i> : Wybierz grupę RADIUS do kontroli dostępu 802.1x.<br><br><i>Note</i> : Jeżeli dostępne są liczne serwery RADIUS, zaleca się dodanie ich do innych grup serwera, oddzielnie do uwierzytelniania i kontroli dostępu. |
| Krok 7  | <b>show radius-server</b><br>(Opcjonalnie) Sprawdź ustawienia serwera RADIUS.                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Krok 8  | <b>show aaa group [ group-name ]</b><br>(Opcjonalnie) Sprawdź ustawienia grupy serwera.                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Krok 9  | <b>show aaa authentication dot1x</b><br>(Opcjonalnie) Sprawdź listę strategii uwierzytelniania.                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Krok 10 | <b>show aaa accounting dot1x</b><br>(Opcjonalnie) Sprawdź listę strategii kontroli dostępu.                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Krok 11 | <b>end</b><br>Powróć do trybu privileged EXEC                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Krok 12 | <b>copy running-config startup-config</b><br>Zapisz ustawienia w pliku konfiguracyjnym.                                                                                                                                                                                                                                                                                                                                                                                                                               |

---

Następny przykład prezentuje włączanie AAA, dodawanie serwera RADIUS do grupy serwera nazwanej radius1 i zastosowanie tej grupy serwera do uwierzytelniania 802.1x. Adres IP serwera RADIUS to 192.168.0.100; klucz wspólny to 123456; port uwierzytelniania to 1812; port rozliczania to 1813.

```
Switch#configure
```

```
Switch(config)#radius-server host 192.168.0.100 auth-port 1812 acct-port 1813 key
123456
```

```
Switch(config)#aaa group radius radius1
```

```
Switch(aaa-group)#server 192.168.0.100
```

```
Switch(aaa-group)#exit
```

```
Switch(config)#aaa authentication dot1x default radius1
```

```
Switch(config)#aaa accounting dot1x default radius1
```

```
Switch(config)#show radius-server
```

| Server Ip     | Auth Port | Acct Port | Timeout | Retransmit | NAS Identifier | Shared key |
|---------------|-----------|-----------|---------|------------|----------------|------------|
| 192.168.0.100 | 1812      | 1813      | 5       | 2          | 000AEB132397   | 123456     |

```
Switch(config)#show aaa group radius1
```

```
192.168.0.100
```

```
Switch(config)#show aaa authentication dot1x
```

| Methodlist | pri1    | pri2 | pri3 | pri4 |
|------------|---------|------|------|------|
| default    | radius1 | --   | --   | --   |

```
Switch(config)#show aaa accounting dot1x
```

| Methodlist | pri1    | pri2 | pri3 | pri4 |
|------------|---------|------|------|------|
| default    | radius1 | --   | --   | --   |

```
Switch(config)#end
```

```
Switch#copy running-config startup-config
```

## 2.2.2 Konfiguracja globalna 802.1x

Wykonaj poniższe kroki, aby skonfigurować globalnie 802.1x:

|        |                                                                              |
|--------|------------------------------------------------------------------------------|
| Krok 1 | <b>configure</b><br>Uruchom tryb konfiguracji globalnej.                     |
| Krok 2 | <b>dot1x system-auth-control</b><br>Włącz uwierzytelnianie 802.1x globalnie. |

---

|        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Krok 3 | <b>dot1x auth-protocol { pap   eap }</b><br>Konfiguracja protokołu uwierzytelniania 802.1x.<br><br><b>pap:</b> Wyznacz PAP jako protokół uwierzytelniania. W przypadku wybrania tej opcji system uwierzytelniania 802.1x wykorzystuje pakiety EAP (Extensible Authentication Protocol) do wymiany informacji między przełącznikiem, a klientem. Przekazywanie pakietów EAP jest zakończone na przełączniku, a pakiety EAP konwertowane są do innych pakietów protokołu (takich jak RADIUS) i przekazywane do serwera uwierzytelniania<br><br><b>eap:</b> Wyznacz EAP jako protokół uwierzytelniania. W przypadku wybrania tej opcji system uwierzytelniania 802.1x wykorzystuje pakiety EAP do wymiany informacji między przełącznikiem, a klientem. Pakiety EAP z danymi uwierzytelniania są kondensowane w pakietach zaawansowanego protokołu (takich jak RADIUS) i przekazywane do serwera uwierzytelniania. |
| Krok 4 | <b>dot1x accounting</b><br>(Opcjonalnie) Włącz funkcję kontroli dostępu.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Krok 5 | <b>dot1x handshake</b><br>(Opcjonalnie) Włącz funkcję Handshake. Funkcja służy do wykrywania stanu połączenia między TP-Link 802.1x Client i przełącznikiem. Wyłącz funkcję Handshake, jeżeli korzystasz z innych oprogramowań niż TP-Link 802.1x Client.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Krok 6 | <b>dot1x vlan-assignment</b><br>(Opcjonalnie) Włącz lub wyłącz funkcję przydziału VLAN 802.1x. Przydział VLAN 802.1x to technologia umożliwiająca serwerowi RADIUS wysłanie przydziału VLAN do portu po jego uwierzytelnieniu.<br><br>Jeżeli przypisanego VLAN nie ma na przełączniku, przełącznik automatycznie utworzy powiązany VLAN, doda do niego port uwierzytelniania i zmieni PVID oparty na przydzielonym VLAN.<br><br>Jeżeli przydzielony VLAN istnieje na przełączniku, zamiast tworzyć nowy VLAN, przełącznik bezpośrednio doda port uwierzytelniania do powiązanego VLAN i zmieni PVID.<br><br>Jeżeli serwer RADIUS nie dostarczy żadnego VLAN lub jeżeli uwierzytelnianie 802.1x jest wyłączone, port po pomyślnym uwierzytelnieniu pozostanie w swojej sieci VLAN.                                                                                                                               |
| Krok 7 | <b>show dot1x global</b><br>(Opcjonalnie) Sprawdź ustawienia globalne 802.1x.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Krok 8 | <b>end</b><br>Powróć do trybu privileged EXEC.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Krok 9 | <b>copy running-config startup-config</b><br>Zapisz ustawienia w pliku konfiguracyjnym.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |

---

Poniższy przykład prezentuje włączanie uwierzytelniania 802.1x, ustawianie PAP na metodę uwierzytelniania i zachowanie ustawień domyślnych dla pozostałych parametrów:

```
Switch#configure
```

```
Switch(config)#dot1x system-auth-control
```

```
Switch(config)#dot1x auth-protocol pap
```

```
Switch(config)#show dot1x global
```

```
802.1X State: Enabled
Authentication Protocol: PAP
Handshake State: Enabled
802.1X Accounting State: Disabled
802.1X VLAN Assignment State: Disabled
```

```
Switch(config)#end
```

```
Switch#copy running-config startup-config
```

## 2.2.3 Konfiguracja 802.1x na portach

Wykonaj poniższe kroki, aby skonfigurować port:

|        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Krok 1 | <p><b>configure</b></p> <p>Uruchom tryb konfiguracji globalnej.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Krok 2 | <p><b>interface {fastEthernet <i>port</i>   range fastEthernet <i>port-list</i>   gigabitEthernet <i>port</i>   range gigabitEthernet <i>port-list</i>   ten-gigabitEthernet <i>port</i>   range ten-gigabitEthernet <i>port-list</i> }</b></p> <p>Uruchom tryb konfiguracji interfejsu.</p> <p><i>port</i>: Wprowadź ID portu do konfiguracji.</p>                                                                                                                                                                                                                                                                               |
| Krok 3 | <p><b>dot1x</b></p> <p>Włącz uwierzytelnianie 802.1x dla portu.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Krok 4 | <p><b>dot1x mab</b></p> <p>Włącz na porcie funkcję MAB (MAC-Based Authentication Bypass).</p> <p>Przy włączonej funkcji MAB przełącznik automatycznie wysyła do serwera uwierzytelniania ramkę żądania dostępu RADIUS z adresem MAC klienta ustawionym jako nazwa użytkownika i hasło. Konieczna jest konfiguracja serwera RADIUS z danymi do uwierzytelniania klienta. Możesz włączyć tę funkcję na portach IEEE 802.1x podłączonych do urządzenia bez obsługi 802.1x. Dla przykładu, większość drukarek, telefonów IP i faksów nie obsługuje 802.1x.</p> <p><i>Note</i>: MAB nie zadziała, jeżeli włączony jest Guest VLAN.</p> |

---

|         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|---------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Krok 5  | <b>dot1x guest-vlan vid</b><br>(Opcjonalnie) Skonfiguruj na porcie VLAN dla gości (Guest VLAN).<br><br><i>vid</i> : Określ ID sieci VLAN, która będzie skonfigurowana jako VLAN dla gości. Wartość powinna mieścić się pomiędzy 0 a 4094. 0 oznacza, że Guest VLAN jest wyłączony na porcie. Skonfigurowany VLAN musi być istniejącym VLAN 802.1Q. Klienci w sieci VLAN dla gości mają dostęp tylko do zasobów z wybranych sieci VLAN.<br><br><i>Note</i> : Aby korzystać z Guest VLAN, typ kontroli portu powinien być ustawiony jako port-based. |
| Krok 6  | <b>dot1x port-control { auto   authorized-force   unauthorized-force }</b><br>Skonfiguruj tryb kontroli dla portu. Domyślnie ustawiony jest tryb auto.<br><br><i>auto</i> : Jeżeli wybierzesz tę opcję, port będzie miał dostęp do sieci tylko po uwierzytelnieniu.<br><br><i>authorized-force</i> : Jeżeli wybierzesz tę opcję, port nie będzie musiał być uwierzytelniony, żeby mieć dostęp do sieci.<br><br><i>unauthorized-force</i> : Jeżeli wybierzesz tę opcję, port nie będzie mógł zostać uwierzytelniony.                                |
| Krok 7  | <b>dot1x port-method { mac-based   port-based }</b><br>Skonfiguruj typ kontroli portu. Domyślnie ustawiona jest opcja MAC Based.<br><br><i>mac-based</i> : Wszyscy klienci podłączeni do portu muszą być uwierzytelnieni.<br><br><i>port-based</i> : Jeżeli jeden klient podłączony do portu jest uwierzytelniony, inni klienci mogą łączyć się z LAN bez uwierzytelniania.                                                                                                                                                                        |
| Krok 8  | <b>dot1x max-req times</b><br>Wyznacz maks. liczbę prób wysłania przez klienta pakietu uwierzytelniania.<br><br><i>times</i> : Maks. liczba prób wysłania pakietu uwierzytelniania przez klienta. Wartość powinna wynosić od 1 do 9. Wartość domyślna to 3 razy.                                                                                                                                                                                                                                                                                   |
| Krok 9  | <b>dot1x quiet-period [time]</b><br>(Opcjonalnie) Wyznacz czas trwania Quiet Period dla uwierzytelniania 802.1x i skonfiguruj Quiet Period.<br><br><i>time</i> : Ustaw wartość Quiet Period między 1 a 999 sekund. Wartość domyślna to 10 sekund. Quiet Period rozpoczyna się po błędzie uwierzytelniania. Jest to czas, w którym przełącznik nie przetwarza żądań uwierzytelniania od tego samego klienta.                                                                                                                                        |
| Krok 10 | <b>dot1x timeout supp-timeout time</b><br>Skonfiguruj Supplicant Timeout (przekroczenie czasu dla suplikanta).<br><br><i>time</i> : Wyznacz maks. czas, przez który przełącznik czeka na odpowiedź klienta. Wartość powinna wynosić od 1 do 9 sekund. Wartość domyślna to 3 sekundy. Jeżeli w wyznaczonym czasie przełącznik nie otrzyma od klienta żadnej odpowiedzi, ponownie wyśle żądanie.                                                                                                                                                     |

---

- 
- Krok 11      **show dot1x interface [fastEthernet *port* | gigabitEthernet *port* | ten-gigabitEthernet *port*]**  
(Opcjonalnie) Sprawdź ustawienia uwierzytelniania 802.1x authentication na porcie.  
*port*: Wprowadź ID portu do konfiguracji. Jeżeli nie wyznaczony zostanie konkretny port, przełącznik wyświetli ustawienia wszystkich portów.
- 
- Krok 12      **end**  
Powróć do trybu privileged EXEC.
- 
- Krok 13      **copy running-config startup-config**  
Zapisz ustawienia w pliku konfiguracyjnym.
- 

Poniższy przykład prezentuje włączanie uwierzytelniania 802.1x na porcie 1/0/2, konfigurację typu kontroli na port-based i zachowanie ustawień domyślnych dla pozostałych parametrów:

**Switch#configure**

**Switch(config)#interface gigabitEthernet 1/0/2**

**Switch(config-if)#dot1x**

**Switch(config-if)#dot1x port-method port-based**

**Switch(config-if)#show dot1x interface gigabitEthernet 1/0/2**

| Port    | State    | MAB State | GuestVLAN | PortControl | PortMethod |
|---------|----------|-----------|-----------|-------------|------------|
| ----    | ----     | -----     | -----     | -----       | -----      |
| Gi1/0/2 | disabled | disabled  | 0         | auto        | port-based |

| MaxReq | QuietPeriod | SuppTimeout | Authorized   | LAG |
|--------|-------------|-------------|--------------|-----|
| -----  | -----       | -----       | -----        | --- |
| 3      | 10          | 3           | unauthorized | N/A |

**Switch(config-if)#end**

**Switch#copy running-config startup-config**

## 2.2.4 Sprawdzanie stanu wystawcy uwierzytelnienia

Możesz sprawdzić stan wystawcy uwierzytelnienia. W razie konieczności możesz też zainicjować lub powtórzyć uwierzytelnianie wybranego klienta:

- 
- Krok 1      **show dot1x auth-state [interface fastEthernet *port* | interface gigabitEthernet *port*]**  
Informacja o stanie wystawcy uwierzytelnienia.
-

---

|        |                                                                                                                                                                                                                                                                                                                                       |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Krok 2 | <b>configure</b><br>Uruchom tryb konfiguracji globalnej.                                                                                                                                                                                                                                                                              |
| Krok 3 | <b>interface {fastEthernet <i>port</i>   range fastEthernet <i>port-list</i>   gigabitEthernet <i>port</i>   range gigabitEthernet <i>port-list</i>   ten-gigabitEthernet <i>port</i>   range ten-gigabitEthernet <i>port-list</i>}</b><br>Uruchom tryb konfiguracji interfejsu.<br><br><i>port</i> : Wpisz ID portu do konfiguracji. |
| Krok 4 | <b>dot1x auth-init [ mac <i>mac-address</i> ]</b><br>Zainicjuj wybranego klienta. Aby mieć dostęp do sieci, klient musi dostarczyć poprawne dane, by powtórnie przejść przez proces uwierzytelniania.<br><br><i>mac-address</i> : Wpisz adres MAC klienta, który będzie nieuwierzytelniony.                                           |
| Krok 5 | <b>dot1x auth-reauth [ mac <i>mac-address</i> ]</b><br>Uwierzytelnij na nowo wybranego klienta.<br><br><i>mac-address</i> : Wpisz adres MAC klienta, który będzie powtórnie uwierzytelniony.                                                                                                                                          |
| Krok 6 | <b>end</b><br>Powróć do trybu privileged EXEC.                                                                                                                                                                                                                                                                                        |
| Krok 7 | <b>copy running-config startup-config</b><br>Zapisz ustawienia w pliku konfiguracyjnym.                                                                                                                                                                                                                                               |

---



# 3 Przykład konfiguracji

## 3.1 Wymagania sieciowe

Administrator sieci firmowej chce kontrolować dostęp użytkowników końcowych (klientów). Wymaga się, aby wszyscy klienci byli poddawani indywidualnemu procesowi uwierzytelniania i aby tylko uwierzytelnieni klienci mogli uzyskać dostęp do Internetu.

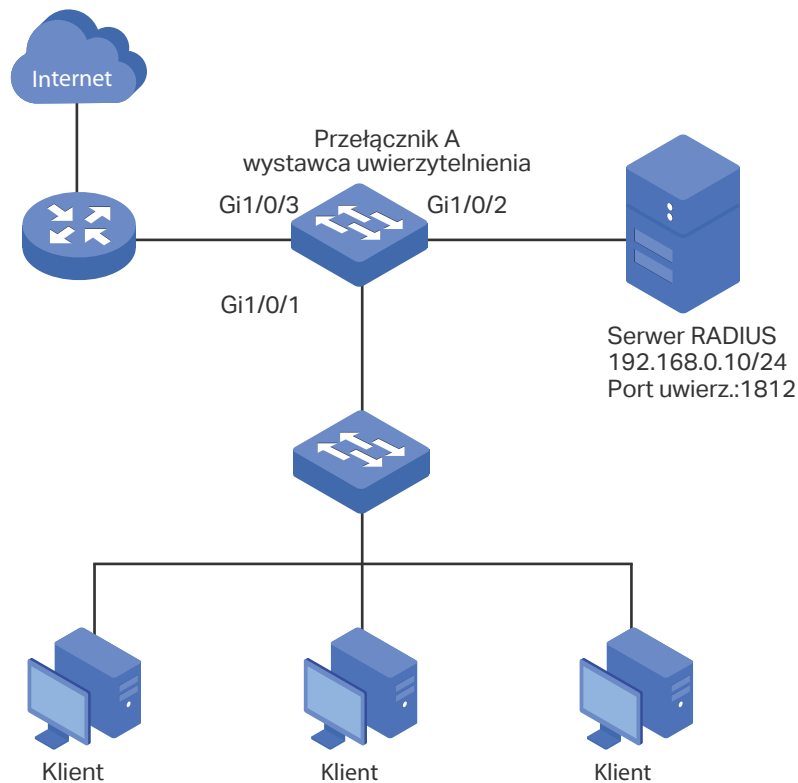
## 3.2 Schemat konfiguracji

- Aby uwierzytelniać klientów oddzielnie, włącz uwierzytelnianie 802.1x, skonfiguruj tryb kontroli jako auto i ustaw typ kontroli jako MAC based.
- Włącz uwierzytelnianie 802.1x na portach podłączonych do klientów.
- Pozostaw uwierzytelnianie 802.1x wyłączone na portach podłączonych do serwera uwierzytelniającego oraz do Internetu, gdyż stwarza to możliwość niegraniczonego nawiązywania połączeń pomiędzy przełącznikiem a serwerem uwierzytelniającym lub Internetem.

## 3.3 Topologia sieci

Jak pokazano na poniższym schemacie, przełącznik A pełni rolę wystawcy uwierzytelnienia. Port 1/0/1 jest podłączony do klienta, port 1/0/2 jest podłączony do serwera RADIUS, a port 1/0/3 jest podłączony do Internetu.

Rys. 3-1 Topologia sieci



W poniższych podrozdziałach opisano dwa sposoby przeprowadzenia procedury konfiguracji: przez GUI oraz przez CLI.

### 3.4 Przez GUI

- 1) Wybierz z menu **SECURITY > AAA > RADIUS Config** i kliknij **+ Add**, aby wyświetlić poniższą stronę. Skonfiguruj parametry serwera RADIUS i kliknij **Create**.

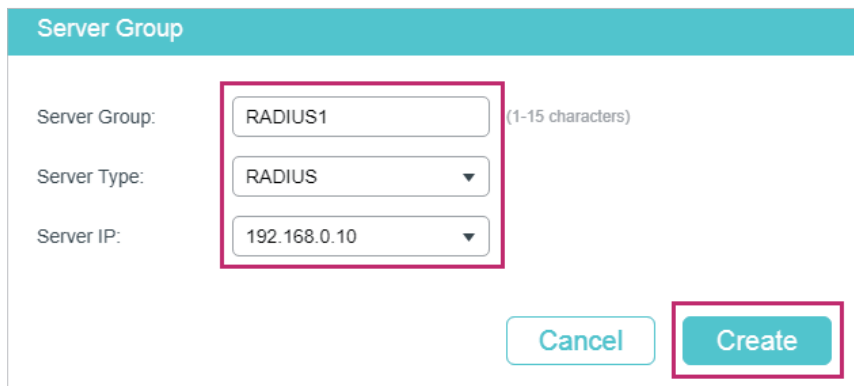
Rys. 3-2 Dodawanie serwera RADIUS

RADIUS Server

|                      |                                           |                                                                                                            |
|----------------------|-------------------------------------------|------------------------------------------------------------------------------------------------------------|
| Server IP:           | <input type="text" value="192.168.0.10"/> | <small>(Format:192.168.0.1)</small>                                                                        |
| Shared Key:          | <input type="text" value="123456"/>       | <small>1-32 characters. Only numbers, letters and the following symbols are allowed: - . / : @ _ .</small> |
| Authentication Port: | <input type="text" value="1812"/>         | <small>(1-65535)</small>                                                                                   |
| Accounting Port:     | <input type="text" value="1813"/>         | <small>(1-65535)</small>                                                                                   |
| Retransmit:          | <input type="text" value="2"/>            | <small>(1-3)</small>                                                                                       |
| Timeout:             | <input type="text" value="5"/>            | <small>seconds (1-9)</small>                                                                               |
| NAS Identifier:      | <input type="text"/>                      | <small>(Optional)</small>                                                                                  |

- 2) Wybierz z menu **SECURITY > AAA > Server Group** i kliknij  **Add**, aby wyświetlić poniższą stronę. Ustaw nazwę grupy jako RADIUS1, wybierz RADIUS jako typ serwera oraz ustaw adres IP serwera jako 192.168.0.10. Kliknij **Create**.

Rys. 3-3 Tworzenie grupy serwera



Server Group

Server Group: RADIUS1 (1-15 characters)

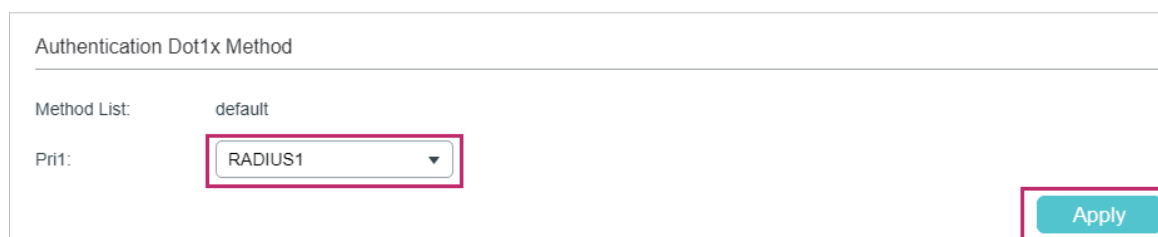
Server Type: RADIUS

Server IP: 192.168.0.10

Cancel Create

- 3) Wybierz z menu **SECURITY > AAA > Dot1x List**, aby wyświetlić poniższą stronę. W sekcji **Authentication Dot1x Method** wybierz RADIUS1 jako grupę serwera RADIUS do uwierzytelniania i kliknij **Apply**.

Rys. 3-4 Konfiguracja uwierzytelniania serwera RADIUS



Authentication Dot1x Method

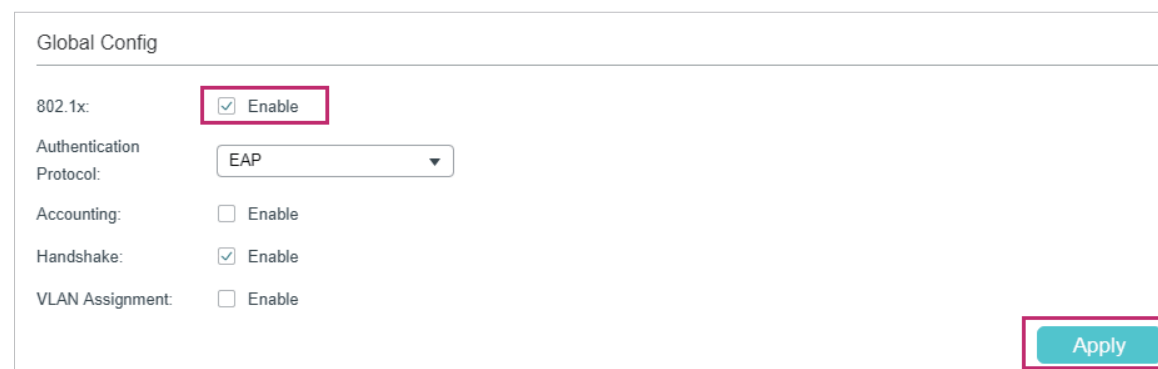
Method List: default

Pri: RADIUS1

Apply

- 4) Wybierz z menu **SECURITY > 802.1x > Global Config**, aby wyświetlić poniższą stronę. Włącz uwierzytelnianie 802.1x i skonfiguruj metodę uwierzytelniania jako EAP. Pozostaw domyślne ustawienia uwierzytelniania. Kliknij **Apply**.

Rys. 3-5 Konfiguracja ustawień globalnych



Global Config

802.1x:  Enable

Authentication Protocol: EAP

Accounting:  Enable

Handshake:  Enable

VLAN Assignment:  Enable

Apply

- 5) Wybierz z menu **SECURITY > 802.1x > Port Config**, aby wyświetlić poniższą stronę. Dla portu 1/0/1 włącz uwierzytelnianie 802.1x, ustaw tryb kontroli jako auto, a typ kontroli jako MAC Based; Dla portów 1/0/2 i 1/0/3 wyłącz uwierzytelnianie 802.1x.

Rys. 3-6 Konfiguracja portów


Port Config

UNIT1

| <input type="checkbox"/>            | ID | Port   | Status  | MAB     | Guest VLAN<br>(0-4094) | Port Control | Port Method | Maximum<br>Request<br>(1-9) | Quiet Period<br>(1-999) | Suppl<br>Time<br>(1- |
|-------------------------------------|----|--------|---------|---------|------------------------|--------------|-------------|-----------------------------|-------------------------|----------------------|
| <input checked="" type="checkbox"/> | 1  | 1/0/1  | Enable  | Disable | 0                      | Auto         | MAC Based   | 3                           | 10                      | 3                    |
| <input type="checkbox"/>            | 2  | 1/0/2  | Disable | Disable | 0                      | Auto         | MAC Based   | 3                           | 10                      | 3                    |
| <input type="checkbox"/>            | 3  | 1/0/3  | Disable | Disable | 0                      | Auto         | MAC Based   | 3                           | 10                      | 3                    |
| <input type="checkbox"/>            | 4  | 1/0/4  | Disable | Disable | 0                      | Auto         | MAC Based   | 3                           | 10                      | 3                    |
| <input type="checkbox"/>            | 5  | 1/0/5  | Disable | Disable | 0                      | Auto         | MAC Based   | 3                           | 10                      | 3                    |
| <input type="checkbox"/>            | 6  | 1/0/6  | Disable | Disable | 0                      | Auto         | MAC Based   | 3                           | 10                      | 3                    |
| <input type="checkbox"/>            | 7  | 1/0/7  | Disable | Disable | 0                      | Auto         | MAC Based   | 3                           | 10                      | 3                    |
| <input type="checkbox"/>            | 8  | 1/0/8  | Disable | Disable | 0                      | Auto         | MAC Based   | 3                           | 10                      | 3                    |
| <input type="checkbox"/>            | 9  | 1/0/9  | Disable | Disable | 0                      | Auto         | MAC Based   | 3                           | 10                      | 3                    |
| <input type="checkbox"/>            | 10 | 1/0/10 | Disable | Disable | 0                      | Auto         | MAC Based   | 3                           | 10                      | 3                    |

Total: 28 1 entry selected.

Cancel Apply

6) Kliknij  Save, aby zapisać ustawienia.

## 3.5 Przez CLI

1) Skonfiguruj parametry serwera RADIUS.

```
Switch_A(config)#radius-server host 192.168.0.10 auth-port 1812 key 123456
```

```
Switch_A(config)#aaa group radius RADIUS1
```

```
Switch_A(aaa-group)#server 192.168.0.10
```

```
Switch_A(aaa-group)#exit
```

```
Switch_A(config)#aaa authentication dot1x default RADIUS1
```

2) Włącz globalnie uwierzytelnianie 802.1x i ustaw protokół uwierzytelniania.

```
Switch_A(config)#dot1x system-auth-control
```

```
Switch_A(config)#dot1x auth-protocol eap
```

3) Wyłącz uwierzytelnianie 802.1x na portach 1/0/2 i 1/0/3. Włącz uwierzytelnianie 802.1x na porcie 1/0/1, ustaw tryb kontroli jako auto, a typ kontroli jako MAC based.

```
Switch_A(config)#interface gigabitEthernet 1/0/2
```

```
Switch_A(config-if)#no dot1x
```

```
Switch_A(config-if)#exit
```

```
Switch_A(config)#interface gigabitEthernet 1/0/3
```

```

Switch_A(config-if)#no dot1x
Switch_A(config-if)#exit
Switch_A(config)#interface gigabitEthernet 1/0/1
Switch_A(config-if)#dot1x
Switch_A(config-if)#dot1x port-method mac-based
Switch_A(config-if)#dot1x port-control auto
Switch_A(config-if)#exit

```

## Sprawdzanie konfiguracji

Sprawdzanie globalnej konfiguracji uwierzytelniania 802.1x:

```

Switch_A#show dot1x global
802.1X State: Enabled
Authentication Protocol: EAP
Handshake State: Enabled
802.1X Accounting State: Disabled
802.1X VLAN Assignment State: Disabled

```

Sprawdzanie konfiguracji uwierzytelniania 802.1x na porcie:

```

Switch_A#show dot1x interface

```

| Port    | State       | MAB State   | GuestVLAN    | PortControl | PortMethod |
|---------|-------------|-------------|--------------|-------------|------------|
| ----    | -----       | -----       | -----        | -----       | -----      |
| Gi1/0/1 | enabled     | disabled    | 0            | auto        | mac-based  |
| Gi1/0/2 | disabled    | disabled    | 0            | auto        | mac-based  |
| Gi1/0/3 | disabled    | disabled    | 0            | auto        | mac-based  |
| .....   |             |             |              |             |            |
| MaxReq  | QuietPeriod | SuppTimeout | Authorized   | LAG         |            |
| -----   | -----       | -----       | -----        | ---         |            |
| 3       | 10          | 3           | unauthorized | N/A         |            |
| 3       | 10          | 3           | unauthorized | N/A         |            |
| 3       | 10          | 3           | unauthorized | N/A         |            |
| .....   |             |             |              |             |            |

Sprawdzenie konfiguracji serwera RADIUS :

```
Switch_A#show aaa authentication dot1x
```

```
Methodlist pri1 pri2 pri3 pri4
default RADIUS1 -- -- --
```

```
Switch_A#show aaa group RADIUS1
```

```
192.168.0.10
```

```
Switch_A#show aaa accounting dot1x
```

```
Methodlist pri1 pri2 pri3 pri4
default radius -- -- --
```

# Część 22

## Konfiguracja Port Security

### ROZDZIAŁY

1. Informacje ogólne
2. Konfiguracja Port Security

# 1 Informacje ogólne

Funkcja Port Security służy do ograniczania liczby adresów MAC zapamiętywanych na każdym z portów, co pomaga zapobiec wyczerpaniu tablicy adresów MAC przez atakujące pakiety. Dodatkowo przełącznik może wysyłać powiadomienia, gdy liczba zapamiętanych na porcie adresów MAC osiągnie ustalony limit.



# 2 Konfiguracja Port Security

## 2.1 Przez GUI

Wybierz z menu **SECURITY > Port Security**, aby wyświetlić poniższą stronę.

Rys. 2-1 Port Security

| Port Security Config                |        |                           |                        |                         |                    |         |
|-------------------------------------|--------|---------------------------|------------------------|-------------------------|--------------------|---------|
| UNIT1                               | Port   | Max Learned Number of MAC | Current Learned Number | Exceed Max Learned Trap | Learn Address Mode | Status  |
| <input checked="" type="checkbox"/> | 1/0/1  | 64                        | 0                      | Disable                 | Delete on Timeout  | Disable |
| <input type="checkbox"/>            | 1/0/2  | 64                        | 0                      | Disable                 | Delete on Timeout  | Disable |
| <input type="checkbox"/>            | 1/0/3  | 64                        | 0                      | Disable                 | Delete on Timeout  | Disable |
| <input type="checkbox"/>            | 1/0/4  | 64                        | 0                      | Disable                 | Delete on Timeout  | Disable |
| <input type="checkbox"/>            | 1/0/5  | 64                        | 0                      | Disable                 | Delete on Timeout  | Disable |
| <input type="checkbox"/>            | 1/0/6  | 64                        | 0                      | Disable                 | Delete on Timeout  | Disable |
| <input type="checkbox"/>            | 1/0/7  | 64                        | 0                      | Disable                 | Delete on Timeout  | Disable |
| <input type="checkbox"/>            | 1/0/8  | 64                        | 0                      | Disable                 | Delete on Timeout  | Disable |
| <input type="checkbox"/>            | 1/0/9  | 64                        | 0                      | Disable                 | Delete on Timeout  | Disable |
| <input type="checkbox"/>            | 1/0/10 | 64                        | 0                      | Disable                 | Delete on Timeout  | Disable |

Total: 10      1 entry selected.      Cancel Apply

Wykonaj poniższe kroki, aby skonfigurować Port Security:

1) Wybierz jeden lub kilka portów i skonfiguruj poniższe parametry.

|                           |                                                                                                                                                                                                                         |
|---------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Port                      | Numer portu.                                                                                                                                                                                                            |
| Max Learned Number of MAC | Podaj maksymalną liczbę adresów MAC, które mogą być zapamiętane na porcie. Gdy liczba zapamiętanych adresów MAC osiągnie ustalony limit, port przerwie zapamiętywanie. Ta wartość musi mieścić się w przedziale 0 - 64. |
| Current Learned MAC       | Aktualna liczba adresów MAC, które zostały zapamiętane na porcie.                                                                                                                                                       |
| Exceed Max Learned Trap   | Gdy włączysz tę opcję, w przypadku przekroczonego limitu zapamiętanych adresów MAC na określonym porcie, do hosta zarządzającego zostanie wysłane powiadomienie.                                                        |

|                    |                                                                                                                                                                                                     |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Learn Address Mode | Wybierz tryb zapamiętywania adresów MAC na porcie. Dostępne są trzy tryby:                                                                                                                          |
|                    | <p><b>Delete on Timeout:</b> Przełącznik usunie adresy MAC, które nie są używane lub aktualizowane przed terminem utraty ważności. To ustawienie jest domyślnie włączone.</p>                       |
|                    | <p><b>Delete on Reboot:</b> Na zapamiętane adresy MAC nie ma wpływu termin utraty ważności i można je usuwać wyłącznie ręcznie. Zapamiętane pozycje zostaną usunięte po restarcie przełącznika.</p> |
|                    | <p><b>Permanent:</b> Na zapamiętane adresy MAC nie ma wpływu termin utraty ważności i można je usuwać wyłącznie ręcznie. Zapamiętane pozycje zostaną zachowane nawet po restarcie przełącznika.</p> |
| Status             | Wybierz stan Port Security spośród trzech typów:                                                                                                                                                    |
|                    | <p><b>Drop:</b> Gdy liczba zapamiętanych adresów MAC osiągnie limit, port przerwie zapamiętywanie i odrzuci pakiety z adresami MAC, które nie zostały zapamiętane.</p>                              |
|                    | <p><b>Forward:</b> Gdy liczba zapamiętanych adresów MAC osiągnie limit, port przerwie zapamiętywanie, ale prześle pakiety z adresami MAC, które nie zostały zapamiętane.</p>                        |
|                    | <p><b>Disable:</b> Limit nie jest aktywny na porcie, dlatego przełącznik stosuje się do pierwotnych reguł przekazywania. To ustawienie jest domyślnie włączone.</p>                                 |

## 2) Kliknij **Apply**.

### Uwaga:

- Funkcji Port Security nie można włączyć na portach należących do LAG, a port o włączonej funkcji Port Security nie może być dodany do LAG.
- Włączenie w tym samym czasie Port Security i 802.1x na jednym porcie nie jest możliwe.

## 2.2 Przez CLI

Wykonaj poniższe kroki, aby skonfigurować Port Security:

|        |                                                                                                                                                                                                                                                                                            |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Krok 1 | <p><b>configure</b><br/>Uruchom tryb konfiguracji globalnej.</p>                                                                                                                                                                                                                           |
| Krok 2 | <p><b>interface { fastEthernet <i>port</i>   range fastEthernet <i>port-list</i>   gigabitEthernet <i>port</i>   range gigabitEthernet <i>port-list</i>   ten-gigabitEthernet <i>port</i>   range ten-gigabitEthernet <i>port-list</i> }</b><br/>Uruchom tryb konfiguracji interfejsu.</p> |

- Krok 3      **mac address-table max-mac-count { [max-number *num*] [exceed-max-learned enable | disable] [mode { dynamic | static | permanent } ] [ status { forward | drop | disable } ] }**  
 Włącz funkcję Port Security na porcie i skonfiguruj odpowiednie parametry.  
*num*: Maksymalna liczba adresów MAC, które mogą być zapamiętane na porcie. Prawidłowa wartość musi mieścić się w przedziale 0 - 64. Wartością domyślną jest 64.
- exceed-max-learned**: Gdy włączysz tę opcję, w przypadku przekroczonego limitu zapamiętanych adresów MAC na określonym porcie, do hosta zarządzającego zostanie wysłane powiadomienie.  
**enable**: Włącz exceed-max-learned.  
**disable**: Wyłącz exceed-max-learned.
- mode**: Tryby zapamiętywania adresów MAC na porcie. Dostępne są trzy tryby:  
**dynamic**: Przełącznik usunie adresy MAC, które nie są używane lub aktualizowane przed terminem utraty ważności.  
**static**: Na zapamiętane adresy MAC nie ma wpływu termin utraty ważności i można je usuwać wyłącznie ręcznie. Zapamiętane pozycje zostaną usunięte po restarcie przełącznika.  
**permanent**: Na zapamiętane adresy MAC nie ma wpływu termin utraty ważności i można je usuwać wyłącznie ręcznie. Zapamiętane pozycje zostaną zachowane nawet po restarcie przełącznika.
- status**: Stan funkcji Port Security. Domyślnie funkcja jest wyłączona.  
**drop**: Gdy liczba zapamiętanych adresów MAC osiągnie limit, port przerwie zapamiętywanie i odrzuci pakiety z adresami MAC, które nie zostały zapamiętane.  
**forward**: Gdy liczba zapamiętanych adresów MAC osiągnie limit, port przerwie zapamiętywanie, ale prześle pakiety z adresami MAC, które nie zostały zapamiętane.  
**disable**: Limit nie jest aktywny na porcie, dlatego przełącznik stosuje się do pierwotnych reguł przekazywania. To ustawienie jest domyślnie włączone.
- 
- Krok 4      **show mac address-table max-mac-count interface { fastEthernet *port* | gigabitEthernet *port* | ten-gigabitEthernet *port* }**  
 Przejrzyj ustawienia Port Security i aktualnie zapamiętanych adresów MAC na porcie.
- 
- Krok 5      **end**  
 Powróć do trybu privileged EXEC.
- 
- Krok 6      **copy running-config startup-config**  
 Zapisz ustawienia w pliku konfiguracyjnym.

 **Uwaga:**

- Funkcji Port Security nie można włączyć na portach należących do LAG, a port o włączonej funkcji Port Security nie może być dodany do LAG.
- Włączenie w tym samym czasie Port Security i 802.1x na jednym porcie nie jest możliwe.

Poniższy schemat przedstawia przykładowy sposób ustawiania maksymalnej liczby adresów MAC, które mogą być zapamiętane na porcie 1/0/1 jako 30, włączania opcji exceed-max-learned, ustawiania trybu jako permanent i stanu jako drop:

**Switch#configure**

```
Switch(config)#interface gigabitEthernet 1/0/1
```

```
Switch(config-if)#mac address-table max-mac-count max-number 30 exceed-max-learned enable mode permanent status drop
```

```
Switch(config-if)#show mac address-table max-mac-count interface gigabitEthernet 1/0/1
```

| Port    | Max-learn | Current-learn | Exceed Max Limit | Mode      | Status |
|---------|-----------|---------------|------------------|-----------|--------|
| ----    | -----     | -----         | -----            | -----     | -----  |
| Gi1/0/1 | 30        | 0             | disable          | permanent | drop   |

```
Switch(config-if)#end
```

```
Switch#copy running-config startup-config
```

# Część 23

## Konfiguracja ACL

### ROZDZIAŁY

1. Informacje ogólne
2. Konfiguracja ACL
3. Przykład konfiguracji ACL

# 1 Informacje ogólne

Funkcja ACL (Access Control List) umożliwia filtrowanie ruchu na przełączniku i akceptowanie lub odrzucanie pakietów przechodzących przez określone interfejsy lub VLAN-y. Precyzyjnie identyfikuje i przetwarza pakiety bazując na regułach ACL. W ten sposób ACL pomaga w ograniczeniu ruchu sieciowego, zarządzaniu dostępem do sieci, przesyłaniu pakietów do określonych portów itp.

Aby skonfigurować ACL, wykonaj poniższe kroki:

- 1) Skonfiguruj zakres czasu obowiązywania ACL.
- 2) Utwórz listę ACL i skonfiguruj reguły filtrowania różnych pakietów.
- 3) Powiąż listę ACL z portem lub VLAN-em, aby umożliwić jej obowiązywanie.

## Wskazówki dotyczące konfiguracji

- Pakiet "pasuje" do reguły ACL, gdy spełnia kryteria dopasowania do danej reguły. Rezultatem będzie albo „zezwozenie”, albo „odmowa” dla pakietu pasującego do reguły.
- Jeśli żadna reguła ACL nie zostanie skonfigurowana, pakiety będą przesyłane bez etapu przetwarzania poprzez ACL. Jeśli reguły ACL zostaną skonfigurowane, ale pakiet nie będzie pasować do żadnej reguły, spowoduje to jego odrzucenie.

# 2 Konfiguracja ACL

## 2.1 Przez GUI

### 2.1.1 Konfiguracja zakresu czasu

Działanie niektórych usług i funkcji opartych na ACL (Access Control List) może musieć być ograniczone do wyznaczonego zakresu czasu. W takim przypadku należy skonfigurować zakres czasu działania ACL. Więcej szczegółów dotyczących konfiguracji zakresu czasu znajdziesz w rozdziale *Zarządzanie systemem*.

### 2.1.2 Tworzenie ACL

Możesz utworzyć różne typy ACL i zdefiniować reguły w oparciu o źródłowy adres MAC lub IP, docelowy adres MAC lub IP, typ protokołu, numer portu itd.

**MAC ACL:** MAC ACL wykorzystuje źródłowy i docelowy adres MAC do czynności dopasowywania.

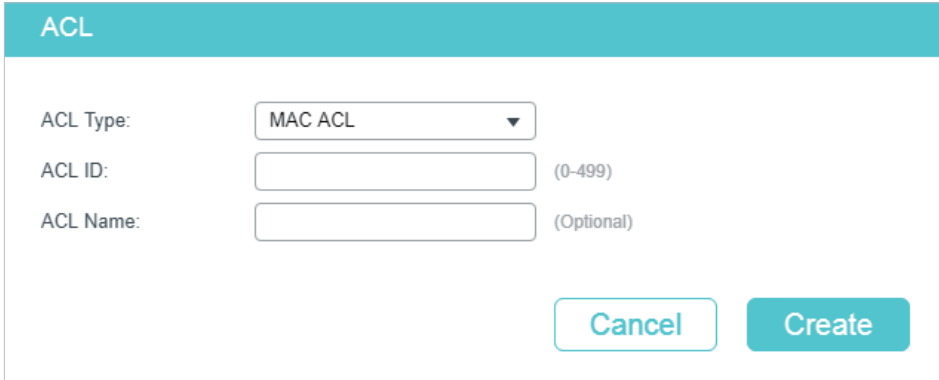
**IP ACL:** IP ACL wykorzystuje źródłowy i docelowy adres IP, protokoły IP itd. do czynności dopasowywania.

**Combined ACL:** Łączona ACL wykorzystuje do czynności dopasowywania źródłowe i docelowe adresy MAC i IP.

**IPv6 ACL:** IPv6 ACL wykorzystuje do czynności dopasowywania źródłowe i docelowe adresy IPv6.

Wybierz z menu **SECURITY > ACL > ACL Config** i kliknij  **Add**, aby wyświetlić poniższą stronę.

Rys. 2-1 Tworzenie ACL



ACL

ACL Type:

ACL ID:  (0-499)

ACL Name:  (Optional)

Wykonaj poniższe kroki, aby utworzyć ACL:

- 1) Wybierz typ ACL i wpisz numer do identyfikacji ACL.

2) (Opcjonalnie) Przypisz nazwę do ALC.

3) Kliknij **Create**.

#### Uwaga:

Obsługiwany typ ACL i zakres ID różni się dla różnych modeli przełącznika. Należy kierować się informacją wyświetlaną na ekranie.

## 2.1.3 Konfiguracja reguł ACL

Utworzone ACL wyświetlane będą na stronie **SECURITY > ACL > ACL Config**.

Rys. 2-2 Edytowanie ACL

| ACL Config               |          |        |          |       |                          |
|--------------------------|----------|--------|----------|-------|--------------------------|
| <input type="checkbox"/> | ACL Type | ACL ID | ACL Name | Rules | Operation                |
| <input type="checkbox"/> | IP ACL   | 500    | ACL1     | None  | <a href="#">Edit ACL</a> |
| Total: 1                 |          |        |          |       |                          |





Aby skonfigurować reguły danej listy, kliknij **Edit ACL** w kolumnie **Operation**.

Poniższe sekcje wprowadzają zagadnienie konfiguracji MAC ACL, IP ACL, Combined ACL i IPv6 ACL.

### Konfiguracja reguły MAC ACL

Kliknij **Edit ACL** przy wpisie MAC ACL, aby wyświetlić poniższą stronę.

Rys. 2-3 Konfiguracja reguły MAC ACL

| ACL Details                                                                                    |         |         |       |       |        |                       |                                                                                           |                                                                                              |                                                                                               |
|------------------------------------------------------------------------------------------------|---------|---------|-------|-------|--------|-----------------------|-------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------|
| ACL Type:                                                                                      | MAC ACL |         |       |       |        |                       |                                                                                           |                                                                                              |                                                                                               |
| ACL ID:                                                                                        | 1       |         |       |       |        |                       |                                                                                           |                                                                                              |                                                                                               |
| ACL Name:                                                                                      | ACL2    |         |       |       |        |                       |                                                                                           |                                                                                              |                                                                                               |
| ACL Rules Table                                                                                |         |         |       |       |        |                       |                                                                                           |                                                                                              |                                                                                               |
|  Resequence |         |         |       |       |        |                       |  Add |  Delete |  Refresh |
| <input type="checkbox"/>                                                                       | ID      | Rule ID | S-MAC | D-MAC | Action | Total Matched Counter | Operation                                                                                 |                                                                                              |                                                                                               |
| No entries in this table.                                                                      |         |         |       |       |        |                       |                                                                                           |                                                                                              |                                                                                               |
| Total: 0                                                                                       |         |         |       |       |        |                       |                                                                                           |                                                                                              |                                                                                               |

W sekcji **ACL Rules Table** kliknij  **Add**, aby pojawiło się następujące okno:



Rys. 2-4 Konfiguracja reguły MAC ACL

**MAC ACL Rule**

---

ACL ID: 1

ACL Name: ACL2

Rule ID:   Auto Assign

Operation: Permit ▼

S-MAC:  (Format FF-FF-FF-FF-FF-FF)

Mask:  (Format FF-FF-FF-FF-FF-FF)

D-MAC:  (Format FF-FF-FF-FF-FF-FF)

Mask:  (Format FF-FF-FF-FF-FF-FF)

VLAN ID:  (1-4094)

EtherType:  (4-hex number)

User Priority: Default ▼

Time Range:  ▼ (Optional)

Logging: Disable ▼

---

**Policy**

Mirroring

Redirect

Rate Limit

QoS Remark

Wykonaj poniższe kroki, aby skonfigurować regułę MAC ACL:

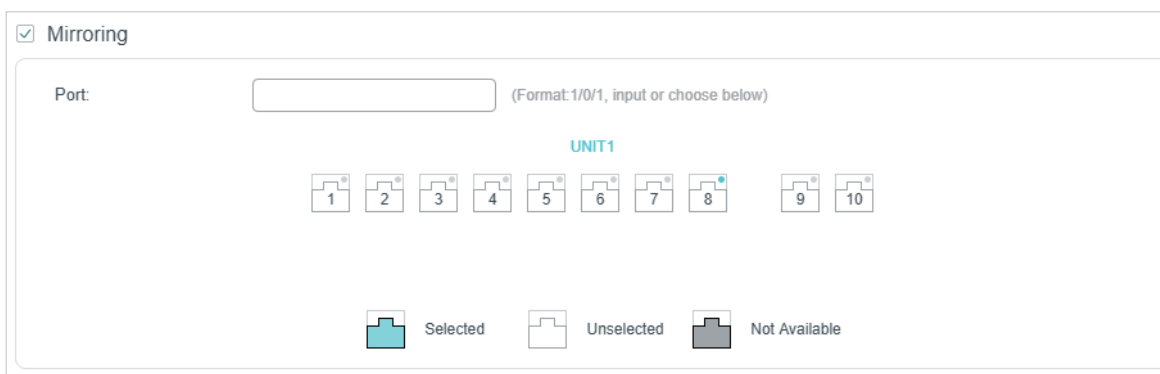
1) W sekcji **MAC ACL Rule** skonfiguruj następujące parametry:

|            |                                                                                                                                                                                                                                                                           |
|------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Rule ID    | <p>Wpisz numer ID, aby umożliwić identyfikację reguły.</p> <p>Numer nie powinien być taki sam, jak jakiegokolwiek numer ID aktualnej reguły na tej samej ACL. W przypadku wybrania opcji Auto Assign, ID reguły będzie przypisywany automatycznie w odstępie czasu 5.</p> |
| Operation  | <p>Wybierz działanie, które ma być wykonane, jeżeli pakiet jest dopasowany do reguły.</p> <p><b>Permit:</b> Jeżeli dopasowane pakiety mają być przekazywane.</p> <p><b>Deny:</b> Jeżeli dopasowane pakiety mają być odrzucone.</p>                                        |
| S-MAC/Mask | Wpisz źródłowy adres MAC z maską. Wartość 1 w masce wskazuje na to, że odpowiadający bit w adresie zostanie dopasowany.                                                                                                                                                   |
| D-MAC/Mask | Wpisz docelowy adres MAC z maską. Wartość 1 w masce wskazuje na to, że odpowiadający bit w adresie zostanie dopasowany.                                                                                                                                                   |
| VLAN ID    | Wpisz numer ID sieci VLAN, do której zastosowanie będzie miała ACL.                                                                                                                                                                                                       |

|               |                                                                                                                                                                                                                                                                                                |
|---------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| EtherType     | Określ EtherType, który będzie dopasowany, używając 4 liczb szesnastkowych.                                                                                                                                                                                                                    |
| User Priority | Określ User Priority, który zostanie dopasowany.                                                                                                                                                                                                                                               |
| Time Range    | Określ zakres czasu, w którym będzie działała reguła. Ustawienie domyślne to No Limit, co oznacza, że reguła jest zawsze aktywna. Zakres czasu ustawić można na stronie <b>SYSTEM &gt; Time Range</b> .                                                                                        |
| Logging       | Włącz funkcję rejestrowania dla reguły ACL. Wtedy co pięć minut dopasowane reguły będą rejestrowane i wygenerowane zostaną powiązane pułapki (ang. trap). Aby sprawdzić, ile razy doszło do dopasowania, idź do Total Matched Counter (licznik wszystkich dopasowań) w sekcji ACL Rules Table. |

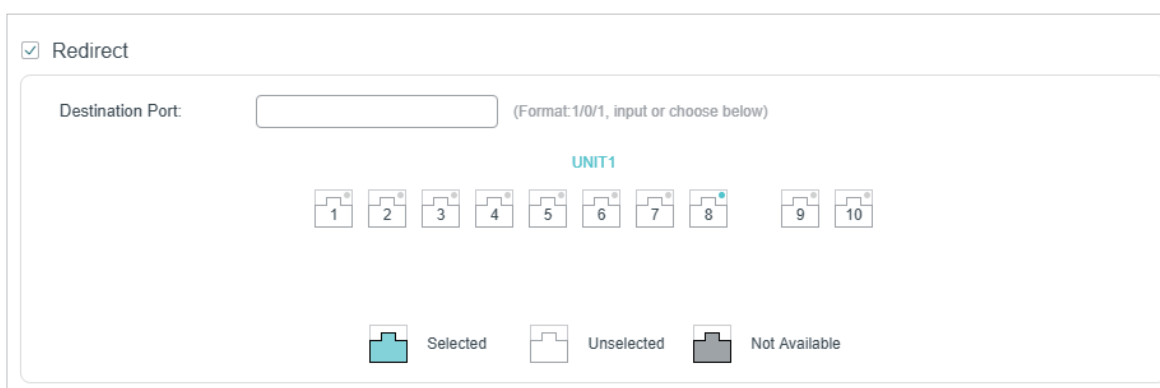
- 2) W sekcji **Policy** włącz lub wyłącz funkcję Mirroring dla dopasowanych pakietów. Jeżeli opcja jest włączona, należy wybrać port docelowy, na którym kopiowane będą pakiety.

Rys. 2-5 Konfiguracja Mirroring



- 3) W sekcji **Policy** włącz lub wyłącz funkcję Redirect dla dopasowanych pakietów. Jeżeli opcja jest włączona, należy wybrać port docelowy, do którego przekierowywane będą pakiety.

Rys. 2-6 Konfiguracja funkcji Redirect



### Uwaga:

Przy włączeniu funkcji Mirroring dopasowane pakiety zostaną skopiowane do portu docelowego, bez straty dla oryginalnego przekazywania. Przy włączeniu funkcji Redirect dopasowane pakiety będą przekazywane jedynie na porcie docelowym.

- 4) W sekcji **Policy** włącz lub wyłącz funkcję Rate Limit dla dopasowanych pakietów. Jeżeli funkcja została włączona, skonfiguruj powiązane parametry.

Rys. 2-7 Konfiguracja funkcji Rate Limit

Rate Limit

Rate:  Kbps (1-10000000)

Burst Size:  KB (1-128)

Out of Band:

|             |                                                                                                                                                                                                      |
|-------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Rate        | Wyznacz prędkość transmisji dopasowanych pakietów.                                                                                                                                                   |
| Burst Size  | Określ maks. dopuszczalną liczbę bitów na sekundę.                                                                                                                                                   |
| Out of Band | <p>Wybierz działanie dla pakietów, których prędkość znajduje się poza wyznaczonym zakresem.</p> <p><b>None:</b> Pakiety będą przekazywane normalnie.</p> <p><b>Drop:</b> Pakiety będą odrzucane.</p> |

- 5) W sekcji **Policy** włącz lub wyłącz funkcję QoS Remark dla dopasowanych pakietów. Jeżeli funkcja jest włączona, należy skonfigurować powiązane parametry, a wprowadzone wartości będą zastosowane w przetwarzaniu QoS na przełączniku.

Rys. 2-8 Konfiguracja QoS Remark

QoS Remark

DSCP:

Local Priority:

802.1p Priority:

|                 |                                                                                                                              |
|-----------------|------------------------------------------------------------------------------------------------------------------------------|
| DSCP            | Określ pole DSCP dla dopasowanych pakietów. Pole DSCP pakietów będzie zmienione na to wyznaczone pole.                       |
| Local Priority  | Określ priorytet lokalny dla dopasowanych pakietów. Priorytet lokalny pakietów będzie zmieniony na ten wyznaczony priorytet. |
| 802.1p Priority | Określ priorytet 802.1p dla dopasowanych pakietów. Priorytet 802.1p pakietów będzie zmieniony na ten wyznaczony priorytet.   |

- 6) Kliknij **Apply**.

## Konfiguracja reguły IP ACL

Kliknij **Edit ACL** dla wpisu IP ACL, aby wyświetlić poniższą stronę.

Rys. 2-9 Konfiguracja reguły IP ACL


ACL Details

---

ACL Type: IP ACL  
 ACL ID: 500  
 ACL Name: ACL1

ACL Rules Table

---

 Resequenece  Add  Delete  Refresh

| <input type="checkbox"/>  | ID | Rule ID | S-IP | D-IP | IP Protocol | Action | Total Matched Counter | Operation |
|---------------------------|----|---------|------|------|-------------|--------|-----------------------|-----------|
| No entries in this table. |    |         |      |      |             |        |                       |           |
| Total: 0                  |    |         |      |      |             |        |                       |           |

W sekcji **ACL Rules Table** kliknij  **Add**, aby pojawiło się poniższe okno.

Rys. 2-10 Konfiguracja reguły IP ACL

IP ACL Rule

---

ACL ID: 500  
 ACL Name: ACL1

Rule ID:   Auto Assign

Operation:

S-IP:  (Format: 192.168.0.1)  
 Mask:  (Format: 255.255.255.0)

D-IP:  (Format: 192.168.0.1)  
 Mask:  (Format: 255.255.255.0)

IP Protocol:

DSCP:

IP ToS:  (Optional, 0-15)

IP Pre:  (Optional, 0-7)

Time Range:  (Optional)

Logging:

Policy

---

Mirroring

Redirect

Rate Limit

QoS Remark

Wykonaj poniższe kroki, aby skonfigurować regułę IP ACL:

1) W sekcji **IP ACL Rule** skonfiguruj następujące parametry:

|                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|-----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Rule ID         | <p>Wpisz numer ID, aby umożliwić identyfikację reguły.</p> <p>Numer nie powinien być taki sam, jak numer ID aktualnej reguły na tej samej ACL. W przypadku wybrania opcji Auto Assign, ID reguły będzie przypisywany automatycznie w odstępie czasu 5.</p>                                                                                                                                                                                                                                                                                                                                                                                       |
| Operation       | <p>Wybierz działanie, które ma być wykonane, jeżeli pakiet jest dopasowany do reguły.</p> <p><b>Permit:</b> Jeżeli dopasowane pakiety mają być przekazywane.</p> <p><b>Deny:</b> Jeżeli dopasowane pakiety mają być odrzucane.</p>                                                                                                                                                                                                                                                                                                                                                                                                               |
| S-IP/Mask       | <p>Wprowadź źródłowy adres IP z maską. Wartość 1 w masce wskazuje na to, że odpowiadający bit w adresie zostanie dopasowany.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| D-IP/Mask       | <p>Wprowadź docelowy adres IP z maską. Wartość 1 w masce wskazuje na to, że odpowiadający bit w adresie zostanie dopasowany.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| IP Protocol     | <p>Wybierz z rozwijanej listy typ protokołu. Ustawienie domyślne to No Limit, co oznacza, że dopasowywane będą pakiety wszystkich protokołów. Można również wybrać opcję User-defined, aby odpowiednio dostosować protokół IP.</p>                                                                                                                                                                                                                                                                                                                                                                                                               |
| TCP Flag        | <p>W przypadku wybrania protokołu TCP dostępna jest opcja konfiguracji TCP Flag, funkcji służącej do działań dopasowywania reguły. Dostępnych jest sześć flag, z czego każda posiada trzy opcje: *, 0 i 1. Domyślnie ustawiona jest opcja *, wskazująca na to, że flaga nie jest wykorzystywana do działań dopasowywania.</p> <p><b>URG (urgent):</b> Flaga oznaczania jako pilne.</p> <p><b>ACK (acknowledge):</b> Flaga potwierdzania.</p> <p><b>PSH (push):</b> Flaga wymuszania przesyłu.</p> <p><b>RST (reset):</b> Flaga resetu.</p> <p><b>SYN (synchronize):</b> Flaga synchronizacji.</p> <p><b>FIN (finish):</b> Flaga zakańczania.</p> |
| S-Port / D-Port | <p>Jeżeli na protokół IP wybrana jest opcja TCP/UDP, określ numer portu źródłowego i docelowego z maską.</p> <p><b>Wartość:</b> Wyznacz numer portu.</p> <p><b>Maska:</b> Wyznacz maskę portu, używając 4 cyfr szesnastkowych.</p>                                                                                                                                                                                                                                                                                                                                                                                                               |
| DSCP            | <p>Określ wartość DSCP do dopasowania, między 0 a 63. Ustawienie domyślne to No Limit.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| IP ToS          | <p>Określ wartość ToS adresu IP do dopasowania, między 0 a 15. Ustawienie domyślne to No Limit.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| IP Pre          | <p>Określ wartość IP Precedencedo dopasowania, między 0 a 7. Ustawienie domyślne to No Limit.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |

|            |                                                                                                                                                                                                                                                                                                |
|------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Time Range | Określ zakres czasu, w którym będzie działała reguła. Ustawienie domyślne to No Limit, co oznacza, że reguła jest zawsze aktywna. Zakres czasu ustawić można na stronie <b>SYSTEM &gt; Time Range</b> .                                                                                        |
| Logging    | Włącz funkcję rejestrowania dla reguły ACL. Wtedy co pięć minut dopasowane reguły będą rejestrowane i wygenerowane zostaną powiązane pułapki (ang. trap). Aby sprawdzić, ile razy doszło do dopasowania, idź do Total Matched Counter (licznik wszystkich dopasowań) w sekcji ACL Rules Table. |

- 2) W sekcji **Policy** włącz lub wyłącz funkcję Mirroring dla dopasowanych pakietów. Jeżeli opcja ta jest włączona, należy wybrać port docelowy, na którym kopiowane będą pakiety.

Rys. 2-11 Konfiguracja funkcji Mirroring

- 3) W sekcji **Policy** włącz lub wyłącz funkcję Redirect dla dopasowanych pakietów. Jeżeli opcja jest włączona, należy wybrać port docelowy, do którego przekierowywane będą pakiety.

Rys. 2-12 Konfiguracja funkcji Redirect

### Uwaga:

Przy włączeniu funkcji Mirroring dopasowane pakiety zostaną skopiowane do portu docelowego, bez straty dla oryginalnego przekazywania. Przy włączeniu funkcji Redirect dopasowane pakiety będą przekazywane jedynie na porcie docelowym.

- 4) W sekcji **Policy** włącz lub wyłącz funkcję Rate Limit dla dopasowanych pakietów. W przypadku włączenia funkcji, należy skonfigurować następujące parametry.

Rys. 2-13 Konfiguracja funkcji Rate Limit

Rate Limit

Rate:  Kbps (1-10000000)

Burst Size:  KB (1-128)

Out of Band:

|                    |                                                                                                                                                                                           |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Rate</b>        | Wyznacz prędkość transmisji dopasowanych pakietów.                                                                                                                                        |
| <b>Burst Size</b>  | Określ maks. dopuszczalną liczbę bitów na sekundę.                                                                                                                                        |
| <b>Out of Band</b> | Wybierz działanie dla pakietów, których prędkość znajduje się poza wyznaczonym zakresem.<br><br><b>None:</b> Pakiety będą przekazywane normalnie.<br><b>Drop:</b> Pakiety będą odrzucane. |

- 5) W sekcji **Policy** włącz lub wyłącz funkcję QoS Remark dla dopasowanych pakietów. Jeżeli funkcja jest włączona, należy skonfigurować powiązane parametry, a wprowadzone wartości będą zastosowane w przetwarzaniu QoS na przełączniku.

Rys. 2-14 Konfiguracja funkcji QoS Remark

QoS Remark

DSCP:

Local Priority:

802.1p Priority:

|                        |                                                                                                                              |
|------------------------|------------------------------------------------------------------------------------------------------------------------------|
| <b>DSCP</b>            | Określ pole DSCP dla dopasowanych pakietów. Pole DSCP pakietów będzie zmienione na to wyznaczone pole.                       |
| <b>Local Priority</b>  | Określ priorytet lokalny dla dopasowanych pakietów. Priorytet lokalny pakietów będzie zmieniony na ten wyznaczony priorytet. |
| <b>802.1p Priority</b> | Określ priorytet 802.1p dla dopasowanych pakietów. Priorytet 802.1p pakietów będzie zmieniony na ten wyznaczony priorytet.   |

- 6) Kliknij **Apply**.

## Konfiguracja łączonej reguły ACL

Kliknij **Edit ACL** dla wpisu Combined ACL, aby wyświetlić poniższą stronę.

Rys.2-15 Konfiguracja łączonej reguły ACL

ACL Details

ACL Type: Combined ACL  
ACL ID: 1000  
ACL Name: ACL\_1000

ACL Rules Table

 Resequence  Add  Delete  Refresh

| <input type="checkbox"/>  | ID | Rule ID | S-MAC | D-MAC | S-IP | D-IP | VID | Action | Total Matched Counter | Operation |
|---------------------------|----|---------|-------|-------|------|------|-----|--------|-----------------------|-----------|
| No entries in this table. |    |         |       |       |      |      |     |        |                       |           |
| Total: 0                  |    |         |       |       |      |      |     |        |                       |           |

W sekcji **ACL Rules Table** kliknij  Add, a pojawi się następujące okno.



Rys. 2-16 Konfiguracja łączonej reguły ACL

**Combined ACL Rule**

---

ACL ID: 1000  
 ACL Name: ACL\_1000  
 Rule ID:   Auto Assign  
 Operation: Permit ▼

S-MAC:  (Format: FF-FF-FF-FF-FF-FF)  
 Mask:  (Format: FF-FF-FF-FF-FF-FF)  
 D-MAC:  (Format: FF-FF-FF-FF-FF-FF)  
 Mask:  (Format: FF-FF-FF-FF-FF-FF)  
 VLAN ID:  (1-4094)  
 EtherType:  (4-hex number)  
 S-IP:  (Format: 192.168.0.1)  
 Mask:  (Format: 255.255.255.0)  
 D-IP:  (Format: 192.168.0.1)  
 Mask:  (Format: 255.255.255.0)  
 IP Protocol: No Limit ▼  
 DSCP: No Limit ▼  
 IP ToS:  (Optional, 0-15)  
 IP Pre:  (Optional, 0-7)  
 User Priority: Default ▼  
 Time Range:  ▼ (Optional)  
 Logging: Disable ▼

---

**Policy**

Mirroring  
 Redirect  
 Rate Limit  
 QoS Remark

Wykonaj poniższe kroki, aby skonfigurować łączonej regułę ACL:

1) W sekcji **Combined ACL Rule** skonfiguruj następujące parametry:

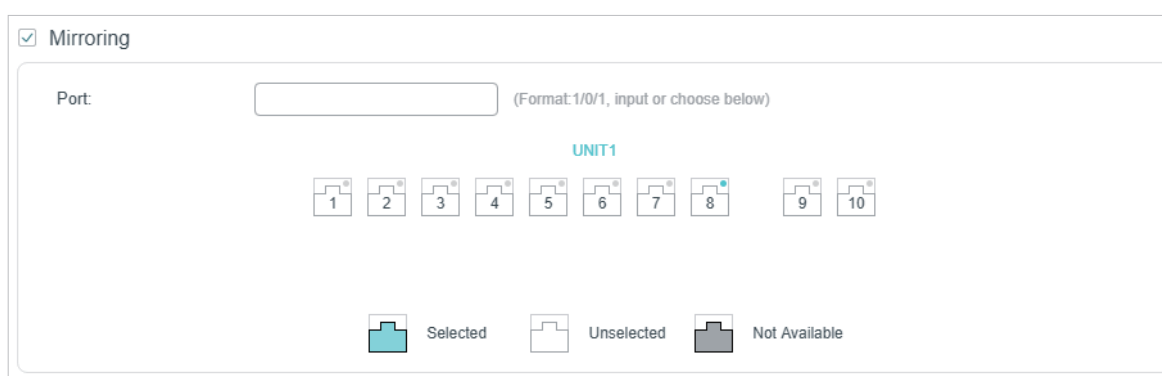
|         |                                                                                                                                                                                                                                                                    |
|---------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Rule ID | Wpisz numer ID, aby umożliwić identyfikację reguły.<br><br>Numer nie powinien być taki sam, jak jakiegokolwiek numer ID aktualnej reguły na tej samej ACL. W przypadku wybrania opcji Auto Assign, ID reguły będzie przypisywany automatycznie w odstępie czasu 5. |
|---------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

|                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|-----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Operation       | <p>Wybierz działanie, które ma być wykonane, jeżeli pakiet jest dopasowany do reguły.</p> <p><b>Permit:</b> Jeżeli dopasowane pakiety mają być przekazywane.</p> <p><b>Deny:</b> Jeżeli dopasowane pakiety mają być odrzucane.</p>                                                                                                                                                                                                                                                                                                                                                                                                               |
| S-MAC/Mask      | Wprowadź źródłowy adres MAC z maską. Wartość 1 w masce wskazuje na to, że odpowiadający bit w adresie zostanie dopasowany.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| D-MAC/Mask      | Wprowadź docelowy adres IP z maską. Wartość 1 w masce wskazuje na to, że odpowiadający bit w adresie zostanie dopasowany.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| VLAN ID         | Wprowadź numer ID sieci VLAN, do której zastosowanie będzie miała ACL.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| EtherType       | Określ EtherType, który będzie dopasowany, używając 4 liczb szesnastkowych.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| S-IP/Mask       | Wprowadź źródłowy adres IP z maską. Wartość 1 w masce wskazuje na to, że odpowiadający bit w adresie zostanie dopasowany.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| D-IP/Mask       | Wprowadź docelowy adres IP z maską. Wartość 1 w masce wskazuje na to, że odpowiadający bit w adresie zostanie dopasowany.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| IP Protocol     | Wybierz z rozwijanej listy typ protokołu. Ustawienie domyślne to No Limit, co oznacza, że dopasowywane będą pakiety wszystkich protokołów. Można również wybrać opcję User-defined, aby odpowiednio dostosować protokół IP.                                                                                                                                                                                                                                                                                                                                                                                                                      |
| TCP Flag        | <p>W przypadku wybrania protokołu TCP dostępna jest opcja konfiguracji TCP Flag, funkcji służącej do działań dopasowywania reguły. Dostępnych jest sześć flag, z czego każda posiada trzy opcje: *, 0 i 1. Domyślnie ustawiona jest opcja *, wskazująca na to, że flaga nie jest wykorzystywana do działań dopasowywania.</p> <p><b>URG (urgent):</b> Flaga oznaczania jako pilne.</p> <p><b>ACK (acknowledge):</b> Flaga potwierdzenia.</p> <p><b>PSH (push):</b> Flaga wymuszania przesyłu.</p> <p><b>RST (reset):</b> Flaga resetu.</p> <p><b>SYN (synchronize):</b> Flaga synchronizacji.</p> <p><b>FIN (finish):</b> Flaga zakańczania.</p> |
| S-Port / D-Port | <p>Jeżeli na protokół IP wybrana jest opcja TCP/UDP, określ numer portu źródłowego i docelowego z maską.</p> <p><b>Wartość:</b> Wyznacz numer portu.</p> <p><b>Maska:</b> Wyznacz maskę portu, używając 4 cyfr szesnastkowych.</p>                                                                                                                                                                                                                                                                                                                                                                                                               |
| DSCP            | Określ wartość DSCP do dopasowania, między 0 a 63. Ustawienie domyślne to No Limit.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| IP ToS          | Określ wartość ToS adresu IP do dopasowania, między 0 a 15. Ustawienie domyślne to No Limit.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| IP Pre          | Określ wartość IP Precedence dopasowania, między 0 a 7. Ustawienie domyślne to No Limit.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |

|               |                                                                                                                                                                                                                                                                                                |
|---------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| User Priority | Wyznacz User Priority do dopasowania.                                                                                                                                                                                                                                                          |
| Time Range    | Określ zakres czasu, w którym będzie działała reguła. Ustawienie domyślne to No Limit, co oznacza, że reguła jest zawsze aktywna. Zakres czasu ustawić można na stronie <b>SYSTEM &gt; Time Range</b> .                                                                                        |
| Logging       | Włącz funkcję rejestrowania dla reguły ACL. Wtedy co pięć minut dopasowane reguły będą rejestrowane i wygenerowane zostaną powiązane pułapki (ang. trap). Aby sprawdzić, ile razy doszło do dopasowania, idź do Total Matched Counter (licznik wszystkich dopasowań) w sekcji ACL Rules Table. |

- 2) W sekcji **Policy** włącz lub wyłącz funkcję Mirroring dla dopasowanych pakietów. Jeżeli opcja jest włączona, należy wybrać port docelowy, do którego pakiety będą kopiowane.

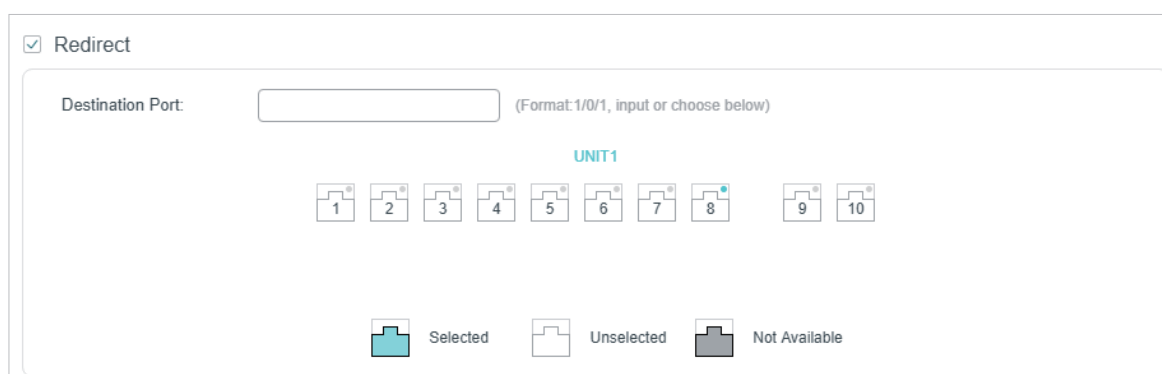
Rys. 2-17 Konfiguracja funkcji Mirroring



Mirroring  
 Port:  (Format: 1/0/1, input or choose below)  
 UNIT1  
 1 2 3 4 5 6 7 8 9 10  
 Selected Unselected Not Available

- 3) W sekcji **Policy** włącz lub wyłącz funkcję Redirect dla dopasowanych pakietów. Jeżeli opcja jest włączona, należy wybrać port docelowy, na który przekierowywane będą pakiety.

Rys. 2-18 Konfiguracja funkcji Redirect



Redirect  
 Destination Port:  (Format: 1/0/1, input or choose below)  
 UNIT1  
 1 2 3 4 5 6 7 8 9 10  
 Selected Unselected Not Available

#### Uwaga:

Przy włączeniu funkcji Mirroring dopasowane pakiety zostaną skopiowane do portu docelowego, bez straty dla oryginalnego przekazywania. Przy włączeniu funkcji Redirect dopasowane pakiety będą przekazywane jedynie na porcie docelowym.

- 4) W sekcji **Policy** włącz lub wyłącz funkcję Rate Limit dla dopasowanych pakietów. Jeżeli funkcja jest włączona, należy skonfigurować powiązane parametry.

Rys. 2-19 Konfiguracja funkcji Rate Limit

Rate Limit

Rate:  Kbps (1-10000000)

Burst Size:  KB (1-128)

Out of Band:

**Rate** Wyznacz prędkość transmisji dopasowanych pakietów.

**Burst Size** Określ maks. dopuszczalną liczbę bitów na sekundę.

**Out of Band** Wybierz działanie dla pakietów, których prędkość znajduje się poza wyznaczonym zakresem.

**None:** Pakiety będą przekazywane normalnie.

**Drop:** Pakiety będą odrzucane.

- 5) W sekcji **Policy** włącz lub wyłącz funkcję QoS Remark dla dopasowanych pakietów. Jeżeli opcja jest włączona, należy skonfigurować powiązane parametry, a wprowadzone wartości będą zastosowane w przetwarzaniu QoS na przełączniku.

Rys. 2-20 Konfiguracja funkcji QoS Remark

QoS Remark

DSCP:  Default ▼

Local Priority:  Default ▼

802.1p Priority:  Default ▼

**DSCP** Określ pole DSCP dla dopasowanych pakietów. Pole DSCP pakietów będzie zmienione na to wyznaczone pole.

**Local Priority** Określ priorytet lokalny dla dopasowanych pakietów. Priorytet lokalny pakietów będzie zmieniony na ten wyznaczony priorytet.

**802.1p Priority** Określ priorytet 802.1p dla dopasowanych pakietów. Priorytet 802.1p pakietów będzie zmieniony na ten wyznaczony priorytet.

- 6) Kliknij **Apply**.

## Konfiguracja reguły IPv6 ACL

Kliknij **Edit ACL** dla wpisu IPv6 ACL, aby wyświetlić poniższą stronę.

Rys. 2-21 Konfiguracja reguły IPv6 ACL





ACL Details

---

ACL Type: IPv6 ACL  
 ACL ID: 1500  
 ACL Name: ACL\_1500

ACL Rules Table

---

 Resequenece  Add  Delete  Refresh

| <input type="checkbox"/>  | ID | Rule ID | IPv6 Source IP | IPv6 Destination IP | Action | Total Matched Counter | Operation |
|---------------------------|----|---------|----------------|---------------------|--------|-----------------------|-----------|
| No entries in this table. |    |         |                |                     |        |                       |           |
| Total: 0                  |    |         |                |                     |        |                       |           |

W sekcji **ACL Rules Table** kliknij  **Add**, aby pojawiło się poniższe okno.

Rys. 2-22 Konfiguracja reguły IPv6 ACL

IPv6 ACL Rule

---

ACL ID: 1500  
 ACL Name: ACL\_1500

Rule ID:   Auto Assign

Operation:

IPv6 Class:  (0-63)

Flow Label:  (5-hex number: 0x00000-0xFFFFF)

IPv6 Source IP:  (Format: 2001::)  
 Mask:  (Format: FFFF:FFFF:FFFF:FFFF)

IPv6 Destination IP:  (Format: 2001::)  
 Mask:  (Format: FFFF:FFFF:FFFF:FFFF)

IP Protocol:

Time Range:  (Optional)

Policy

---

Mirroring

Redirect

Rate Limit

QoS Remark

Wykonaj poniższe kroki, aby skonfigurować regułę IPv6 ACL:

1) W sekcji **IPv6 ACL Rule** skonfiguruj następujące parametry:

|                     |                                                                                                                                                                                                                                                                                                                                                             |
|---------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Rule ID             | <p>Wpisz numer ID, aby umożliwić identyfikację reguły.</p> <p>Numer nie powinien być taki sam, jak jakiegokolwiek numer ID aktualnej reguły na tej samej ACL. W przypadku wybrania opcji Auto Assign, ID reguły będzie przypisywany automatycznie w odstępie czasu 5.</p>                                                                                   |
| Operation           | <p>Wybierz działanie, które ma być wykonane, jeżeli pakiet jest dopasowany do reguły.</p> <p><b>Permit:</b> Jeżeli dopasowane pakiety mają być przekazywane.</p> <p><b>Deny:</b> Jeżeli dopasowane pakiety mają być odrzucane.</p>                                                                                                                          |
| IPv6 Class          | Wyznacz wartość klasy IPv6 do dopasowania. Przełącznik sprawdzi pole klasy nagłówka IPv6.                                                                                                                                                                                                                                                                   |
| Flow Label          | Wyznacz wartość Flow Label do dopasowania.                                                                                                                                                                                                                                                                                                                  |
| IPv6 Source IP      | Wpisz źródłowy adres IPv6 do dopasowania. Sprawdzony zostanie każdy typ adresu IPv6. Możesz wprowadzić pełny 128-bitowy adres IPv6, ale znaczenie będą miały tylko pierwsze 64 bity.                                                                                                                                                                        |
| Mask                | <p>Maska jest wymagana, jeżeli podany jest źródłowy adres IPv6. Wpisz maskę w pełnym formacie (np. FFFF:FFFF:0000:FFFF).</p> <p>Maska adresu IP wyznacza, które bity w źródłowym adresie IPv6 mają być dopasowane do reguły. Wartość 1 w masce wskazuje na to, że odpowiadający bit w adresie zostanie dopasowany.</p>                                      |
| IPv6 Destination IP | Wpisz źródłowy adres IPv6 do dopasowania. Sprawdzony zostanie każdy typ adresu IPv6. Możesz wprowadzić pełny 128-bitowy adres IPv6, ale znaczenie będą miały tylko pierwsze 64 bity.                                                                                                                                                                        |
| Mask                | <p>Maska jest wymagana, jeżeli podany jest docelowy adres IPv6. Wpisz maskę w pełnym formacie (np. FFFF:FFFF:0000:FFFF).</p> <p>Maska adresu IP wyznacza, które bity w źródłowym adresie IP mają być dopasowane do reguły. Wartość 1 w masce wskazuje na to, że odpowiadający bit w adresie zostanie dopasowany.</p>                                        |
| IP Protocol         | <p>Wybierz z rozwijanej listy typ protokołu.</p> <p><b>No Limit:</b> Dopasowane będą pakiety wszystkich protokołów.</p> <p><b>UDP:</b> Wyznacz port źródłowy i docelowy do dopasowania pakietu UDP.</p> <p><b>TCP:</b> Wyznacz port źródłowy i docelowy do dopasowania pakietu TCP.</p> <p><b>User-defined:</b> Możesz dowolnie dostosować protokół IP.</p> |
| S-Port / D-Port     | Jeżeli na protokół IP wybrana jest opcja TCP/UDP, określ numer portu źródłowego i docelowego.                                                                                                                                                                                                                                                               |
| Time Range          | Określ zakres czasu, w którym będzie działała reguła. Ustawienie domyślne to No Limit, co oznacza, że reguła jest zawsze aktywna. Zakres czasu ustawić można na stronie <b>SYSTEM &gt; Time Range</b> .                                                                                                                                                     |

- 2) W sekcji **Policy** włącz lub wyłącz funkcję Mirroring dla dopasowanych pakietów. Jeżeli opcja jest włączona, wybierz port docelowy, na który kopiowane będą pakiety.

Rys. 2-23 Konfiguracja funkcji Mirroring

- 3) W sekcji **Policy** włącz lub wyłącz funkcję Redirect dla dopasowanych pakietów. Jeżeli opcja jest włączona, należy wybrać port docelowy, do którego pakiety będą przekierowywane.

Rys. 2-24 Konfiguracja funkcji Redirect

#### Uwaga:

Przy włączeniu funkcji Mirroring dopasowane pakiety zostaną skopiowane do portu docelowego, bez straty dla oryginalnego przekazywania. Przy włączeniu funkcji Redirect dopasowane pakiety będą przekazywane jedynie na porcie docelowym.

- 4) W sekcji **Policy** włącz lub wyłącz funkcję Rate Limit dla dopasowanych pakietów. Jeżeli opcja jest włączona, należy skonfigurować powiązane parametry.

Rys. 2-25 Konfiguracja funkcji Rate Limit

**Rate** Wyznacz prędkość transmisji dopasowanych pakietów.

**Burst Size** Określ maks. dopuszczalną liczbę bitów na sekundę.

**Out of Band**

Wybierz działanie dla pakietów, których prędkość znajduje się poza wyznaczonym zakresem.

**None:** Pakiety będą przekazywane normalnie.

**Drop:** Pakiety będą odrzucane.

- 5) W sekcji **Policy** włącz lub wyłącz funkcję QoS Remark dla dopasowanych pakietów. Jeżeli funkcja jest włączona, należy skonfigurować powiązane parametry, a wprowadzone wartości będą zastosowane w przetwarzaniu QoS na przełączniku.

Rys. 2-26 Konfiguracja funkcji QoS Remark

QoS Remark

DSCP: Default ▼

Local Priority: Default ▼

802.1p Priority: Default ▼

**DSCP**

Określ pole DSCP dla dopasowanych pakietów. Pole DSCP pakietów będzie zmienione na to wyznaczone pole.

**Local Priority**

Określ priorytet lokalny dla dopasowanych pakietów. Priorytet lokalny pakietów będzie zmieniony na ten wyznaczony priorytet.

**802.1p Priority**

Określ priorytet lokalny dla dopasowanych pakietów. Priorytet lokalny pakietów będzie zmieniony na ten wyznaczony priorytet.

- 6) Kliknij **Apply**.

## Wyświetlanie reguł ACL

Reguły ACL wymienione są w kolejności rosnącej ID reguły. Przełącznik dopasowuje otrzymany pakiet do reguł według ich kolejności. Jeżeli pakiet jest dopasowany do reguły, przełącznik przerywa proces dopasowywania i wykonuje działanie wyznaczone przez regułę.

Kliknij **Edit ACL** przy utworzonym przez siebie wpisie, a wyświetli się tablica reguł. Jako przykład pokazana jest tablica reguł IP ACL.

Rys. 2-27 Wyświetlanie tablicy reguł ACL

| ACL Rules Table          |    |            |             |             |             |                          |                       |           |
|--------------------------|----|------------|-------------|-------------|-------------|--------------------------|-----------------------|-----------|
|                          |    | Resequence |             |             |             | + Add - Delete ↻ Refresh |                       |           |
| <input type="checkbox"/> | ID | Rule ID    | S-IP        | D-IP        | IP Protocol | Action                   | Total Matched Counter | Operation |
| <input type="checkbox"/> | 1  | 1          | 192.168.1.0 | 192.168.5.0 |             | Permit                   | 0                     |           |
| <input type="checkbox"/> | 2  | 3          | 192.168.7.0 |             |             | Permit                   | 0                     |           |
| <input type="checkbox"/> | 3  | 5          | 192.168.0.0 |             |             | Deny                     | 0                     |           |
| <b>Total: 3</b>          |    |            |             |             |             |                          |                       |           |



Tutaj możesz wyświetlać i edytować reguły ACL. Możesz również kliknąć **Resequence**, aby zmienić kolejność reguł, podając ID pierwszej reguły (Start Rule ID) i wartość krokową.

## 2.1.4 Konfiguracja wiązania ACL

Możesz powiązać ACL z portem lub siecią VLAN. Pakiety odebrane na porcie lub w sieci VLAN będą dopasowane i przetworzone zgodnie z regułami ACL. ACL zacznie działać dopiero po powiązaniu jej z portem lub siecią VLAN.

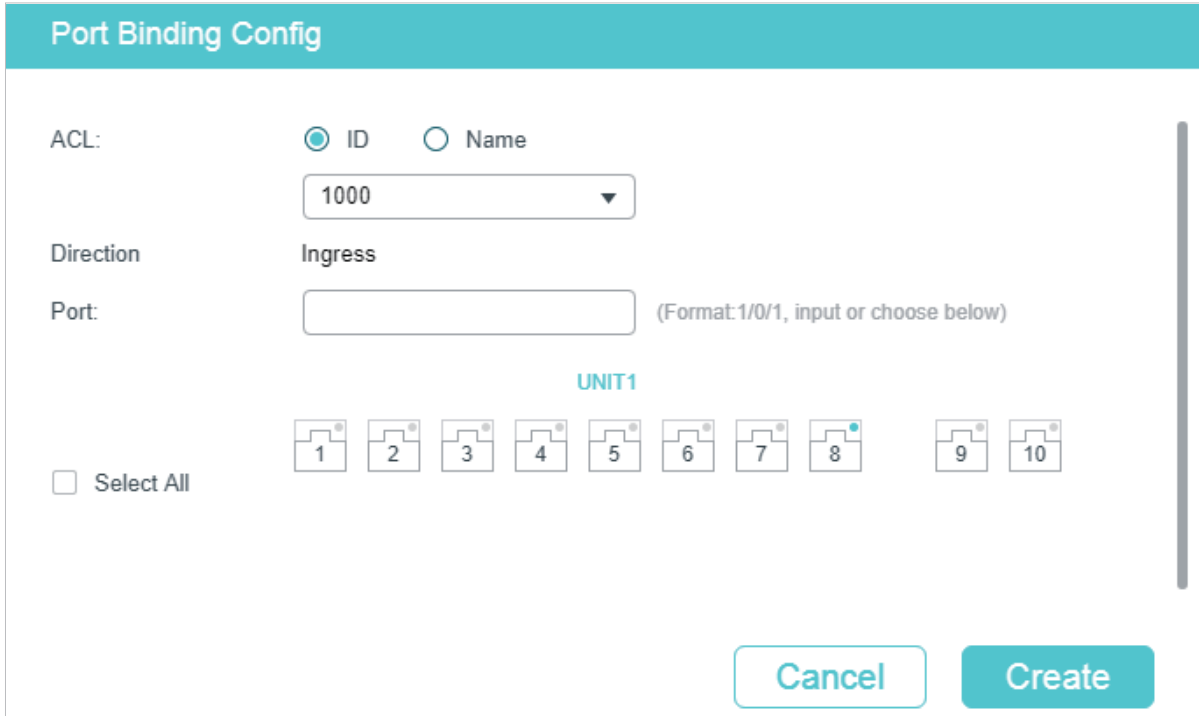
### Uwaga:

- Różne typy ACL nie mogą być powiązane z tym samym portem lub siecią VLAN.
- Liczne ACL tego samego typu mogą być powiązane z tym samym portem lub siecią VLAN. Przełącznik dopasowuje odebrane pakiety wykorzystując listy ACL, zgodnie z kolejnością. Im wcześniej ACL została powiązana, tym większy ma priorytet.

### ■ Wiązanie ACL z portem

Wybierz z menu **SECURITY > ACL > ACL Binding > Port Binding** i kliknij  **Add**, aby wyświetlić poniższą stronę.

Rys. 2-28 Wiązanie ACL z portem



Wykonaj poniższe kroki, aby powiązać ACL z portem:

- 1) Wybierz ID lub Nazwę, wykorzystywane do dopasowywania ACL. Następnie wybierz ACL z rozwijanej listy.
- 2) Wyznacz port do wiązania.
- 3) Kliknij **Create**.

## ■ Wiązanie ACL z VLAN

Wybierz z menu **SECURITY > ACL > ACL Binding > VLAN Binding**, aby wyświetlić poniższą stronę.

Rys. 2-29 Wiązanie ACL z VLAN-em

Wykonaj poniższe kroki, aby powiązać ACL z VLAN-em:

- 1) Wybierz ID lub Nazwę, wykorzystywane do dopasowywania ACL. Następnie wybierz ACL z rozwijanej listy.
- 2) Wprowadź ID sieci VLAN do wiązania.
- 3) Click **Create**.

## 2.2 Przez CLI

### 2.2.1 Konfiguracja zakresu czasu

Niektóre usługi lub funkcje bazujące na ACL mogą wymagać ograniczenia ich działania do wyznaczonego zakresu czasu. W tym przypadku możesz skonfigurować zakres czasu ACL. Więcej szczegółów dotyczących konfiguracji zakresu czasu znajdziesz w rozdziale *Zarządzanie systemem*.

### 2.2.2 Konfiguracja ACL

Aby utworzyć ACL różnego typu i skonfigurować reguły ACL, wykonaj poniższe kroki.

Możesz zdefiniować reguły w oparciu o źródłowy adres MAC lub IP, docelowy adres MAC lub IP, typ protokołu, numer portu itd.

#### ■ MAC ACL

---

Krok 1     **configure**

Uruchom tryb konfiguracji globalnej.

---

---

**Krok 2      `access-list create acl-id [name acl-name]`**

Utwórz MAC ACL.

*acl-id*: Wprowadź ACL ID. ID mieści się w zakresie od 0 do 499.

*acl-name*: Wprowadź nazwę, aby umożliwić identyfikację ACL.

---

**Krok 3      `access-list mac acl-id-or-name rule { auto | rule-id } { deny | permit } logging {enable | disable} [ smac source-mac smask source-mac-mask ] [ dmac destination-mac dmask destination-mac-mask ] [type ether-type] [pri dot1p-priority] [vid vlan-id] [tseg time-range-name]`**

Dodaj regułę MAC ACL.

*acl-id-or-name*: Wprowadź ID lub nazwę ACL, do której chcesz dodać regułę.

*auto*: ID reguły będzie przypisany automatycznie. Odstęp czasu między przypisywaniem regułom ID to 5 sekund.

*rule-id*: Przypisz ID do reguły.

*deny | permit*: Określ, jakie działanie ma być wykonane względem pakietów dopasowanych do reguły. Domyślnie ustawiona jest opcja Permit. W przypadku wybrania opcji Deny pakiety będą odrzucane; w przypadku wybrania funkcji Permit pakiety będą przekazywane.

**logging {enable | disable}**: Włącz lub wyłącz funkcję Logging dla reguły ACL. W przypadku włączenia funkcji, dopasowane reguły będą rejestrowane raz na 5 minut. Jeżeli włączysz funkcję ACL Counter trap, po zmianie czasu dopasowania wygenerowana zostanie powiązana pułapka (ang. trap).

*source-mac*: Wprowadź źródłowy adres MAC. Prawidłowy format to FF:FF:FF:FF:FF:FF.

*source-mac-mask*: Wprowadź maskę źródłowego adresu MAC. Jest to konieczne w przypadku wprowadzenia źródłowego adresu MAC. Prawidłowy format to FF:FF:FF:FF:FF:FF.

*destination-mac*: Wprowadź docelowy adres MAC. Prawidłowy format to FF:FF:FF:FF:FF:FF.

*destination-mac-mask*: Wprowadź maskę docelowego adresu MAC. Jest to konieczne w przypadku wprowadzenia docelowego adresu MAC. Prawidłowy format to FF:FF:FF:FF:FF:FF.

*ether-type*: Wyznacz typ Ethernet, używając 4 cyfr szesnastkowych.

*dot1p-priority*: Priorytet użytkownika wynosi od 0 do 7. Ustawienie domyślne to No Limit.

*vlan-id*: VLAN ID wynosi od 1 do 4094.

*time-range-name*: Nazwa zakresu czasu. Ustawienie domyślne to No Limit.

---

**Krok 4      `exit`**

Wróć do trybu konfiguracji globalnej.

---

**Krok 5      `show access-list [ acl-id-or-name ]`**

Wyświetl aktualną konfigurację ACL.

*acl-id-or-name*: Numer ID i nazwa ACL.

---

**Krok 6      `end`**

Powróć do trybu privileged EXEC.

---

---

**Krok 7    copy running-config startup-config**

Zapisz ustawienia w pliku konfiguracyjnym.

---

Poniższy przykład prezentuje tworzenie MAC ACL 50 i konfigurację reguły 5 (Rule 5) do przesyłania pakietów (permit) o źródłowym adresie MAC 00:34:A2:D4:34:B5:

**Switch#configure**

**Switch(config)#access-list create 50**

**Switch(config-mac-acl)#access-list mac 50 rule 5 permit logging disable smac 00:34:A2:D4:34:B5 smask FF:FF:FF:FF:FF:FF**

**Switch(config-mac-acl)#exit**

**Switch(config)#show access-list 50**

MAC access list 50 name: ACL\_50

rule 5 permit logging disable smac 00:34:a2:d4:34:b5 smask ff:ff:ff:ff:ff:ff

**Switch(config)#end**

**Switch#copy running-config startup-config**

## ■ IP ACL

---

**Krok 1    configure**

Uruchom tryb konfiguracji globalnej.

---

**Krok 2    access-list create *acl-id* [*name acl-name*]**

Utwórz IP ACL.

*acl-id*: Wprowadź ACL ID. ID wynosi od 500 do 999.

*acl-name*: Wprowadź nazwę, aby umożliwić identyfikację ACL.

---

Krok 3 **access-list ip** *acl-id-or-name* **rule** {auto | *rule-id* } {deny | permit} **logging** {enable | disable} [**sip** *sip-address* **sip-mask** *sip-address-mask* ] [ **dip** *dip-address* **dip-mask** *dip-address-mask* ] [**dscp** *dscp-value*] [**tos** *tos-value*] [**pre** *pre-value*] [**frag** {enable | disable}] [**protocol** *protocol* [**s-port** *s-port-number* **s-port-mask** *s-port-mask*] [**d-port** *d-port-number* **d-port-mask** *d-port-mask*] [**tcpflag** *tcpflag*]] [**tseg** *time-range-name*]

Dodaj reguły do ACL.

*acl-id-or-name*: Wprowadź ID lub nazwę ACL, do której chcesz dodać regułę.

*auto*: ID reguły będzie przypisany automatycznie. Odstęp czasu między przypisywaniem regułom ID to 5 sekund.

*rule-id*: Przypisz ID do reguły.

*deny* | *permit*: Określ, jakie działanie ma być wykonane względem pakietów dopasowanych do reguły. Domyślnie ustawiona jest opcja Permit. W przypadku wybrania opcji Deny pakiety będą odrzucane; w przypadku wybrania funkcji Permit pakiety będą przekazywane.

**logging** {enable | disable}: Włącz lub wyłącz funkcję Logging dla reguły ACL. W przypadku włączenia funkcji, dopasowane reguły będą rejestrowane raz na 5 minut. Jeżeli włączysz funkcję ACL Counter trap, po zmianie czasu dopasowania wygenerowana zostanie powiązana pułapka (ang. trap).

*sip-address*: Wprowadź źródłowy adres IP.

*sip-address-mask*: Wprowadź maskę źródłowego adresu IP. Jest to konieczne w przypadku wprowadzenia źródłowego adresu IP.

*dip-address*: Wprowadź docelowy adres IP.

*dip-address-mask*: Wprowadź maskę docelowego adresu IP. Jest to konieczne w przypadku wprowadzenia docelowego adresu IP.

*dscp-value*: Wyznacz wartość DSCP, między 0 a 63.

*tos-value*: Wyznacz wartość ToS adresu IP do dopasowania, między 0 a 15.

*pre-value*: Wyznacz wartość IP Precedence do dopasowania, między 0 a 7.

**frag** {enable | disable}: Włącz lub wyłącz dopasowywanie pakietów podzielonych na fragmenty. Funkcja jest domyślnie wyłączona. Jeżeli funkcja jest włączona, reguła będzie miała zastosowanie do wszystkich pakietów podzielonych na fragmenty i zawsze dopuści przekazywanie ostatniego fragmetu pakietu.

*protocol*: Wyznacz numer protokołu, między 0 a 255.

*s-port-number*: W przypadku ustawienia na protokół TCP lub UDP należy wyznaczyć numer portu źródłowego.

*s-port-mask*: W przypadku ustawienia na protokół TCP lub UDP należy wyznaczyć maskę portu źródłowego, używając 4 cyfr szesnastkowych.

*d-port-number*: W przypadku ustawienia na protokół TCP lub UDP należy wyznaczyć numer portu docelowego.

*d-port-mask*: W przypadku ustawienia na protokół TCP lub UDP należy wyznaczyć maskę portu docelowego, używając 4 cyfr szesnastkowych.

*tcpflag*: W przypadku ustawienia na protokół TCP należy wyznaczyć wartość flagi, używając liczb binarnych lub \* (np. 01\*010\*). Ustawienie domyślne to \*, oznaczające, że flaga nie zostanie dopasowana.

Dostępne flagi to URG (Urgent flag), ACK (Acknowledge Flag), PSH (Push Flag), RST (Reset Flag), SYN (Synchronize Flag) and FIN (Finish Flag).

*time-range-name*: Nazwa zakresu czasu. Ustawienie domyślne to No Limit.

---

Krok 4     **end**

Powrót do trybu privileged EXEC.

---

Krok 5     **copy running-config startup-config**

Zapisz ustawienia w pliku konfiguracyjnym.

---

Poniższy przykład prezentuje tworzenie IP ACL 600, konfigurację Rule 1 na przesyłanie (permit) pakietów o źródłowym adresie IP 192.168.1.100:

**Switch#configure**

**Switch(config)#access-list create 600**

**Switch(config)#access-list ip 600 rule 1 permit logging disable sip 192.168.1.100 sip-mask 255.255.255.255**

**Switch(config)#show access-list 600**

IP access list 600 name: ACL\_600

rule 1 permit logging disable sip 192.168.1.100 smask 255.255.255.255

**Switch(config)#end**

**Switch#copy running-config startup-config**

## ■ Combined ACL

### Krok 1 **configure**

Uruchom tryb konfiguracji globalnej.

### Krok 2 **access-list create *acl-id* [name *acl-name*]**

Utwórz Combined ACL (łązoną ACL).

*acl-id*: Wprowadź ACL ID. ID wynosi od 1000 do 1499.

*acl-name*: Wprowadź nazwę, aby umożliwić identyfikację ACL.

### Krok 3

**access-list combined *acl-id-or-name* rule {auto | *rule-id* } {deny | permit} logging {enable | disable} [*smac* *source-mac-address* *smask* *source-mac-mask*] [*dmac* *dest-mac-address* *dmask* *dest-mac-mask*] [*vid* *vlan-id*] [*type* *ether-type*] [*pri* *priority*] [*sip* *sip-address* *sip-mask* *sip-address-mask*] [*dip* *dip-address* *dip-mask* *dip-address-mask*] [*dscp* *dscp-value*] [*tos* *tos-value*] [*pre* *pre-value*] [*protocol* *protocol*] [*s-port* *s-port-number* *s-port-mask* *s-port-mask*] [*d-port* *d-port-number* *d-port-mask* *d-port-mask*] [*tcpflag* *tcpflag*] [*tseg* *time-range-name*]**

Dodaj reguły do ACL.

*acl-id-or-name*: Wprowadź ID lub nazwę ACL, go której chcesz dodać regułę.

*auto*: ID reguły będzie przypisany automatycznie. Odstęp czasu między przypisywaniem regułom ID to 5 sekund.

*rule-id*: Przypisz ID do reguły.

*deny* | *permit*: kreśl, jakie działanie ma być wykonane względem pakietów dopasowanych do reguły. Domyślnie ustawiona jest opcja Permit. W przypadku wybrania opcji Deny pakiety będą odrzucane; w przypadku wybrania funkcji Permit pakiety będą przekazywane.

**logging** {enable | disable}: Włącz lub wyłącz funkcję Logging dla reguły ACL. W przypadku włączenia funkcji, dopasowane reguły będą rejestrowane raz na 5 minut. Jeżeli włączysz funkcję ACL Counter trap, po zmianie czasu dopasowania wygenerowana zostanie powiązana pułapka (ang. trap).

*source-mac-address*: Wprowadź źródłowy adres MAC.

*source-mac-mask*: Wprowadź maskę źródłowego adresu MAC.

*dest-mac-address*: Wprowadź docelowy adres MAC

*dest-mac-mask*: Wprowadź maskę docelowego adresu MAC. Jest to konieczne w przypadku wprowadzenia docelowego adresu MAC.

*vlan-id*: VLAN ID wynosi od 1 do 4094.

*ether-type*: Wyznacz typ Ethernet, używając 4 cyfr szesnastkowych.

*priority*: Priorytet użytkownika wynosi od 0 do 7. Ustawienie domyślne to No Limit.

*sip-address*: Wprowadź źródłowy adres IP.

*sip-address-mask*: Wprowadź maskę źródłowego adresu IP. Jest to konieczne w przypadku wprowadzenia źródłowego adresu IP.

*dip-address*: Jest to konieczne w przypadku wprowadzenia źródłowego adresu IP.

*dip-address-mask*: Wprowadź maskę docelowego adresu IP. Jest to konieczne w przypadku wprowadzenia docelowego adresu IP.

*dscp-value*: Wyznacz wartość DSCP między 0 a 63.

*tos-value*: Wyznacz wartość ToS adresu IP do dopasowania, między 0 a 15.

*protocol*: Wyznacz numer protokołu, między 0 a 255.

*s-port-number*: W przypadku ustawienia na protokół TCP lub UDP należy wyznaczyć numer portu źródłowego.

*s-port-mask*: W przypadku ustawienia na protokół TCP lub UDP należy wyznaczyć maskę portu źródłowego, używając 4 cyfr szesnastkowych.

*d-port-number*: W przypadku ustawienia na protokół TCP lub UDP należy wyznaczyć numer portu docelowego.

*d-port-mask*: W przypadku ustawienia na protokół TCP lub UDP należy wyznaczyć maskę portu docelowego, używając 4 cyfr szesnastkowych.

*tcpflag*: W przypadku ustawienia na protokół TCP należy wyznaczyć wartość flagi, używając liczb binarnych lub \* (np. 01\*010\*). Ustawienie domyślne to \*, oznaczające, że flaga nie zostanie dopasowana.

Dostępne flagi to URG (Urgent flag), ACK (Acknowledge Flag), PSH (Push Flag), RST (Reset Flag), SYN (Synchronize Flag) i FIN (Finish Flag).

*time-range-name*: Nazwa zakresu czasu. Ustawienie domyślne to No Limit.

Krok 4     **end**

Wróć do trybu privileged EXEC.

Krok 5     **copy running-config startup-config**

Zapisz ustawienia w pliku konfiguracyjnym.

Poniższy przykład prezentuje tworzenie Combined ACL 1100 i konfigurację Rule 1 (reguły 1) odrzucania pakietów o źródłowym adresie IP 192.168.3.100 in VLAN 2:

**Switch#configure**

**Switch(config)#access-list create 1100**

**Switch(config)#access-list combined 1100 logging disable rule 1 permit vid 2 sip 192.168.3.100 sip-mask 255.255.255.255**

**Switch(config)#show access-list 2600**

Combined access list 2600 name: ACL\_2600

rule 1 permit logging disable vid 2 sip 192.168.3.100 sip-mask 255.255.255.255

**Switch(config)#end**

**Switch#copy running-config startup-config**

## ■ IPv6 ACL

Krok 1     **configure**

Uruchom tryb konfiguracji globalnej.



---

**Krok 2** **access-list create *acl-id* [name *acl-name*]**

Utwórz IPv6 dla ACL.

*acl-id*: Wprowadź ID listy ACL. ID mieści się w zakresie od 1500 do 1999.

*acl-name*: Wprowadź nazwę, aby umożliwić identyfikację ACL.

---

**Krok 3** **access-list ipv6 *acl-id-or-name* rule {auto | *rule-id* } {deny | permit} logging {enable | disable} [class *class-value*] [flow-label *flow-label-value*] [sip *source-ip-address* sip-mask *source-ip-mask*] [dip *destination-ip-address* dip-mask *destination-ip-mask*] [s-port *source-port-number*] [d-port *destination-port-number*] [tseg *time-range-name*]**

Dodaj reguły do ACL.

*acl-id-or-name*: Wprowadź ID lub nazwę ACL, do której chcesz dodać regułę.

*auto*: ID reguły będzie przypisany automatycznie. Odstęp czasu między przypisywaniem regułom ID to 5 sekund.

*rule-id*: Przypisz ID do reguły.

*deny* | *permit*: Określ, jakie działanie ma być wykonane względem pakietów dopasowanych do reguły. Domyślnie ustawiona jest opcja Permit. W przypadku wybrania opcji Deny pakiety będą odrzucane; w przypadku wybrania funkcji Permit pakiety będą przekazywane.

**logging** {enable | disable}: Włącz lub wyłącz funkcję Logging dla reguły ACL. W przypadku włączenia funkcji, dopasowane reguły będą rejestrowane raz na 5 minut. Jeżeli włączysz funkcję ACL Counter trap, po zmianie czasu dopasowania wygenerowana zostanie powiązana pułapka (ang. trap).

*class-value*: Wyznacz wartość klasy do dopasowania, w zakresie od 0 do 63.

*flow-label-value*: Wyznacz wartość Flow Label do dopasowania

*source-ip-address*: Wpisz źródłowy adres IP. Wpisz źródłowy adres IPv6 do dopasowania. Sprawdzony zostanie każdy typ adresu IPv6. Możesz wprowadzić pełny 128-bitowy adres IPv6, ale znaczenie będą miały tylko pierwsze 64 bity.

*source-ip-mask*: Wprowadź maskę źródłowego adresu IP. Maska jest wymagana, jeżeli podany został źródłowy adres IPv6. Wprowadź maskę w pełnym formacie (np. ffff:ffff:0000:ffff). Maska wyznacza, które bity w źródłowym adresie IPv6 będą dopasowywane do reguły.

*destination-ip-address*: Wpisz docelowy adres IP. Wpisz źródłowy adres IPv6 do dopasowania. Sprawdzony zostanie każdy typ adresu IPv6. Możesz wprowadzić pełny 128-bitowy adres IPv6, ale znaczenie będą miały tylko pierwsze 64 bity.

*destination-ip-mask*: Wprowadź maskę docelowego adresu IP. Maska jest wymagana, jeżeli podany został źródłowy adres IPv6. Wprowadź maskę w pełnym formacie (np. ffff:ffff:0000:ffff). Maska wyznacza, które bity w źródłowym adresie IPv6 będą dopasowywane do reguły.

*source-port-number*: Wprowadź port źródłowy TCP/UDP, jeżeli wybrany został protokół TCP/UDP.

*destination-port-number*: Wprowadź port docelowy TCP/UDP, jeżeli wybrany został protokół TCP/UDP.

---

**Krok 4** **end**

Powróć do trybu privileged EXEC.

---

---

Krok 5     **copy running-config startup-config**  
Zapisz ustawienia w pliku konfiguracyjnym.

---

Poniższy przykład prezentuje tworzenie listy ACL IPv6 1600 i konfigurację Rule 1 do odrzucania pakietów o adresie źródłowym IPv6 CDCD:910A:2222:5498:8475:1111:3900:2020:

**Switch#configure**

**Switch(config)#access-list create 1600**

**Switch(config)#access-list ipv6 1600 rule 1 deny logging disable sip  
CDCD:910A:2222:5498:8475:1111:3900:2020 sip-mask ffff:ffff:ffff:ffff**

**Switch(config)#show access-list 1600**

IPv6 access list 1600 name: ACL\_1600

rule 1 deny logging disable sip cdc:910a:2222:5498:8475:1111:3900:2020 sip-mask ffff:ff  
ff:ffff:ffff

**Switch(config)#end**

**Switch#copy running-config startup-config**

### Zmiana kolejności reguł

Możesz zmienić kolejność reguł, podając ID pierwszej reguły (Start Rule ID) i wartość krokową.

---

Krok 1     **configure**  
Uruchom tryb konfiguracji globalnej.

---

Krok 2     **access-list resequence *acl-id-or-name* start *start-rule-id* Krok *rule-id-Krok-value***  
Zmień kolejność reguł na wybranej ACL.  
*acl-id-or-name*: Wpisz ID lub nazwę ACL.  
*start-rule-id*: Wpisz pierwszy ID reguły.  
*rule-id-Krok-value*: Wprowadź wartość krokową.

---

Krok 3     **end**  
Wróć do trybu privileged EXEC.

---

Krok 4     **copy running-config startup-config**  
Zapisz ustawienia w pliku konfiguracyjnym.

---

Poniższy przykład prezentuje zmianę kolejności reguł ACL MAC 100: ustawianie pierwszego ID reguły na 1 i ustawianie wartości krokowej na 10:

**Switch#configure**

**Switch(config)#access-list resequence 100 start 1 step 10**

```
Switch(config)#show access-list 100
```

```
MAC access list 100 name: "ACL_100"
```

```
rule 1 deny logging disable smac aa:bb:cc:dd:ee:ff smask ff:ff:ff:ff:ff:ff
```

```
rule 11 permit logging disable vid 18
```

```
rule 21 permit logging disable dmac aa:cc:ee:ff:dd:33 dmask ff:ff:ff:ff:ff:ff
```

```
Switch(config)#end
```

```
Switch#copy running-config startup-config
```

### 2.2.3 Strategie konfiguracji

Strategie konfiguracji umożliwiają dalsze przetwarzanie dopasowanych pakietów poprzez takie działania jak mirroring, ograniczanie prędkości, przekierowywanie lub zmiana priorytetu.

Wykonaj poniższe kroki, aby skonfigurować strategie dla reguły ACL.

---

|        |                                                                                                                                                                                                                |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Krok 1 | <b>configure</b><br>Uruchom tryb konfiguracji globalnej.                                                                                                                                                       |
| Krok 2 | <b>access-list action <i>acl-id-or-name</i> rule <i>rule-id</i></b><br>Skonfiguruj strategie dla reguły ACL.<br><i>acl-id-or-name</i> : Wprowadź ID lub nazwę ACL.<br><i>rule-id</i> : Wprowadź ID reguły ACL. |

---

---

Krok 3     **redirect interface { fastEthernet *port* | gigabitEthernet *port* | ten-gigabitEthernet *port* }**  
(Opcjonalnie) Ustaw strategię na przekierowywanie dopasowanych pakietów do wybranego portu.

*port*: Port docelowy, do którego przekierowywane będą pakiety. Ustawienie domyślne to All (wszystkie).

**s-mirror interface { fastEthernet *port* | gigabitEthernet *port* | ten-gigabitEthernet *port* }**

(Opcjonalnie) Ustaw strategię na kopiowanie (mirroring) dopasowanych pakietów na wybranym porcie.

*port*: Port docelowy, na którym kopiowane będą pakiety.

**s-condition rate *rate* burst *burst-size* osd { none | discard }**

(Opcjonalnie) Ustaw strategię na monitorowanie prędkości dopasowanych pakietów.

*rate*: Ustaw prędkość między 1 a 1000000 kb/s.

*burst-size*: Określ maks. dopuszczalną liczbę bajtów na sekundę, od 1 do 128.

**osd**: Wpisz „none” (brak) lub „discard” (odrzucaj) jako działanie, które ma być podejmowane względem pakietów, których prędkość przekracza granicę wyznaczonego zakresu. Ustawienie domyślne to None.

**qos-remark [dscp *dscp*] [ priority *pri* ] [ dot1p *pri* ]**

(Opcjonalnie) Wyznacz strategię oznaczania priorytetu dopasowanych pakietów.

*dscp*: Wyznacz region DSCP dla pakietów danych. Wartość wynosi od 0 do 63.

**priority *pri***: Wyznacz priorytet lokalny dla pakietów danych. Wartość wynosi od 0 do 7.

**dot1p *pri***: Wyznacz priorytet 802.1p dla pakietów danych. Wartość wynosi od 0 do 7.

---

Krok 4     **end**  
Wróć do trybu privileged EXEC.

---

Krok 5     **copy running-config startup-config**  
Zapisz ustawienia w pliku konfiguracyjnym.

---

Przekierowywanie dopasowanych pakietów do portu 1/0/4 w regule 1 ACL MAC 10:

**Switch#configure**

**Switch(config)#access-list action 10 rule 1**

**Switch(config-action)#redirect interface gigabitEthernet 1/0/4**

```
Switch(config-action)#exit
```

```
Switch(config)#show access-list 10
```

```
MAC access list 10 name: ACL_10
```

```
rule 5 permit logging disable action redirect Gi1/0/4
```

```
Switch(config)#end
```

```
Switch#copy running-config startup-config
```

## 2.2.4 Konfiguracja wiązania ACL

Możesz powiązać ACL z portem lub siecią VLAN. Pakiety odebrane na porcie lub w sieci VLAN będą dopasowane i przetworzone zgodnie z regułami ACL. ACL zacznie działać dopiero po powiązaniu jej z portem lub siecią VLAN.

### Uwaga:

- Różne typy ACL nie mogą być powiązane z tym samym portem lub siecią VLAN.
- Liczne ACL tego samego typu mogą być powiązane z tym samym portem lub siecią VLAN. Przełącznik dopasowuje odebrane pakiety wykorzystując listy ACL, zgodnie z kolejnością. Im wcześniej ACL została powiązana, tym większy ma priorytet.

Wykonaj poniższe kroki, aby powiązać ACL z portem lub VLAN:

|        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Krok 1 | <b>configure</b><br>Uruchom tryb konfiguracji globalnej.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Krok 2 | <b>access-list bind <i>acl-id-or-name</i> interface { [ <b>vlan</b> <i>vlan-list</i> ]   [ <b>fastEthernet</b> <i>port-list</i> ]   [ <b>gigabitEthernet</b> <i>port-list</i> ]   [ <b>ten-gigabitEthernet</b> <i>port-list</i> ] }</b><br>Powiąż ACL z portem lub VLAN.<br><i>acl-id-or-name</i> : Wprowadź ID lub nazwę ACL, do której chcesz dodać regułę.<br><i>vlan-list</i> : Wyznacz ID lub listę ID sieci VLAN, którą(-e) chcesz powiązać z ACL. Wartość powinna wynosić między 1 a 4094, np. 2-3,5.<br><i>port-list</i> : Wyznacz numer lub listę portu Ethernet, który chcesz powiązać z ACL. |
| Krok 3 | <b>show access-list bind</b><br>Sprawdź ustawienia wiązania ACL.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Krok 4 | <b>end</b><br>Wróć do trybu privileged EXEC.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Krok 5 | <b>copy running-config startup-config</b><br>Zapisz ustawienia w pliku konfiguracyjnym.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |

Poniższy przykład prezentuje wiązanie ACL 1 z portem 3 i VLAN 4:

```
Switch#configure
```

```
Switch(config)#access-list bind 1 interface vlan 4 gigabitEthernet 1/0/3
```

```
Switch(config)#show access-list bind
```

| ACL ID | ACL NAME | Interface/VID | Direction | Type |
|--------|----------|---------------|-----------|------|
| -----  | -----    | -----         | -----     | ---- |
| 1      | ACL_1    | Gi1/0/3       | Ingress   | Port |
| 1      | ACL_1    | 4             | Ingress   | VLAN |

```
Switch(config)#end
```

```
Switch#copy running-config startup-config
```

## 2.2.5 Wyświetlanie liczby dopasowanych pakietów ACL

Za pomocą poniższego polecenia możesz wyświetlić liczbę dopasowanych pakietów każdej ACL, w trybie użytkownika uprzywilejowanego i w każdym innym trybie:

---

```
show access-list acl-id-or-name counter
```

Wyświetl liczbę dopasowanych pakietów wybranej ACL.

*acl-id-or-name*: Podaj ID lub nazwę ACL do wyświetlenia.

---

# 3 Przykład konfiguracji ACL

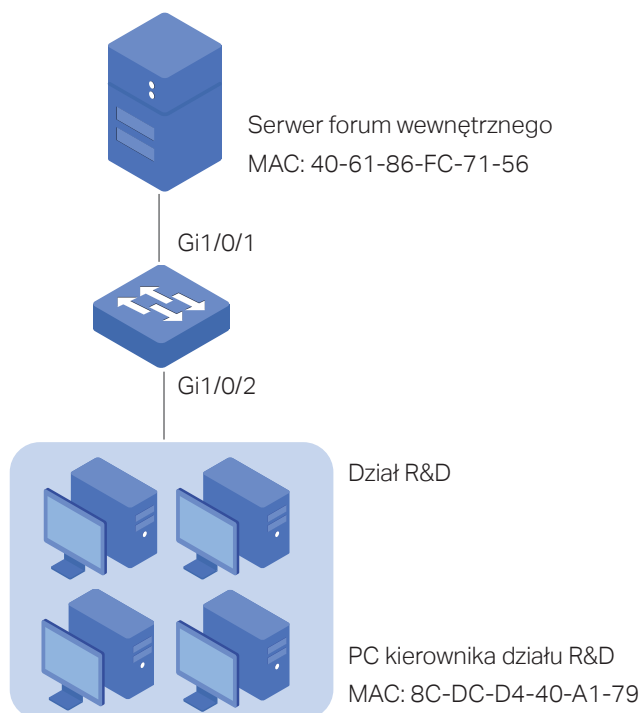
## 3.1 Przykład konfiguracji MAC ACL

### 3.1.1 Wymagania sieciowe

Firma nie zezwala na dostęp pracowników działu R&D do forum wewnętrznego w godzinach ich pracy. Natomiast kierownik działu R&D ma nieograniczony dostęp do forum wewnętrznego.

Jak pokazano poniżej, serwer forum wewnętrznego podłączony jest do przełącznika poprzez port 1/0/1, a komputery działu R&D podłączone są poprzez port 1/0/2.

Rys. 3-1 Topologia sieci



### 3.1.2 Schemat konfiguracji

Aby możliwe było spełnienie powyższego wymogu, należy skonfigurować filtrowanie pakietów poprzez utworzenie MAC ACL i konfigurację stosowanych reguł.

- Konfiguracja zakresu czasu

Utwórz wpis zakresu czasu, obejmujący godziny pracy w firmie. Zastosuj ten wpis do reguły ACL, która blokuje dostęp do serwera forum wewnętrznego.

### ■ Konfiguracja ACL

Utwórz MAC ACL i skonfiguruj następujące reguły:

- Skonfiguruj regułę zezwoleń tak, aby możliwe było dopasowywanie pakietów o źródłowym adresie MAC 8C-DC-D4-40-A1-79 i docelowym adresie MAC 40-61-86-FC-71-56. Ta reguła pozwala kierownikowi działu R&D na nieograniczony dostęp do forum wewnętrznego.
- Skonfiguruj regułę odrzucania, aby możliwe było dopasowywanie pakietów o docelowym adresie MAC 40-61-86-FC-71-56 i zastosuj do niej wpis zakresu czasu dla godzin pracy.
- Skonfiguruj regułę zezwoleń, aby możliwe było dopasowywanie wszystkich pozostałych pakietów, które nie pasują do powyższych reguł.

### ■ Konfiguracja wiązania

Powiąz MAC ACL z portem 1/0/2 tak, aby reguły ACL miały zastosowanie dla komputerów z działu R&D, które nie mogą mieć dostępu do forum wewnętrznego firmy w godzinach pracy.

W poniższych podrozdziałach opisano dwa sposoby przeprowadzenia procedury konfiguracji: przez GUI oraz przez CLI.

## 3.1.3 Przez GUI

- 1) Wybierz z menu **SYSTEM > Time Range > Time Range Config** i kliknij **+ Add**, aby wyświetlić poniższą stronę. Utwórz wpis zakresu czasu o nazwie **Work\_time**.

Rys. 3-2 Konfiguracja zakresu czasu

Time-Range Config

Name:  (1-16 characters)

Holiday:  Exclude  Include

Period Time Config

**+ Add** **- Delete**

| <input type="checkbox"/>  | Index | Date | Day | Time | Operation |
|---------------------------|-------|------|-----|------|-----------|
| No entries in this table. |       |      |     |      |           |
| Total: 0                  |       |      |     |      |           |

**Discard** **Create**

- 2) W sekcji **Period Time Config** kliknij **+ Add**, aby wyświetlić poniższe okno. Dodaj godziny pracy firmy w **Period Time** i kliknij **Save**.



Rys. 3-3 Dodawanie czasu pracy

### Period Time Config

**Date**

---

**From**

Month:

Day:

Year:

**To**

Month:

Day:

Year:

**Time**

---

**From:**  (Format: HH:MM)

**To:**  (Format: HH:MM)

**Day of Week**

Mon
  Tue
  Wed
  Thu
  Fri
  Sat
  Sun

- 3) Po dodaniu czasu pracy, kliknij **Create**, aby zapisać ten wpis.

Rys. 3-4 Tworzenie zakresu czasu

### Time-Range Config

**Name:**  (1-16 characters)

**Holiday:**  Exclude  Include

**Period Time Config**

|                          | Index | Date                              | Day                     | Time          | Operation                                                          |
|--------------------------|-------|-----------------------------------|-------------------------|---------------|--------------------------------------------------------------------|
| <input type="checkbox"/> | 0     | January 1, 2018 - January 1, 2019 | Mon, Tue, Wed, Thu, Fri | 08:00 - 18:00 | <input type="button" value="✎"/> <input type="button" value="🗑️"/> |
| Total: 0                 |       |                                   |                         |               |                                                                    |

- 4) Wybierz z menu **SECURITY > ACL > ACL Config** i kliknij **+ Add**, aby wyświetlić poniższą stronę. Następnie utwórz MAC ACL dla działu marketingu.

Rys. 3-5 Tworzenie MAC ACL

### ACL

ACL Type: MAC ACL ▼

ACL ID:  (0-499)

ACL Name:  (Optional)

Cancel
Create

- 5) Kliknij **Edit ACL** w kolumnie Operation.

Rys. 3-6 Edytowanie MAC ACL

ACL Config + Add - Delete

|                          | ACL Type | ACL ID | ACL Name      | Rules | Operation                                                              |
|--------------------------|----------|--------|---------------|-------|------------------------------------------------------------------------|
| <input type="checkbox"/> | MAC ACL  | 100    | Forum_Control | None  | <span style="border: 1px solid #a020f0; padding: 2px;">Edit ACL</span> |
| Total: 1                 |          |        |               |       |                                                                        |

- 6) Na stronie konfiguracji ACL kliknij + Add.

Rys. 3-7 Edytowanie MAC ACL

ACL Details

ACL Type: MAC ACL

ACL ID: 100

ACL Name: Forum\_Control

ACL Rules Config

↕ Resequence + Add - Delete ↻ Refresh

|                           | Index | Rule ID | S-MAC | D-MAC | Action | Total Matched Counter | Operation |
|---------------------------|-------|---------|-------|-------|--------|-----------------------|-----------|
| No entries in this table. |       |         |       |       |        |                       |           |
| Total: 0                  |       |         |       |       |        |                       |           |

- 7) Skonfiguruj regułę 5, aby zezwolić na przyjmowanie pakietów o źródłowym adresie MAC 8C-DC-D4-40-A1-79 i docelowym adresie MAC 40-61-86-FC-71-56.

Rys. 3-8 Konfiguracja reguły 5

MAC ACL Rule

ACL ID: 100

ACL Name: Forum\_Control

Rule ID:   Auto Assign

Operation:

S-MAC:  (Format: FF-FF-FF-FF-FF-FF)

Mask:  (Format: FF-FF-FF-FF-FF-FF)

D-MAC:  (Format: FF-FF-FF-FF-FF-FF)

Mask:  (Format: FF-FF-FF-FF-FF-FF)

VLAN ID:  (1-4094)

EtherType:  (4-hex number)

User Priority:

Time Range:  (Optional)

Logging:

Policy

Mirroring

Redirect

Rate Limit

QoS Remark

- 8) W ten sam sposób skonfiguruj regułę 15, aby pakiety o adresie docelowym MAC 40-61-86-FC-71-56 były odrzucane i zastosuj dla tej reguły wpis zakresu czasu dla godzin pracy.

Rys. 3-9 Konfiguracja reguły 15

MAC ACL Rule

ACL ID: 100  
ACL Name: Forum\_Control

Rule ID: 15  Auto Assign  
Operation: Deny

S-MAC: (Format: FF-FF-FF-FF-FF-FF)  
Mask: (Format: FF-FF-FF-FF-FF-FF)

D-MAC: 40-61-86-FC-71-56 (Format: FF-FF-FF-FF-FF-FF)  
Mask: FF-FF-FF-FF-FF-FF (Format: FF-FF-FF-FF-FF-FF)

VLAN ID: (1-4094)  
 EtherType: (4-hex number)

User Priority: Default

Time Range: Work\_time (Optional)

Logging: Disable

Policy

Mirroring  
 Redirect  
 Rate Limit  
 QoS Remark

- 9) Skonfiguruj regułę 25, aby zezwolić na przyjmowanie pakietów, które nie pasują do żadnej z powyższych reguł.

Rys. 3-10 Konfiguracja reguły 25

MAC ACL Rule

ACL ID: 100  
 ACL Name: Forum\_Control

Rule ID: 25  Auto Assign  
 Operation: Permit

S-MAC: (Format: FF-FF-FF-FF-FF-FF)  
 Mask: (Format: FF-FF-FF-FF-FF-FF)

D-MAC: (Format: FF-FF-FF-FF-FF-FF)  
 Mask: (Format: FF-FF-FF-FF-FF-FF)

VLAN ID: (1-4094)  
 EtherType: (4-hex number)

User Priority: Default  
 Time Range: (Optional)  
 Logging: Disable

Policy

Mirroring  
 Redirect  
 Rate Limit  
 QoS Remark

Discard Apply

- 10) Wybierz z menu **SECURITY > ACL > ACL Binding** i kliknij **+** Add, aby wyświetlić poniższą stronę. Powiąż ACL 100 z portem 1/0/2, aby konfiguracja była obowiązująca.

Rys. 3-11 Wiązanie ACL z portem 1/0/2

Port Binding Config


ACL:  ID  Name  
 100  
 Direction: Ingress  
 Port: 1/0/2 (Format: 1/0/1, input or choose below)

UNIT1

Select All

1 2 3 4 5 6 7 8 9 10

Cancel Create

- 11) Kliknij , aby zapisać ustawienia.

### 3.1.4 Przez CLI

- 1) Utwórz wpis zakresu czasu.

```
Switch#config
```

```
Switch(config)#time-range Work_time
```

```
Switch(config-time-range)#holiday include
```

```
Switch(config-time-range)#absolute from 01/01/2018 to 01/01/2019
```

```
Switch(config-time-range)#periodic start 08:00 end 18:00 day-of-the-week 1,2,3,4,5
```

```
Switch(config-time-range)#end
```

```
Switch#copy running-config startup-config
```

- 2) Utwórz MAC ACL.

```
Switch#configure
```

```
Switch(config)#access-list create 100 name Forum_Control
```

- 3) Skonfiguruj regułę 5, aby przyjmować pakiety o źródłowym adresie MAC 8C-DC-D4-40-A1-79 i docelowym adresie MAC 40-61-86-FC-71-56.

```
Switch(config)#access-list mac 100 rule 5 permit logging disable smac 8C:DC:D4:40:A1:79 smask FF: FF: FF: FF: FF: FF dmac 40:61:86:FC:71:56 dmask FF: FF: FF: FF: FF: FF
```

- 4) Skonfiguruj regułę 15, aby odrzucać pakiety o adresie docelowym MAC 40-61-86-FC-71-56.

```
Switch(config)#access-list mac 100 rule 15 deny logging disable dmac 40:61:86:FC:71:56 dmask FF: FF: FF: FF: FF: FF tseg Work_time
```

- 5) Skonfiguruj regułę 25, aby przyjmować wszystkie pakiety. Ta reguła sprawia, że ruch skierowany w stronę innych zasobów sieci nie będzie blokowany przez przełącznik.

```
Switch(config)#access-list mac 100 rule 25 permit logging disable
```

- 6) Powiąż ACL100 z portem 1/0/2.

```
Switch(config)#access-list bind 100 interface gigabitEthernet 1/0/2
```

```
Switch(config)#end
```

```
Switch#copy running-config startup-config
```

### Sprawdzanie konfiguracji

Sprawdzanie konfiguracji MAC ACL 100:

```
Switch#show access-list 100
```

```
MAC access list 100 name: "Forum_Control"
```

```
rule 5 permit logging disable smac 8c:dc:d4:40:a1:79 smask ff:ff:ff:ff:ff:ff dmac
40:61:86:fc:71:56 dmask ff:ff:ff:ff:ff:ff
```

```
rule 15 deny logging disable dmac 40:61:86:fc:71:56 dmask ff:ff:ff:ff:ff:ff tseg "Work_time"
```

```
rule 25 permit logging disable
```

```
Switch#show access-list bind
```

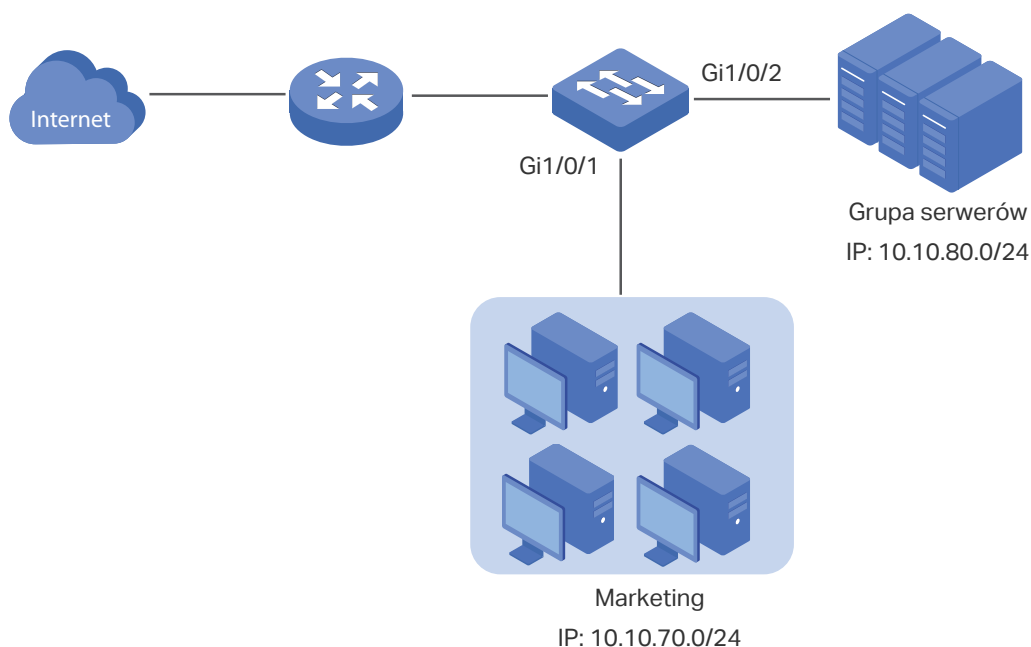
| ACL ID | ACL NAME      | Interface/VID | Direction | Type |
|--------|---------------|---------------|-----------|------|
| -----  | -----         | -----         | -----     | ---- |
| 100    | Forum_Control | Gi1/0/2       | Ingress   | Port |

## 3.2 Przykład konfiguracji IP ACL

### 3.2.1 Wymagania sieciowe

Jak pokazano poniżej, wewnętrzna grupa serwerów firmy może zapewniać różne typy usług. Komputery w dziale marketingu są podłączone do przełącznika poprzez port 1/0/1, a wewnętrzna grupa serwerów poprzez port 1/0/2.

Rys. 3-12 Topologia sieci



Oczekuje się, że:

- dział marketingu może mieć dostęp do wewnętrznej grupy serwerów tylko w sieci intranet;

- dział marketingu może odwiedzać w Internecie tylko witryny http i https.

### 3.2.2 Schemat konfiguracji

Aby spełnić powyższe warunki, należy skonfigurować filtrowanie pakietów poprzez utworzenie IP ACL i konfigurację odpowiednich reguł.

- **Konfiguracja ACL**

Utwórz IP ACL i skonfiguruj poniższe reguły:

- Skonfiguruj regułę zezwoleń tak, aby możliwe było dopasowywanie pakietów o źródłowym adresie IP 10.10.70.0/24 i docelowym adresie IP 10.10.80.0/24. Ta reguła umożliwia działowi marketingu dostęp do wewnętrznych serwerów sieci z poziomu intranet.
- Skonfiguruj cztery reguły zezwoleń, aby możliwe było dopasowywanie pakietów o źródłowym adresie IP 10.10.70.0/24 i docelowych portach TCP 80, TCP 443 oraz TCP/UDP 53. Ta reguła umożliwia działowi marketingu dostęp do witryn http i https w Internecie.
- Skonfiguruj regułę odrzucania, aby możliwe było dopasowywanie pakietów o źródłowym adresie IP 10.10.70.0/24. Ta reguła blokuje inne usługi sieciowe.

Przełącznik po kolei dopasowuje pakiety do reguł zaczynając od reguł 1. Jeśli pakiet pasuje do reguły, przełącznik przerywa proces dopasowywania i inicjuje działanie określone w regule.

- **Konfiguracja wiązania**

Powiąz IP ACL z portem 1/0/1 tak, aby reguły ACL miały zastosowanie tylko dla działu marketingu.

W poniższych podrozdziałach opisano dwa sposoby przeprowadzenia procedury konfiguracji: przez GUI oraz przez CLI.

### 3.2.3 Przez GUI

- 1) Wybierz z menu **SECURITY > ACL > ACL Config** i kliknij  Add, aby wyświetlić poniższą stronę. Następnie utwórz IP ACL dla działu marketingu.



Rys. 3-13 Tworzenie IP ACL

ACL

ACL Type: IP ACL

ACL ID: 500 (500-999)

ACL Name: marketing (Optional)

Cancel Create

- 2) Kliknij **Edit ACL** w kolumnie Operation.

Rys. 3-14 Edytowanie IP ACL

ACL Config

+ Add - Delete

| <input type="checkbox"/> | ACL Type | ACL ID | ACL Name  | Rules | Operation |
|--------------------------|----------|--------|-----------|-------|-----------|
| <input type="checkbox"/> | IP ACL   | 500    | marketing | None  | Edit ACL  |

Total: 1

- 3) Na stronie konfiguracji ACL kliknij **+ Add**.

Rys. 3-15 Edytowanie IP AC

ACL Details

ACL Type: IP ACL

ACL ID: 500

ACL Name: marketing

ACL Rules Table

1 Resequence + Add - Delete Refresh

| <input type="checkbox"/>  | ID | Rule ID | S-IP | D-IP | IP Protocol | Action | Total Matched Counter | Operation |
|---------------------------|----|---------|------|------|-------------|--------|-----------------------|-----------|
| No Entries in this table. |    |         |      |      |             |        |                       |           |

Total: 0

- 4) Skonfiguruj regułę 1, aby zezwolić na przyjmowanie pakietów o źródłowym adresie IP 10.10.70.0/24 i docelowym adresie IP 10.10.80.0/24.

Rys. 3-16 Konfiguracja reguły 1

IP ACL Rule

ACL ID: 500

ACL Name: marketing

Rule ID:   Auto Assign

Operation:

Fragment:  Enable

S-IP:  (Format: 192.168.0.1)

Mask:  (Format: 255.255.255.0)

D-IP:  (Format: 192.168.0.1)

Mask:  (Format: 255.255.255.0)

IP Protocol:

DSCP:

IP ToS:  (Optional, 0-15)

IP Pre:  (Optional, 0-7)

- 5) W ten sam sposób skonfiguruj regułę 2 i regułę 3, aby zezwolić na przyjmowanie pakietów o źródłowym adresie IP 10.10.70.0 oraz docelowych portach TCP 80 (port usługi http) i TCP 443 (port usługi https).

Rys. 3-17 Konfiguracja reguły 2

IP ACL Rule

ACL ID: 500

ACL Name: marketing

Rule ID:   Auto Assign

Operation:

Fragment:  Enable

S-IP:  (Format: 192.168.0.1)

Mask:  (Format: 255.255.255.0)

D-IP:  (Format: 192.168.0.1)

Mask:  (Format: 255.255.255.0)

IP Protocol:

URG:  ACK:  PSH:

RST:  SYN:  FIN:

S-Port

Value:  (0-65535)

Mask:  (0000-ffff)

D-Port

Value:  (0-65535)

Mask:  (0000-ffff)

DSCP:

IP ToS:  (Optional, 0-15)

Rys. 3-18 Konfiguracja reguły 3

IP ACL Rule

ACL ID: 500

ACL Name: marketing

Rule ID:   Auto Assign

Operation:

Fragment:  Enable

S-IP:  (Format: 192.168.0.1)

Mask:  (Format: 255.255.255.0)

D-IP:  (Format: 192.168.0.1)

Mask:  (Format: 255.255.255.0)

IP Protocol:

URG:  ACK:  PSH:

RST:  SYN:  FIN:

S-Port

Value:  (0-65535)

Mask:  (0000-ffff)

D-Port

Value:  (0-65535)

Mask:  (0000-ffff)

DSCP:

IP ToS:  (Optional, 0-15)

- 6) W ten sam sposób skonfiguruj regułę 4 i regułę 5, aby przyjmować pakiety o źródłowym adresie IP 10.10.70.0 oraz docelowych portach TCP 53 lub UDP 53 (portu usługi DNS).

Rys. 3-19 Konfiguracja reguły 4

IP ACL Rule

ACL ID: 500

ACL Name: marketing

Rule ID: 4  Auto Assign

Operation: Permit

Fragment:  Enable

S-IP: 10.10.70.0 (Format: 192.168.0.1)

Mask: 255.255.255.0 (Format: 255.255.255.0)

D-IP: (Format: 192.168.0.1)

Mask: (Format: 255.255.255.0)

IP Protocol: TCP

URG: \* ACK: \* PSH: \*

RST: \* SYN: \* FIN: \*

S-Port

Value: (0-65535)

Mask: (0000-ffff)

DSCP: No Limit

IP ToS: (Optional, 0-15)

D-Port

Value: 53 (0-65535)

Mask: ffff (0000-ffff)

Rys. 3-20 Konfiguracja reguły 5

IP ACL Rule

ACL ID: 500

ACL Name: marketing

Rule ID:   Auto Assign

Operation:

Fragment:  Enable

S-IP:  (Format: 192.168.0.1)

Mask:  (Format: 255.255.255.0)

D-IP:  (Format: 192.168.0.1)

Mask:  (Format: 255.255.255.0)

IP Protocol:

S-Port

Value:  (0-65535)

Mask:  (0000-ffff)

D-Port

Value:  (0-65535)

Mask:  (0000-ffff)

DSCP:

IP ToS:  (Optional, 0-15)

- 7) W ten sam sposób skonfiguruj regułą 6, aby odrzucać pakiety o źródłowym adresie IP 10.10.70.0.

Rys. 3-21 Konfiguracja reguły 6

IP ACL Rule

ACL ID: 500

ACL Name: marketing

Rule ID:   Auto Assign

Operation:

Fragment:  Enable

S-IP:  (Format: 192.168.0.1)

Mask:  (Format: 255.255.255.0)

D-IP:  (Format: 192.168.0.1)

Mask:  (Format: 255.255.255.0)

IP Protocol:

DSCP:


IP ToS:  (Optional, 0-15)

IP Pre:  (Optional, 0-7)

- 8) Wybierz z menu **SECURITY > ACL > ACL Binding** i kliknij **+ Add**, aby wyświetlić poniższą stronę. Powiąż listę ACL działu marketingu z portem 1/0/1, aby zapewnić jej obowiązywanie.

Rys. 3-22 Wiązanie ACL z portem 1/0/1

The screenshot shows the 'Port Binding Config' window. At the top, there are radio buttons for 'ID' (selected) and 'Name'. Below that is a dropdown menu showing '500'. The 'Direction' is set to 'Ingress'. The 'Port' field contains '1/0/1' with a note '(Format: 1/0/1, input or choose below)'. Under the 'UNIT1' section, there are ten port icons numbered 1 to 10. Port 1 is highlighted with a red box. To the left of the ports is a 'Select All' checkbox. At the bottom right, there are 'Cancel' and 'Create' buttons, with the 'Create' button highlighted by a red box.

- 9) Kliknij  **Save**, aby zapisać ustawienia.

### 3.2.4 Przez CLI

- 1) Utwórz IP ACL.

```
Switch#configure
```

```
Switch(config)#access-list create 500 name marketing
```

- 2) Skonfiguruj regułę 1, aby przyjmować pakiety o źródłowym adresie IP 10.10.70.0/24 i docelowym adresie IP 10.10.80.0/24.

```
Switch(config)#access-list ip 500 rule 1 permit logging disable sip 10.10.70.0 sip-mask 255.255.255.0 dip 10.10.80.0 dmask 255.255.255.0
```

- 3) Skonfiguruj regułę 2 i regułę 3, aby przyjmować pakiety o źródłowym adresie 10.10.70.0/24 oraz docelowych portach TCP 80 (port usługi http) lub TCP 443 (port usługi https).

```
Switch(config)#access-list ip 500 rule 2 permit logging disable sip 10.10.70.0 sip-mask 255.255.255.0 protocol 6 d-port 80 d-port-mask ffff
```

```
Switch(config)#access-list ip 500 rule 3 permit logging disable sip 10.10.70.0 sip-mask 255.255.255.0 protocol 6 d-port 443 d-port-mask ffff
```

- 4) Skonfiguruj regułę 4 i regułę 5, aby przyjmować pakiety o źródłowym adresie IP 10.10.70.0/24 i docelowym porcie TCP53 lub UDP 53.

```
Switch(config)#access-list ip 500 rule 4 permit logging disable sip 10.10.70.0 sip-mask
255.255.255.0 protocol 6 d-port 53 d-port-mask ffff
```

```
Switch(config)#access-list ip 500 rule 5 permit logging disable sip 10.10.70.0 sip-mask
255.255.255.0 protocol 17 d-port 53 d-port-mask ffff
```

- 5) Skonfiguruj regułę 6, aby odrzucać pakiety o źródłowym adresie IP 10.10.70.0/24.

```
Switch(config)#access-list ip 500 rule 2 deny logging disable sip 10.10.70.0 sip-mask
255.255.255.0
```

- 6) Powiąż ACL500 z portem 1.

```
Switch(config)#access-list bind 500 interface gigabitEthernet 1/0/1
```

```
Switch(config)#end
```

```
Switch#copy running-config startup-config
```

## Sprawdzanie konfiguracji

Sprawdzanie konfiguracji IP ACL 500:

```
Switch#show access-list 500
```

```
rule 1 permit logging disable sip 10.10.70.0 smask 255.255.255.0 dip 10.10.80.0 dmask
255.255.255.0
```

```
rule 2 permit logging disable sip 10.10.70.0 smask 255.255.255.0 protocol 6 d-port 80
```

```
rule 3 permit logging disable sip 10.10.70.0 smask 255.255.255.0 protocol 6 d-port 443
```

```
rule 4 permit logging disable sip 10.10.70.0 smask 255.255.255.0 protocol 6 d-port 53
```

```
rule 5 permit logging disable sip 10.10.70.0 smask 255.255.255.0 protocol 17 d-port 53
```

```
rule 6 deny loggin disable sip 10.10.70.0 smask 255.255.255.0
```

```
Switch#show access-list bind
```

| ACL ID | ACL NAME  | Interface/VID | Direction | Type |
|--------|-----------|---------------|-----------|------|
| -----  | -----     | -----         | -----     | ---- |
| 500    | marketing | Gi1/0/1       | Ingress   | Port |

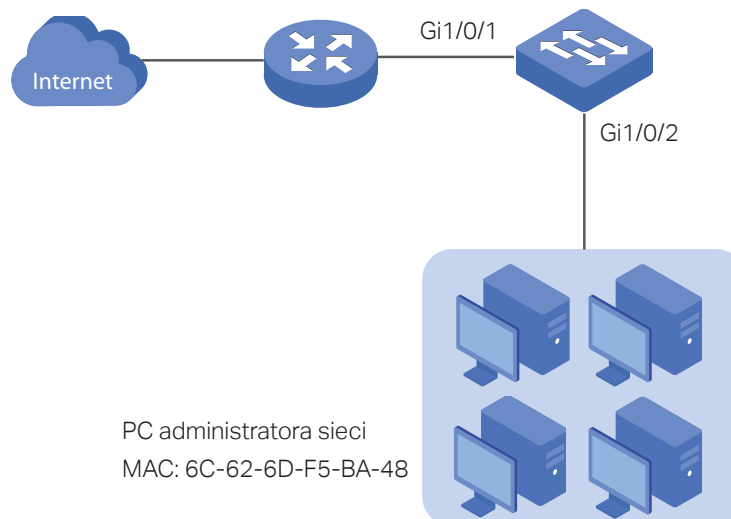


## 3.3 Przykład konfiguracji dla łączonej listy ACL

### 3.3.1 Wymagania sieciowe

Aby zwiększyć bezpieczeństwo sieci, firma chce, aby tylko administrator sieci mógł się logować do przełącznika poprzez połączenie Telnet. Komputery są podłączone do przełącznika poprzez port 1/0/2. Topologia sieci wygląda tak, jak poniżej.

Rys. 3-23 Topologia sieci



### 3.3.2 Schemat konfiguracji

Aby spełnić powyższy warunek, należy skonfigurować filtrowanie pakietów poprzez utworzenie połączonej listy ACL i konfigurację odpowiednich reguł.

- Konfiguracja ACL

Utwórz połączoną listę ACL i skonfiguruj poniższe reguły:

- Skonfiguruj regułę zezwoleń tak, aby możliwe było dopasowywanie pakietów o źródłowym adresie MAC 6C-62-6D-F5-BA-48 i docelowym porcie TCP 23. Ta reguła pozwala komputerowi administratora sieci na dostęp do przełącznika poprzez połączenie Telnet.
- Skonfiguruj regułę odrzucania, aby możliwe było dopasowywanie wszystkich pakietów oprócz pakietów o źródłowym adresie MAC 6C-62-6D-F5-BA-48 i docelowym porcie TCP 23. Ta reguła blokuje uzyskiwanie dostępu innych komputerów do przełącznika poprzez połączenie Telnet.
- Skonfiguruj regułę zezwoleń tak, aby możliwe było dopasowywanie wszystkich pakietów. Ta reguła pozwala innym urządzeniom na korzystanie z usług sieciowych oprócz usługi połączenia Telnet.

Przełącznik po kolei dopasowuje pakiety do reguł zaczynając od reguły 1. Jeśli pakiet pasuje do reguły, przełącznik przerywa proces dopasowywania i inicjuje działanie określone w regule.

#### ■ Konfiguracja wiązań

Powiąz połączoną listę ACL z portem 1/0/2 tak, aby reguły ACL miały zastosowanie dla komputera administratora sieci oraz urządzeń, które nie mogą korzystać z połączenia Telnet.

W poniższych podrozdziałach opisano dwa sposoby przeprowadzenia procedury konfiguracji: przez GUI oraz przez CLI.

### 3.3.3 Przez GUI

- 1) Wybierz z menu **SECURITY > ACL > ACL Config** i kliknij **+ Add**, aby wyświetlić poniższą stronę. Następnie utwórz połączoną listę ACL dla działu marketingu.

Rys. 3-24 Tworzenie połączonej listy ACL

- 2) Kliknij **Edit ACL** w kolumnie Operation.

Rys. 3-25 Edytowanie połączonej listy ACL

| ACL Config               |              |        |            |       |                 |
|--------------------------|--------------|--------|------------|-------|-----------------|
| <input type="checkbox"/> | ACL Type     | ACL ID | ACL Name   | Rules | Operation       |
| <input type="checkbox"/> | Combined ACL | 1000   | ACL_Telnet | None  | <b>Edit ACL</b> |
| Total: 1                 |              |        |            |       |                 |

- 3) Na stronie konfiguracyjnej ACL kliknij **+ Add**.

Rys. 3-25 Edytowanie połączonej listy ACL

ACL Details

ACL Type: Combined ACL  
ACL ID: 1000  
ACL Name: ACL\_Telnet

ACL Rules Config

🔄 Resequence + Add - Delete ↻ Refresh

| <input type="checkbox"/>  | Index Rule ID | S-MAC | D-MAC | S-IP | D-IP | VID | Action | Total Matched Counter | Operation |
|---------------------------|---------------|-------|-------|------|------|-----|--------|-----------------------|-----------|
| No entries in this table. |               |       |       |      |      |     |        |                       |           |
| Total: 0                  |               |       |       |      |      |     |        |                       |           |

- 4) Skonfiguruj regułę 5, aby przyjmować pakiety o źródłowym adresie MAC 6C-62-6D-F5-BA-48 i porcie docelowym TCP 23 (port usługi Telnet).

Rys. 3-26 Konfiguracja reguły 5

| Combined ACL Rule                              |                                               |
|------------------------------------------------|-----------------------------------------------|
| ACL ID:                                        | 1000                                          |
| ACL Name:                                      | ACL_Telnet                                    |
| Rule ID:                                       | 5                                             |
| Operation:                                     | Permit                                        |
| <input checked="" type="checkbox"/> S-MAC:     | 6C-62-6D-F5-BA-48 (Format: FF-FF-FF-FF-FF-FF) |
| Mask:                                          | FF-FF-FF-FF-FF-FF (Format: FF-FF-FF-FF-FF-FF) |
| <input type="checkbox"/> D-MAC:                | (Format: FF-FF-FF-FF-FF-FF)                   |
| Mask:                                          | (Format: FF-FF-FF-FF-FF-FF)                   |
| <input type="checkbox"/> VLAN ID:              | (1-4094)                                      |
| <input checked="" type="checkbox"/> EtherType: | 0800 (4-hex number)                           |
| <input type="checkbox"/> S-IP:                 | (Format: 192.168.0.1)                         |
| Mask:                                          | (Format: 255.255.255.0)                       |
| <input type="checkbox"/> D-IP:                 | (Format: 192.168.0.1)                         |
| Mask:                                          | (Format: 255.255.255.0)                       |
| IP Protocol:                                   | TCP                                           |
| URG:                                           | *                                             |
| ACK:                                           | *                                             |
| PSH:                                           | *                                             |
| RST:                                           | *                                             |
| SYN:                                           | *                                             |
| FIN:                                           | *                                             |
| <input type="checkbox"/> S-Port                |                                               |
| Value:                                         | (0-65535)                                     |
| Mask:                                          | (0000-FFFF)                                   |
| <input checked="" type="checkbox"/> D-Port     |                                               |
| Value:                                         | 23 (0-65535)                                  |
| Mask:                                          | FFFF (0000-FFFF)                              |
| DSCP:                                          | No Limit                                      |
| IP ToS:                                        | (Optional, 0-15)                              |

- 5) Skonfiguruj regułę 15, aby odrzucać wszystkie pakiety za wyjątkiem pakietów o adresie MAC 6C-62-6D-F5-BA-48 i porcie docelowym TCP 23 (port usługi Telnet).


Rys. 3-27 Konfiguracja reguły 15

| Combined ACL Rule                              |                                                  |
|------------------------------------------------|--------------------------------------------------|
| ACL ID:                                        | 1000                                             |
| ACL Name:                                      | ACL_Telnet                                       |
| Rule ID:                                       | 15                                               |
| Operation:                                     | Deny                                             |
| <input type="checkbox"/> S-MAC:                | <input type="text"/> (Format: FF-FF-FF-FF-FF-FF) |
| Mask:                                          | <input type="text"/> (Format: FF-FF-FF-FF-FF-FF) |
| <input type="checkbox"/> D-MAC:                | <input type="text"/> (Format: FF-FF-FF-FF-FF-FF) |
| Mask:                                          | <input type="text"/> (Format: FF-FF-FF-FF-FF-FF) |
| <input type="checkbox"/> VLAN ID:              | <input type="text"/> (1-4094)                    |
| <input checked="" type="checkbox"/> EtherType: | 0800 (4-hex number)                              |
| <input type="checkbox"/> S-IP:                 | <input type="text"/> (Format: 192.168.0.1)       |
| Mask:                                          | <input type="text"/> (Format: 255.255.255.0)     |
| <input type="checkbox"/> D-IP:                 | <input type="text"/> (Format: 192.168.0.1)       |
| Mask:                                          | <input type="text"/> (Format: 255.255.255.0)     |
| IP Protocol:                                   | TCP                                              |
| URG:                                           | *                                                |
| ACK:                                           | *                                                |
| PSH:                                           | *                                                |
| RST:                                           | *                                                |
| SYN:                                           | *                                                |
| FIN:                                           | *                                                |
| <input type="checkbox"/> S-Port                |                                                  |
| Value:                                         | <input type="text"/> (0-65535)                   |
| Mask:                                          | <input type="text"/> (0000-FFFF)                 |
| <input checked="" type="checkbox"/> D-Port     |                                                  |
| Value:                                         | 23 (0-65535)                                     |
| Mask:                                          | FFFF (0000-FFFF)                                 |
| DSCP:                                          | No Limit                                         |
| IP ToS:                                        | <input type="text"/> (Optional, 0-15)            |

- 6) W ten sam sposób skonfiguruj regułę 25, aby przyjmować wszystkie pakiety. Reguła zapewni wszystkim urządzeniom możliwość korzystania z innych usług sieciowych.

Rys. 3-28 Konfiguracja reguły 25

| Combined ACL Rule                   |                                                  |
|-------------------------------------|--------------------------------------------------|
| ACL ID:                             | 1000                                             |
| ACL Name:                           | ACL_Telnet                                       |
| Rule ID:                            | 25                                               |
| Operation:                          | Permit                                           |
| <input type="checkbox"/> S-MAC:     | <input type="text"/> (Format: FF-FF-FF-FF-FF-FF) |
| Mask:                               | <input type="text"/> (Format: FF-FF-FF-FF-FF-FF) |
| <input type="checkbox"/> D-MAC:     | <input type="text"/> (Format: FF-FF-FF-FF-FF-FF) |
| Mask:                               | <input type="text"/> (Format: FF-FF-FF-FF-FF-FF) |
| <input type="checkbox"/> VLAN ID:   | <input type="text"/> (1-4094)                    |
| <input type="checkbox"/> EtherType: | <input type="text"/> (4-hex number)              |
| <input type="checkbox"/> S-IP:      | <input type="text"/> (Format: 192.168.0.1)       |
| Mask:                               | <input type="text"/> (Format: 255.255.255.0)     |
| <input type="checkbox"/> D-IP:      | <input type="text"/> (Format: 192.168.0.1)       |
| Mask:                               | <input type="text"/> (Format: 255.255.255.0)     |
| IP Protocol:                        | No Limit                                         |
| DSCP:                               | No Limit                                         |
| IP ToS:                             | <input type="text"/> (Optional, 0-15)            |
| IP Pre:                             | <input type="text"/> (Optional, 0-7)             |
| User Priority:                      | Default                                          |
| Time Range:                         | <input type="text"/> (Optional)                  |
| Logging:                            | Disable                                          |

- 7) Wybierz z menu **SECURITY > ACL > ACL Binding** i kliknij  Add, aby wyświetlić poniższą stronę. Powiąż Policy ACL\_Telnet z portem 1/0/2, aby zapewnić jej działanie.

Rys. 3-29 Wiązanie ACL z portem 1/0/2

The screenshot shows the 'Port Binding Config' window. At the top, there are two radio buttons: 'ID' (selected) and 'Name'. Below them is a dropdown menu showing '1000'. The 'Direction' is set to 'Ingress' and the 'Port' is '1/0/2'. Under the 'UNIT1' section, there are ten port icons numbered 1 to 10. Port 2 is highlighted with a red box. At the bottom right, there are two buttons: 'Cancel' and 'Create' (highlighted with a red box).

- 8) Kliknij  Save, aby zapisać ustawienia.

### 3.3.4 Przez CLI

- 1) Utwórz łączoną listę ACL.

```
Switch#configure
```

```
Switch(config)#access-list create 1000 name ACL_Telnet
```

- 2) Skonfiguruj regułę 5, aby przyjmować pakiety o źródłowym adresie MAC 6C-62-6D-F5-BA-48 i porcie docelowym TCP 23 (port usługi Telnet).

```
Switch(config)#access-list combined 1000 rule 5 permit logging disable smac 6C:62:6D:F5:BA:48 smask FF:FF:FF:FF:FF:FF type 0800 protocol 6 d-port 23 d-port-mask FFFF
```

- 3) Skonfiguruj regułę 15, aby odrzucać wszystkie pakiety oprócz pakietów o źródłowym adresie MAC 6C-62-6D-F5-BA-48 i porcie docelowym TCP 23 (port usługi Telnet).

```
Switch(config)#access-list combined 1000 rule 15 deny logging disable type 0800 protocol 6 d-port 23 d-port-mask FFFF
```

- 4) Skonfiguruj regułę 25, aby przyjmować na wszystkie pakiety. Reguła zapewnia wszystkim urządzeniom możliwość korzystania z innych usług sieciowych.

```
Switch(config)#access-list combined 1000 rule 25 permit logging disable type 0800 protocol 6 d-port 23 d-port-mask FFFF
```

- 5) Powiąż ACL500 z portem 1/0/2.

```
Switch(config)#access-list bind 500 interface gigabitEthernet 1/0/2
```

```
Switch(config)#end
```

```
Switch#copy running-config startup-config
```

### Sprawdzanie konfiguracji

Sprawdzanie konfiguracji łączonej listy ACL 1000:

```
Switch#show access-list 1000
```

```
Combined access list 1000 name: "ACL_Telnet"
```

```
rule 5 permit logging disable smac 6c:62:6d:f5:ba:48 smask ff:ff:ff:ff:ff:ff type 0800 protocol 6 d-port 23
```

```
rule 15 deny logging disable type 0800 protocol 6 d-port 23
```

```
rule 25 permit logging disable
```

```
Switch#show access-list bind
```

| ACL ID | ACL NAME   | Interface/VID | Direction | Type |
|--------|------------|---------------|-----------|------|
| 1000   | ACL_Telnet | Gi1/0/2       | Ingress   | Port |



# Część 24

## Konfiguracja IMPB IPv4

### ROZDZIAŁY

1. IMPB IPv4
2. Konfiguracja wiązania IP-MAC
3. Konfiguracja funkcji ARP Detection
4. Konfiguracja funkcji IPv4 Source Guard
5. Przykłady konfiguracji

# 1 IMPB IPv4

## 1.1 Informacje ogólne

IMPB (IP-MAC-Port Binding) IPv4 służy do wiązania adresu IP, adresu MAC, VLAN ID i numeru połączonego portu określonego hosta. W oparciu o tablicę wiązań przełącznik może zapobiegać atakom ARP Cheating za pomocą funkcji ARP Detection i filtrować pakiety, które nie pasują do wpisów wiązań za pomocą funkcji IP Source Guard.

## 1.2 Obsługiwane funkcje

### Wiązanie IP-MAC

Funkcja ta służy do dodawania wpisów wiązania. Wpisy wiązania mogą być konfigurowane ręcznie lub wyuczane przez ARP scanning (skanowanie ARP) lub DHCP snooping. Funkcje ARP Detection i IPv4 Source Guard bazują na wpisach wiązania IP-MAC.

### ARP Detection

W rozbudowanej sieci wdrażanie protokołu ARP wiąże się z dużym zagrożeniem dla bezpieczeństwa samej sieci. Sieć często narażona jest na ataki opierające się na fałszowaniu danych (ARP cheating), np. imitowanie bramy sieciowej, podawanie błędnej bramy sieciowej czy błędnego terminala hosta oraz na ataki ARP flooding, polegające na wypełnianiu pamięci przełącznika błędnymi informacjami. Funkcja ARP Detection może ochronić sieć przed atakami ARP.

- Zapobieganie atakom ARP Cheating

Bazując na wpisach wiązania adresów IP i MAC, funkcję ARP Detection można skonfigurować tak, by wykrywała pakiety ARP i filtrowała te nielegalne w celu ochrony sieci przed atakami fałszowania ARP (ARP cheating).

- Zapobieganie atakom ARP Flooding

Aby zapobiec atakom ARP Flooding możesz ograniczyć prędkość odbierania przez port legalnych pakietów ARP.

### IPv4 Source Guard

Funkcja IPv4 Source Guard służy do filtrowania pakietów IPv4 w oparciu o tablicę wiązania IP-MAC. Przekazywane są jedynie pakiety zgodne z regułami wiązania.

# 2 Konfiguracja wiązania IP-MAC

Wpisy wiązania IP-MAC można dodawać trzema sposobami:

- poprzez wiązanie ręczne;
- poprzez ARP Scanning;
- poprzez DHCP Snooping.

Dodatkowo można wyświetlać, wyszukiwać i edytować wpisy na tablicy wiązania (Binding Table).

## 2.1 Przez GUI

### 2.1.1 Ręczne wiązanie wpisów

Możesz ręcznie powiązać adres IP, adres MAC, VLAN ID i numer portu pod warunkiem, że posiadasz szczegółowe dane hostów.

Wybierz z menu **SECURITY > IPv4 IMPB > IP-MAC Binding > Manual Binding** i kliknij **+ Add**, aby załadować poniższą stronę.

Rys. 2-1 Wiązanie ręczne

### IPv4-MAC Binding

Host Name:  (20 characters maximum)

IP Address:  (Format: 192.168.0.1)

MAC Address:  (Format: 00-00-00-00-00-01)

VLAN ID:  (1-4094)

Protect Type: None ▼

Port:  (Format: 1/0/1, input or choose below)

**UNIT1**

**LAGS**

Selected

Unselected

Not Available

Cancel
Apply

Wykonaj poniższe kroki, aby ręcznie utworzyć wiązanie IP-MAC:

- 1) Wprowadź następujące informacje, aby określić hosta.

|             |                                                    |
|-------------|----------------------------------------------------|
| Host Name   | Wprowadź nazwę, aby umożliwić identyfikację hosta. |
| IP Address  | Wprowadź adres IP.                                 |
| MAC Address | Wprowadź adres MAC.                                |
| VLAN ID     | Wprowadź VLAN ID.                                  |

- 2) Wybierz typ ochrony wpisu.

---

|              |                                                                                                                                                                                                                                                                                                                                                                                                                 |
|--------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Protect Type | Wybierz typ ochrony wpisu. Wpis będzie zastosowany do wybranej funkcji. Dostępne są następujące opcje:<br><br><b>None:</b> Wpis nie będzie zastosowany do żadnej funkcji.<br><br><b>ARP Detection:</b> Wpis zostanie zastosowany do funkcji ARP Detection.<br><br><b>IP Source Guard:</b> Wpis zostanie zastosowany do funkcji IPv4 Source Guard.<br><br><b>Both:</b> Wpis zostanie zastosowany do obu funkcji. |
|--------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

---

3) Wpisz lub wybierz port podłączony do tego hosta.

4) Kliknij **Apply**.

## 2.1.2 Wiązanie wpisów poprzez ARP Scanning

Przy włączonej funkcji ARP Scanning przełącznik wysyła do hostów pakiety żądania ARP wybranego pola IP. W przypadku otrzymania pakiet odpowiedzi ARP przełącznik może pozyskać adres IP, adres MAC, VLAN ID i numer portu podłączonego do hosta. Możesz dogodnie powiązać wpisy.

---

### Uwaga:

Przed włączeniem tej funkcji upewnij się, że sieć jest bezpieczna, i że aktualnie nie występują ataki ARP na hosty. W przeciwnym wypadku możesz uzyskać błędne wpisy wiązania IP-MAC. Jeżeli sieć jest atakowana, zaleca się przeprowadzenie ręcznego wiązania wpisów.

---

Wybierz z menu **SECURITY > IPv4 IMPB > IP-MAC Binding > ARP Scanning**, aby wyświetlić poniższą stronę.

Rys. 2-2 ARP Scanning

**Scanning Option**

Starting IP Address:  (Format: 192.168.0.1)

Ending IP Address:  (Format: 192.168.0.1)

VLAN ID:  (1-4094)

[Scan](#)

---

**Scanning Result**

[-](#) Delete

| <input type="checkbox"/>            | Host Name | IP Address    | MAC Address       | VLAN ID | Port   | Protect Type |
|-------------------------------------|-----------|---------------|-------------------|---------|--------|--------------|
| <input checked="" type="checkbox"/> | ---       | 192.168.0.28  | c4-6e-1f-bf-72-51 | 1       | 1/0/20 | None         |
| <input type="checkbox"/>            | ---       | 192.168.0.52  | 00-0a-eb-13-23-7b | 1       | 1/0/20 | None         |
| <input type="checkbox"/>            | ---       | 192.168.0.73  | 00-0a-eb-00-13-01 | 1       | 1/0/20 | None         |
| <input type="checkbox"/>            | ---       | 192.168.0.200 | 00-19-66-35-e1-b0 | 1       | 1/0/20 | None         |
| <input type="checkbox"/>            | ---       | 192.168.0.225 | ea-23-51-06-22-52 | 1       | 1/0/20 | None         |
| <input type="checkbox"/>            | ---       | 192.168.0.226 | 00-0a-eb-13-23-97 | 1       | 1/0/20 | None         |
| <input type="checkbox"/>            | ---       | 192.168.0.253 | 14-cc-20-00-00-13 | 1       | 1/0/20 | None         |

1 entry selected. [Cancel](#) [Bind](#)

Wykonaj poniższe kroki, aby skonfigurować wiązanie IP-MAC poprzez ARP scanning:

- 1) W sekcji **Scanning Option** wyznacz zakres adresu IP i VLAN ID. Następnie kliknij **Scan**, aby przeskanować wpisy w wyznaczonym zakresie adresu IP i VLAN.

**Starting IP Address/Ending IP Address** Wyznacz zakres IP, wpisując początkowy i końcowy adres IP.

**VLAN ID** Wyznacz VLAN ID.

- 2) W sekcji **Scanning Result** wybierz co najmniej jeden wpis i skonfiguruj odpowiednie parametry. Następnie kliknij **Bind**.

**Host Name** Wprowadź nazwę, aby umożliwić identyfikację hosta.

**IP Address** Informacja o adresie IP.

**MAC Address** Informacja o adresie MAC.

**VLAN ID** Informacja o VLAN ID.

**Port** Informacja o numerze portu.

|                     |                                                                                                                                                                                                                                                                                                                                                                                                                        |
|---------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Protect Type</b> | <p>Wybierz typ ochrony wpisu. Wpis będzie zastosowany do wybranej funkcji. Dostępne są następujące opcje:</p> <p><b>None:</b> Wpis nie będzie zastosowany do żadnej funkcji.</p> <p><b>ARP Detection:</b> Wpis zostanie zastosowany do funkcji ARP Detection.</p> <p><b>IP Source Guard:</b> Wpis zostanie zastosowany do funkcji IPv4 Source Guard.</p> <p><b>Both:</b> Wpis zostanie zastosowany do obu funkcji.</p> |
|---------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

### 2.1.3 Wiązanie wpisów poprzez DHCP Snooping

Przy włączonej funkcji DHCP Snooping przełącznik może monitorować proces przyjmowania przez host adresu IP i zarejestrować adres IP, adres MAC, VLAN ID i numer portu podłączonego do hosta.

Wybierz z menu **SECURITY > IPv4 IMPB > IP-MAC Binding > DHCP Snooping**, aby wyświetlić poniższą stronę.

Rys. 2-3 DHCP Snooping

**Global Config**

DHCP Snooping:  Enable Apply

---

**VLAN Config**

Filter by VLAN: From  To  Apply

| <input checked="" type="checkbox"/> | VLAN ID | Status   |
|-------------------------------------|---------|----------|
| <input checked="" type="checkbox"/> | 1       | Disabled |

Total: 1 1 entry selected. Cancel Apply

---

**Port Config**

UNIT1

LAGS

| <input type="checkbox"/>            | Port   | Maximum Entries | LAG |
|-------------------------------------|--------|-----------------|-----|
| <input checked="" type="checkbox"/> | 1/0/1  | 512             | --- |
| <input type="checkbox"/>            | 1/0/2  | 512             | --- |
| <input type="checkbox"/>            | 1/0/3  | 512             | --- |
| <input type="checkbox"/>            | 1/0/4  | 512             | --- |
| <input type="checkbox"/>            | 1/0/5  | 512             | --- |
| <input type="checkbox"/>            | 1/0/6  | 512             | --- |
| <input type="checkbox"/>            | 1/0/7  | 512             | --- |
| <input type="checkbox"/>            | 1/0/8  | 512             | --- |
| <input type="checkbox"/>            | 1/0/9  | 512             | --- |
| <input type="checkbox"/>            | 1/0/10 | 512             | --- |

Total: 10 1 entry selected. Cancel Apply

Wykonaj poniższe kroki, aby skonfigurować wiązanie IP-MAC poprzez DHCP Snooping:

- 1) W sekcji **Global Config** włącz DHCP Snooping globalnie. Kliknij **Apply**.
- 2) W sekcji **VLAN Config** włącz DHCP Snooping w sieci VLAN lub w kilku sieciach VLAN. Kliknij **Apply**.

|         |                                              |
|---------|----------------------------------------------|
| VLAN ID | Informacja o VLAN ID.                        |
| Status  | Włącz lub wyłącz DHCP Snooping w sieci VLAN. |

- 3) W sekcji **Port Config** skonfiguruj maks. liczbę wpisów wiązania, których może nauczyć się port przez DHCP Snooping. Kliknij **Apply**.

|                 |                                                                                              |
|-----------------|----------------------------------------------------------------------------------------------|
| Port            | Informacja o numerze portu.                                                                  |
| Maximum Entries | Skonfiguruj maks. liczbę wpisów wiązania, których może nauczyć się port przez DHCP snooping. |
| LAG             | Informacja o grupie LAG, do której należy port.                                              |

- 4) Wyuczone wpisy będą wyświetlane na tablicy wiązania (Binding Table). Aby wyświetlać lub edytować wpisy, idź do **SECURITY > IPv4 IMPB > IP-MAC Binding > Binding Table**.

## 2.1.4 Wyświetlanie wpisów wiązania

Na tablicy wiązania możesz wyświetlić, wyszukać lub edytować wybrane wpisy wiązania.

Wybierz menu **SECURITY > IPv4 IMPB > IP-MAC Binding > Binding Table**, aby załadować następującą stronę.

Rys. 2-4 Binding Table

Binding Table

Source:

IP Address:  (Format: 192.168.0.1)

| <input type="checkbox"/>            | Host Name | IP Address   | MAC Address       | VLAN ID | Port   | Protect Type | Source         |
|-------------------------------------|-----------|--------------|-------------------|---------|--------|--------------|----------------|
| <input checked="" type="checkbox"/> | ---       | 192.168.0.28 | c4-6e-1f-bf-72-51 | 1       | 1/0/20 | None         | ARP Scanning   |
| <input type="checkbox"/>            | PC1       | 192.168.0.98 | 74-d4-35-76-a4-d8 | 1       | 1/0/6  | None         | Manual Binding |

1 entry selected.

Możesz ustawić kryteria wyszukiwania wpisów.



|        |                                                                                                                                                                                                                                                                                                                                                              |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Source | Wybierz źródło wpisu i kliknij <b>Search</b> .<br><br><b>All:</b> Wyświetlanie wpisów ze wszystkich źródeł.<br><br><b>Manual Binding:</b> Wyświetlanie wpisów powiązanych ręcznie.<br><br><b>ARP Scanning:</b> Wyświetlanie wpisów wiązania wyuczonych z ARP Scanning.<br><br><b>DHCP Snooping:</b> Wyświetlanie wpisów wiązania wyuczonych z DHCP Snooping. |
| IP     | Wpisz adres IP i kliknij <b>Search, aby wyszukać konkretny wpis</b> .                                                                                                                                                                                                                                                                                        |

Dodatkowo wybierz co najmniej jeden wpis, aby edytować nazwę hosta i typ ochrony. Kliknij **Apply**.

|              |                                                                                                                                                                                                                                                                                                                                                                                                                 |
|--------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Host Name    | Wpisz nazwę, aby umożliwić identyfikację hosta.                                                                                                                                                                                                                                                                                                                                                                 |
| IP Address   | Informacja o adresie IP.                                                                                                                                                                                                                                                                                                                                                                                        |
| MAC Address  | Informacja o adresie MAC.                                                                                                                                                                                                                                                                                                                                                                                       |
| VLAN ID      | Informacja o VLAN ID.                                                                                                                                                                                                                                                                                                                                                                                           |
| Port         | Informacja o numerze portu.                                                                                                                                                                                                                                                                                                                                                                                     |
| Protect Type | Wybierz typ ochrony wpisu. Wpis będzie zastosowany do wybranej funkcji. Dostępne są następujące opcje:<br><br><b>None:</b> Wpis nie będzie zastosowany do żadnej funkcji.<br><br><b>ARP Detection:</b> Wpis zostanie zastosowany do funkcji ARP Detection.<br><br><b>IP Source Guard:</b> Wpis zostanie zastosowany do funkcji IPv4 Source Guard.<br><br><b>Both:</b> Wpis zostanie zastosowany do obu funkcji. |
| Source       | Informacja o źródle wpisu.                                                                                                                                                                                                                                                                                                                                                                                      |

## 2.2 Przez CLI

Wiązanie wpisów przez ARP scanning nie jest obsługiwane przez CLI. Poniższe sekcje opisują, w jaki sposób powiązać wpisy ręcznie i przez DHCP Snooping oraz jak wyświetlać wpisy wiązania.

### 2.2.1 Ręczne wiązanie wpisów

Możesz ręcznie powiązać adres IP, adres MAC, VLAN ID i numer portu pod warunkiem, że posiadasz szczegółowe dane hostów.

Wykonaj poniższe kroki, aby ręcznie powiązać wpisy:

|        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Krok 1 | <b>configure</b><br>Uruchom tryb konfiguracji globalnej.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Krok 2 | <b>ip source binding</b> <i>hostname ip-addr mac-addr</i> <b>vlan</b> <i>vlan-id</i> <b>interface</b> { <b>fastEthernet</b> <i>port</i>   <b>gigabitEthernet</b> <i>port</i>   <b>ten-gigabitEthernet</b> <i>port</i>   <b>port-channel</b> <i>port-channel-id</i> } { <b>none</b>   <b>arp-detection</b>   <b>ip-verify-source</b>   <b>both</b> }<br><br>Ręcznie powiąz nazwę hosta, adres IP, adres MAC, VLAN ID i numer portu hosta oraz skonfiguruj typ ochrony hosta.<br><br><i>hostname</i> : Wyznacz nazwę hosta, składającą się z maks. 20 znaków.<br><br><i>ip-addr</i> : Wpisz adres IP hosta.<br><br><i>mac-addr</i> : Wpisz adres MAC hosta w formacie xx:xx:xx:xx:xx:xx.<br><br><i>vlan-id</i> : Wpisz VLAN ID hosta.<br><br><i>port</i> : Wpisz numer portu, do którego podłączony jest host.<br><br><b>none</b>   <b>arp-detection</b>   <b>ip-verify-source</b>   <b>both</b> : Wyznacz typ ochrony wpisu. „None” oznacza, że wpis nie będzie zastosowany do żadnej funkcji; „arp-detection” oznacza, że wpis zostanie zastosowany do funkcji ARP Detection; „ip-verify-source” oznacza, że wpis zostanie zastosowany do IPv4 Source Guard. |
| Krok 3 | <b>show ip source binding</b><br>Sprawdź wpis wiązania.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Krok 4 | <b>end</b><br>Powróć do trybu privileged EXEC.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Krok 5 | <b>copy running-config startup-config</b><br>Zapisz ustawienia w pliku konfiguracyjnym.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |

Poniższy przykład prezentuje wiązanie wpisu z nazwą hosta host1, adresem IP 192.168.0.55, adresem MAC 74:d4:35:76:a4:d8, VLAN ID 10, portem numer 1/0/5 i włączenie dla wpisu funkcji ARP detection.

### Switch#configure

```
Switch(config)#ip source binding host1 192.168.0.55 74:d4:35:76:a4:d8 vlan 10 interface
gigabitEthernet 1/0/5 arp-detection
```

### Switch(config)#show ip source binding

| U | Host  | IP-Addr      | MAC-Addr          | VID | Port    | ACL   | SOURCE |
|---|-------|--------------|-------------------|-----|---------|-------|--------|
| - | ----  | -----        | -----             | --- | ----    | ---   | -----  |
| 1 | host1 | 192.168.0.55 | 74:d4:35:76:a4:d8 | 10  | Gi1/0/5 | ARP-D | Manual |

Notice:

1.Here, 'ARP-D' for 'ARP-Detection',and'IP-V-S' for 'IP-Verify-Source'.

```
Switch(config)#end
```

```
Switch#copy running-config startup-config
```

## 2.2.2 Wiązanie wpisów poprzez DHCP Snooping

Wykonaj poniższe kroki, aby powiązać wpisy poprzez DHCP Snooping:

|        |                                                                                                                                                                                                                                                                                                                                                                                               |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Krok 1 | <b>configure</b><br>Uruchom tryb konfiguracji globalnej.                                                                                                                                                                                                                                                                                                                                      |
| Krok 2 | <b>ip dhcp snooping</b><br>Włącz DHCP Snooping globalnie.                                                                                                                                                                                                                                                                                                                                     |
| Krok 3 | <b>ip dhcp snooping vlan <i>vlan-range</i></b><br>Włącz DHCP Snooping w wyznaczonym VLAN.<br><br><i>vlan-range</i> : Wprowadź zakres VLAN w formacie 1-3, 5.                                                                                                                                                                                                                                  |
| Krok 4 | <b>interface { fastEthernet <i>port</i>   range fastEthernet <i>port-list</i>   gigabitEthernet <i>port</i>   range gigabitEthernet <i>port-list</i>   ten-gigabitEthernet <i>port</i>   range ten-gigabitEthernet <i>port-list</i>   interface port-channel <i>port-channel-id</i>   interface range port-channel <i>port-channel-id-list</i> }</b><br>Wejdź w tryb konfiguracji interfejsu. |
| Krok 5 | <b>ip dhcp snooping max-entries <i>value</i></b><br>Skonfiguruj maks. liczbę wpisów wiązania, których port może nauczyć się przez DHCP snooping.<br><br><i>value</i> : Wpisz maks. dopuszczalną liczbę wpisów. Wartość powinna wynosić od 0 do 512.                                                                                                                                           |
| Krok 6 | <b>show ip dhcp snooping</b><br>Sprawdź konfigurację globalną DHCP Snooping.                                                                                                                                                                                                                                                                                                                  |
| Krok 7 | <b>end</b><br>Powróć do trybu privileged EXEC.                                                                                                                                                                                                                                                                                                                                                |
| Krok 8 | <b>copy running-config startup-config</b><br>Zapisz ustawienia w pliku konfiguracyjnym.                                                                                                                                                                                                                                                                                                       |

Poniższy przykład prezentuje globalne włączanie DHCP Snooping we VLAN 5 i ustawianie maks. liczby wpisów wiązania, których może nauczyć się port 1/0/1 przez DHCP snooping na100:

```
Switch#configure
```

```
Switch(config)#ip dhcp snooping
```

```
Switch(config)#ip dhcp snooping vlan 5
```

```
Switch(config)#interface gigabitEthernet 1/0/1
```

```
Switch(config-if)#ip dhcp snooping max-entries 100
```

```
Switch(config-if)#show ip dhcp snooping
```

```
Global Status: Enable
```

```
VLAN ID: 5
```

```
Switch(config-if)#show ip dhcp snooping interface gigabitEthernet 1/0/1
```

```
Interface max-entries LAG
```

```

```

| Interface | max-entries | LAG |
|-----------|-------------|-----|
| Gi1/0/1   | 100         | N/A |

```
Switch(config-if)#end
```

```
Switch#copy running-config startup-config
```

### 2.2.3 Wyświetlanie wpisów wiązania

W trybie użytkownika uprzywilejowanego (privileged EXEC mode), tak jak i w każdym innym trybie konfiguracji, możesz wyświetlać wpisy wiązania, korzystając z poniższego polecenia:

---

```
show ip source binding
```

Wyświetl dane wpisów wiązania (nazwa hosta, adres IP, adres MAC, VLAN ID, numer portu, typ ochrony).

---

# 3 Konfiguracja funkcji ARP Detection

Aby przeprowadzić konfigurację funkcji ARP Detection, wykonaj poniższe kroki:

- 1) Dodaj wpisy wiązania IP-MAC.
- 2) Włącz ARP Detection.
- 3) Skonfiguruj ARP Detection na portach.
- 4) Sprawdź statystyki ARP.

## 3.1 Przez GUI

### 3.1.1 Dodawanie wpisów wiązania IP-MAC

Funkcja ARP Detection polega na wykrywaniu przez przełącznik pakietów ARP w oparciu o wpisy wiązania na tablicy wiązania IP-MAC (IP-MAC Binding Table.) Przed konfiguracją funkcji ARP Detection należy przeprowadzić konfigurację wiązania IP-MAC. Więcej informacji na ten temat znajdziesz w części *Konfiguracja wiązania IP-MAC*.

### 3.1.2 Włączanie funkcji ARP Detection

Wybierz z menu **SECURITY > IPv4 IMPB > ARP Detection > Global Config**, aby wyświetlić poniższą stronę.

Rys. 3-1 Globalna konfiguracja ARP Detection

Global Config

---

ARP Detect:  Enable

Validate Source MAC:  Enable

Validate Destination MAC:  Enable

Validate IP:  Enable

[Apply](#)

VLAN Config

|                                     | VLAN ID | Status            | Log Status                                   |
|-------------------------------------|---------|-------------------|----------------------------------------------|
| <input checked="" type="checkbox"/> | 1       | Disabled          | Disabled                                     |
| Total: 1                            |         | 1 entry selected. | <a href="#">Cancel</a> <a href="#">Apply</a> |

Wykonaj poniższe kroki, aby włączyć ARP Detection:

- 1) W sekcji **Global Config** włącz ARP Detection i skonfiguruj powiązane parametry. Kliknij **Apply**.

|                          |                                                                                                                                                                                                                                                                                                           |
|--------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ARP Detect               | Włącz lub wyłącz ARP Detection globalnie.                                                                                                                                                                                                                                                                 |
| Validate Source MAC      | Możesz włączyć na przełączniku sprawdzanie, czy przy odbieraniu pakietu ARP źródłowy adres MAC i adres MAC nadawcy są takie same. Jeżeli adresy są różne, pakiet ARP zostanie odrzucony.                                                                                                                  |
| Validate Destination MAC | Możesz włączyć na przełączniku sprawdzanie, czy podczas odbierania pakietu odpowiedzi ARP docelowy adres MAC i źródłowy adres MAC są takie same. Jeżeli adresy są różne, pakiet ARP zostanie odrzucony.                                                                                                   |
| Validate IP              | Możesz włączyć na przełączniku sprawdzanie, czy adres IP nadawcy wszystkich pakietów ARP i docelowy adres IP pakietów odpowiedzi ARP są legalne. Nielegalne pakiety ARP, takie jak adresy broadcast, adresy multicast, adresu klasy E, adresy loopback (127.0.0.0/8) i adres 0.0.0.0., zostaną odrzucone. |

2) W sekcji **VLAN Config** włącz ARP Detection w wybranych sieciach VLAN. Kliknij **Apply**.

|            |                                                                                                                                                                                |
|------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| VLAN ID    | Informacja o VLAN ID.                                                                                                                                                          |
| Status     | Włącz lub wyłącz ARP Detection w sieci VLAN.                                                                                                                                   |
| Log Status | Włącz lub wyłącz w sieci VLAN Log Feature (funkcja rejestru zdarzeń). Jeżeli funkcja jest włączona, przełącznik po odrzuceniu nielegalnego pakietu ARP będzie generował zapis. |

### 3.1.3 Konfiguracja funkcji ARP Detection na portach

Wybierz z menu **SECURITY > IPv4 IMPB > ARP Detection > Port Config**, aby wyświetlić poniższą stronę.

Rys. 3-2 ARP Detection na porcie

| Port Config                         |        |              |                           |                        |                                  |        |           |     |
|-------------------------------------|--------|--------------|---------------------------|------------------------|----------------------------------|--------|-----------|-----|
| UNIT1                               |        | LAGS         |                           |                        |                                  |        |           |     |
| <input type="checkbox"/>            | Port   | Trust Status | Limit Rate<br>pps (0-300) | Current Speed<br>(pps) | Burst Interval<br>seconds (1-15) | Status | Operation | LAG |
| <input checked="" type="checkbox"/> | 1/0/1  | Disabled     | 100                       | 0                      | 1                                | Normal | ---       | --- |
| <input type="checkbox"/>            | 1/0/2  | Disabled     | 100                       | 0                      | 1                                | Normal | ---       | --- |
| <input type="checkbox"/>            | 1/0/3  | Disabled     | 100                       | 0                      | 1                                | Normal | ---       | --- |
| <input type="checkbox"/>            | 1/0/4  | Disabled     | 100                       | 0                      | 1                                | Normal | ---       | --- |
| <input type="checkbox"/>            | 1/0/5  | Disabled     | 100                       | 0                      | 1                                | Normal | ---       | --- |
| <input type="checkbox"/>            | 1/0/6  | Disabled     | 100                       | 0                      | 1                                | Normal | ---       | --- |
| <input type="checkbox"/>            | 1/0/7  | Disabled     | 100                       | 0                      | 1                                | Normal | ---       | --- |
| <input type="checkbox"/>            | 1/0/8  | Disabled     | 100                       | 0                      | 1                                | Normal | ---       | --- |
| <input type="checkbox"/>            | 1/0/9  | Disabled     | 100                       | 0                      | 1                                | Normal | ---       | --- |
| <input type="checkbox"/>            | 1/0/10 | Disabled     | 100                       | 0                      | 1                                | Normal | ---       | --- |

Total: 10      1 entry selected.      Cancel Apply

Wykonaj poniższe kroki, aby skonfigurować ARP Detection na portach:

1) Wybierz co najmniej jeden port i skonfiguruj odpowiednie parametry.

|                |                                                                                                                                                                                                                                                                                                                  |
|----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Trust Status   | Włącz lub wyłącz dla tego portu status portu zaufanego. Na porcie zaufanym pakiety ARP przekierowywane są bezpośrednio, bez sprawdzania. Zaleca się ustawienie portów niektórych typów, np. portów uplink czy portów routingu, jako zaufane.                                                                     |
| Limit Rate     | Wyznacz maks. liczbę pakietów ARP, które mogą być odbierane na porcie na jedną sekundę.                                                                                                                                                                                                                          |
| Current Speed  | Informacja o aktualnej prędkości odbierania pakietów ARP na porcie.                                                                                                                                                                                                                                              |
| Burst Interval | Wyznacz zakres czasu. Jeżeli prędkość otrzymywanych pakietów ARP osiągnie górną granicę tego zakresu, port zostanie zamknięty.                                                                                                                                                                                   |
| Status         | Informacja o stanie ataku ARP:<br><br><b>Normal:</b> Przekierowywanie pakietów ARP na porcie przebiega normalnie.<br><br><b>Down:</b> Prędkość przekazywania legalnych pakietów ARP przekracza wyznaczoną wartość. Port zostanie zamknięty za 300 sekund. Aby na nowo uaktywnić port, kliknij przycisk Recovery. |
| Operation      | Jeżeli stan zmieni się na Down, pojawi się przycisk <b>Recover</b> . Możesz kliknąć ten przycisk, aby przywrócić port do normalnego stanu.                                                                                                                                                                       |
| LAG            | Informacja o grupie LAG, do której należy port.                                                                                                                                                                                                                                                                  |

2) Kliknij **Apply**.

### 3.1.4 Wyświetlanie statystyk ARP

Możesz zobaczyć liczbę nielegalnych pakietów ARP otrzymanych przez każdy port. Ułatwi to zlokalizowanie przyczyny wadliwego działania sieci i podjęcie odpowiednich środków dla zabezpieczenia sieci.

Wybierz z menu **SECURITY > IPv4 IMPB > ARP Detection > ARP Statistics**, aby wyświetlić poniższą stronę.

Rys. 3-3 Statystyki ARP

| Auto Refresh        |                                 |               |
|---------------------|---------------------------------|---------------|
| Auto Refresh:       | <input type="checkbox"/> Enable | <b>Apply</b>  |
| Illegal ARP Packets |                                 |               |
|                     |                                 | Refresh Clear |
| VLAN ID             | Forwarded                       | Dropped       |
| 1                   | 0                               | 0             |
| Total: 1            |                                 |               |

W sekcji **Auto Refresh** możesz włączyć funkcję automatycznego odświeżania i wyznaczyć odstęp czasu, w którym strona internetowa będzie automatycznie odświeżana.

W sekcji **Illegal ARP Packet** możesz sprawdzić liczbę nielegalnych pakietów ARP w każdej sieci VLAN.

|           |                                                                  |
|-----------|------------------------------------------------------------------|
| VLAN ID   | Informacja o VLAN ID.                                            |
| Forwarded | Informacja o liczbie przekazanych pakietów ARP w tej sieci VLAN. |
| Dropped   | Informacja o liczbie odrzuconych pakietów ARP w tej sieci VLAN.  |

## 3.2 Przez CLI

### 3.2.1 Dodawanie wpisów wiązania IP-MAC

Funkcja ARP Detection polega na wykrywaniu przez przełącznik pakietów ARP w oparciu o wpisy wiązania na tablicy wiązania IP-MAC (IP-MAC Binding Table.) Przed konfiguracją funkcji ARP Detection należy przeprowadzić konfigurację wiązania IP-MAC. Więcej informacji na ten temat znajdziesz w części *Konfiguracja wiązania IP-MAC*.

### 3.2.2 Włączanie funkcji ARP Detection

Wykonaj poniższe kroki, aby włączyć ARP Detection:

|        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Krok 1 | <b>configure</b><br>Uruchom tryb konfiguracji globalnej.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Krok 2 | <b>ip arp inspection</b><br>Włącz funkcję ARP Detection globalnie.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Krok 3 | <b>ip arp inspection validate { src-mac   dst-mac   ip }</b><br>Skonfiguruj na przełączniku sprawdzanie adresów IP lub adresów MAC otrzymanych pakietów.<br><br><b>src-mac:</b> Włącz na przełączniku sprawdzanie podczas odbierania pakietu ARP, czy źródłowy adres MAC i adres MAC nadawcy są takie same. Jeżeli adresy są różne, pakiet ARP zostanie odrzucony.<br><br><b>dst-mac:</b> Włącz na przełączniku sprawdzanie podczas odbierania pakietu odpowiedzi ARP, czy docelowy adres MAC i źródłowy adres MAC są takie same. Jeżeli adresy są różne, pakiet ARP zostanie odrzucony.<br><br><b>ip:</b> Włącz na przełączniku sprawdzanie, czy adres IP nadawcy wszystkich pakietów ARP i docelowy adres IP pakietów odpowiedzi ARP są legalne. Nielegalne pakiety ARP, takie jak adresy broadcast, adresy multicast, adresy klasy E, adresy loopback (127.0.0.0/8) i adres 0.0.0.0., zostaną odrzucone |



- 
- Krok 4      **ip arp inspection vlan *vlan-list***  
 Włącz ARP Detection na co najmniej jednej istniejącej sieci VLAN 802.1Q.  
*vlan-list*: Wpisz VLAN ID. Format to 1,5-9.
- 
- Krok 5      **ip arp inspection vlan *vlan-list* logging**  
 (Opcjonalnie) Włącz funkcję Log feature (funkcja rejestru zdarzeń, aby przełącznik po odrzuceniu nielegalnego pakietu ARP generował zapis.  
*vlan-list*: Wpisz VLAN ID. Format to 1,5-9.
- 
- Krok 6      **show ip arp inspection**  
 Sprawdź ustawienia ARP Detection.
- 
- Krok 7      **end**  
 Powróć do trybu privileged EXEC.
- 
- Krok 8      **copy running-config startup-config**  
 Zapisz ustawienia w pliku konfiguracyjnym.
- 

Poniższy przykład prezentuje włączanie globalne ARP Detection na VLAN 2 i włączanie na przełączniku sprawdzania przy odbieraniu pakietów, czy ARP źródłowy adres MAC i adres MAC nadawcy są takie same:

**Switch#configure**

**Switch(config)#ip arp inspection**

**Switch(config)#ip arp inspection validate src-mac**

**Switch(config)#ip arp inspection vlan 2**

**Switch(config)#show ip arp inspection**

Global Status: Enable

Verify SMAC: Enable

Verify DMAC: Disable

Verify IP: Disable

**Switch(config)#show ip arp inspection vlan**

| VID  | Enable status | Log Status |
|------|---------------|------------|
| ---- | -----         | -----      |
| 1    | Disable       | Disable    |
| 2    | Enable        | Disable    |

**Switch(config)#end**

**Switch#copy running-config startup-config****3.2.3 Konfiguracja funkcji ARP Detection na portach**

Wykonaj poniższe kroki, aby skonfigurować ARP Detection na portach:

|         |                                                                                                                                                                                                                                                                                     |
|---------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Krok 1  | <b>configure</b><br>Uruchom tryb konfiguracji globalnej.                                                                                                                                                                                                                            |
| Krok 2  | <b>interface { fastEthernet <i>port</i>   range fastEthernet <i>port-list</i>   gigabitEthernet <i>port</i>   range gigabitEthernet <i>port-list</i>   ten-gigabitEthernet <i>port</i>   range ten-gigabitEthernet <i>port-list</i> }</b><br>Uruchom tryb konfiguracji interfejsu.  |
| Krok 3  | <b>ip arp inspection trust</b><br>Ustaw port jako zaufany, który nie będzie objęty działaniem funkcji ARP Detection. Zaleca się ustawienie portów niektórych typów, np. portów uplink czy portów routingu, jako zaufane.                                                            |
| Krok 4  | <b>ip arp inspection limit-rate <i>value</i></b><br>Wyznacz maks. liczbę pakietów ARP, które mogą być odbierane na porcie na jedną sekundę.<br><i>value</i> : Wyznacz wartość maksymalną. Wartość powinna wynosić od 0 do 300 p/s (pakiety na sekundę); wartość domyślna to 100.    |
| Krok 5  | <b>ip arp inspection burst-interval <i>value</i></b><br>Wyznacz zakres czasu. Jeżeli prędkość otrzymywanych pakietów ARP osiągnie górną granicę tego zakresu, port zostanie zamknięty.<br><i>value</i> : Wyznacz zakres czasu, między 1 a 15 sekund. Wartość domyślna to 1 sekunda. |
| Krok 6  | <b>show ip arp inspection interface</b><br>Sprawdź konfigurację i stan portu.                                                                                                                                                                                                       |
| Krok 7  | <b>show ip arp inspection vlan</b><br>Sprawdź konfigurację i stan sieci VLAN.                                                                                                                                                                                                       |
| Krok 8  | <b>ip arp inspection recover</b><br>(Opcjonalnie) Porty, których prędkość odbierania pakietów przekroczyła wyznaczony limit można przywrócić do stanu Normal za pomocą tego polecenia.                                                                                              |
| Krok 9  | <b>end</b><br>Powróć do trybu privileged EXEC.                                                                                                                                                                                                                                      |
| Krok 10 | <b>copy running-config startup-config</b><br>Zapisz ustawienia w pliku konfiguracyjnym.                                                                                                                                                                                             |

Poniższy przykład prezentuje ustawienie portu 1/0/2 jako zaufany, ustawienie limitu prędkości na 20 p/s i zakresu czasu (burst interval) na porcie 1/0/2 na 2 sekundy:

```
Switch#configure
```

```
Switch(config)#interface gigabitEthernet 1/0/2
```

```
Switch(config-if)#ip arp inspection trust
```

```
Switch(config-if)#ip arp inspection limit-rate 20
```

```
Switch(config-if)#ip arp inspection burst-interval 2
```

```
Switch(config-if)#show ip arp inspection interface gigabitEthernet 1/0/2
```

| Interface | Trust state | limit Rate(pps) | Current speed(pps) | Burst Interval | Status | LAG |
|-----------|-------------|-----------------|--------------------|----------------|--------|-----|
| -----     | -----       | -----           | -----              | -----          | -----  | --- |
| Gi1/0/2   | Enable      | 20              | 0                  | 2              | ---    | N/A |

```
Switch(config-if)#end
```

```
Switch#copy running-config startup-config
```

Poniższy przykład przedstawia sposób przywracania portu 1/0/1 w stanie Down do stanu Normal:

```
Switch#configure
```

```
Switch(config)#interface gigabitEthernet 1/0/1
```

```
Switch(config-if)#ip arp inspection recover
```

```
Switch(config-if)#end
```

```
Switch#copy running-config startup-config
```

### 3.2.4 Wyświetlanie statystyk ARP

W trybie privileged EXEC, tak jak i w każdym innym trybie konfiguracji, możesz wyświetlać wpisy wiązania, korzystając z poniższego polecenia:

```
show ip arp inspection statistics
```

Wyświetl statystyki ARP dla każdego portu (liczba przekazanych pakietów ARP, liczba odrzuconych pakietów ARP).

# 4 Konfiguracja funkcji IPv4 Source Guard

Aby przeprowadzić konfigurację IPv4 Source Guard, wykonaj poniższe kroki:

- 1) Dodaj wpis wiązania IP-MAC.
- 2) Skonfiguruj funkcję IPv4 Source Guard.

## 4.1 Przez GUI

### 4.1.1 Dodawanie wpisów wiązania IP-MAC

Funkcja IPv4 Source Guard polega na filtrowaniu przez przełącznik pakietów, które nie są dopasowane do reguł tabeli wiązania IPv4-MAC. Przed konfiguracją funkcji ARP Detection należy więc przeprowadzić konfigurację wiązania IP-MAC. Więcej informacji na ten temat znajdziesz w części *Konfiguracja wiązania IP-MAC*.

### 4.1.2 Konfiguracja funkcji IPv4 Source Guard

Wybierz z menu **SECURITY > IPv4 IMPB > IPv4 Source Guard**, aby wyświetlić poniższą stronę.

Rys. 4-1 Konfiguracja funkcji IPv4 Source Guard

Global Config

---

IPv4 Source Guard Log:  Enable Apply

Port Config

UNIT1
LAGS

|                                     | Port   | Security Type | LAG |
|-------------------------------------|--------|---------------|-----|
| <input checked="" type="checkbox"/> | 1/0/1  | Disable       | --  |
| <input type="checkbox"/>            | 1/0/2  | Disable       | --  |
| <input type="checkbox"/>            | 1/0/3  | Disable       | --  |
| <input type="checkbox"/>            | 1/0/4  | Disable       | --  |
| <input type="checkbox"/>            | 1/0/5  | Disable       | --  |
| <input type="checkbox"/>            | 1/0/6  | Disable       | --  |
| <input type="checkbox"/>            | 1/0/7  | Disable       | --  |
| <input type="checkbox"/>            | 1/0/8  | Disable       | --  |
| <input type="checkbox"/>            | 1/0/9  | Disable       | --  |
| <input type="checkbox"/>            | 1/0/10 | Disable       | --  |

Total: 10 1 entry selected. Cancel Apply

Wykonaj poniższe kroki, aby skonfigurować IPv4 Source Guard:

- 1) W sekcji **Global Config** section zdecyduj, czy chcesz włączyć funkcję Log. Kliknij **Apply**.

|                      |                                                                                                                                                                                     |
|----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Pv4 Source Guard Log | Włącz lub wyłącz funkcję IPv4 Source Guard Log (funkcja rejestru zdarzeń). Jeżeli funkcja jest włączona, przełącznik po odrzuceniu nielegalnego pakietu ARP będzie generował zapis. |
|----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

- 2) W sekcji **Port Config** skonfiguruj tryb ochrony portów i kliknij **Apply**.

|               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|---------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Port          | Informacja o numerze portu.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Security Type | Wybierz tryb ochrony na porcie dla pakietów IPv4. Dostępne są następujące opcje:<br><br><b>Disable:</b> Funkcja IP Source Guard jest wyłączona na porcie.<br><br><b>SIP+MAC:</b> Przetwarzane mogą być jedynie pakiety ze źródłowym adresem IP, źródłowym adresem MAC i numerem portu dopasowanym do reguł wiązania IPv4-MAC. Pozostałe pakiety będą odrzucane.<br><br><b>SIP:</b> Przetwarzane mogą być jedynie pakiety ze źródłowym adresem IP i numerem portu dopasowanym do reguł wiązania IPv4-MAC. Pozostałe pakiety będą odrzucane. |
| LAG           | Informacja o grupie LAG, do której należy port.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |

## 4.2 Przez CLI

### 4.2.1 Dodawanie wpisów wiązania IP-MAC

Funkcja IPv4 Source Guard polega na filtrowaniu przez przełącznik pakietów, które nie są dopasowane do reguł tabeli wiązania IPv4-MAC. Przed konfiguracją funkcji ARP Detection należy więc przeprowadzić konfigurację wiązania IP-MAC. Więcej informacji na ten temat znajdziesz w części *Konfiguracja wiązania IP-MAC*.

### 4.2.2 Konfiguracja funkcji IPv4 Source Guard

Wykonaj poniższe kroki, aby skonfigurować IPv4 Source Guard:

|        |                                                                                                                                                                                                                                          |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Krok 1 | <b>configure</b><br>Uruchom tryb konfiguracji globalnej.                                                                                                                                                                                 |
| Krok 2 | <b>interface { fastEthernet port   range fastEthernet port-list   gigabitEthernet port   range gigabitEthernet port-list   ten-gigabitEthernet port   range ten-gigabitEthernet port-list }</b><br>Uruchom tryb konfiguracji interfejsu. |

- 
- Krok 3      **ip verify source { sip+mac | sip }**  
 Włącz IP Source Guard dla pakietów IPv4.
- sip+mac:** Przetwarzane mogą być jedynie pakiety ze źródłowym adresem IP, źródłowym adresem MAC i numerem portu dopasowanym do reguł wiązania IPv4-MAC. Pozostałe pakiety będą odrzucane.
- sip:** Przetwarzane mogą być jedynie pakiety ze źródłowym adresem IP i numerem portu dopasowanym do reguł wiązania IPv4-MAC. Pozostałe pakiety będą odrzucane.
- 
- Krok 4      **show ip verify source [ interface { fastEthernet *port* | gigabitEthernet *port* | ten-gigabitEthernet *port* | port-channel *port-channel-id* } ]**  
 Sprawdź konfigurację IP Source Guard dla pakietów IPv4.
- 
- Krok 5      **end**  
 Powróć do trybu privileged EXEC.
- 
- Krok 6      **copy running-config startup-config**  
 Zapisz ustawienia w pliku konfiguracyjnym.
- 

Poniższy przykład prezentuje włączanie IPv4 Source Guard na porcie 1/0/1:

**Switch#configure**

**Switch(config)#interface gigabitEthernet 1/0/1**

**Switch(config-if)#ip verify source sip+mac**

**Switch(config-if)#show ip verify source interface gigabitEthernet 1/0/1**

| Port    | Security-Type | LAG  |
|---------|---------------|------|
| ----    | -----         | ---- |
| Gi1/0/1 | SIP+MAC       | N/A  |

**Switch(config-if)#end**

**Switch#copy running-config startup-config**

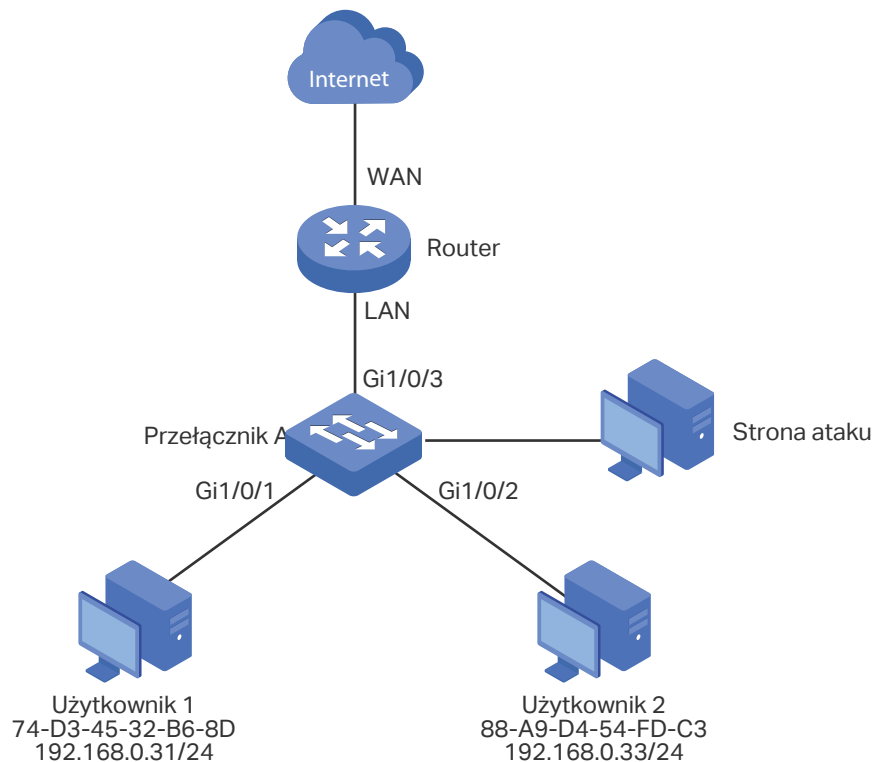
# 5 Przykłady konfiguracji

## 5.1 Przykład dla ARP Detection

### 5.1.1 Wymagania sieciowe

Jak pokazano poniżej, użytkownik 1 i użytkownik 2 to legalni użytkownicy w sieci LAN, podłączeni do portów 1/0/1 i 1/0/2. Obaj są w domyślnej sieci VLAN 1. Na routerze skonfigurowana została funkcja zabezpieczająca, aby zapobiegać atakom z sieci WAN. Administrator sieci planuje także skonfigurować przełącznik A, aby zapobiegać atakom ARP z sieci LAN.

Rys. 5-1 Topologia sieci



### 5.1.2 Schemat konfiguracji

Aby spełnić powyższy warunek, należy skonfigurować ARP Detection, aby chronić sieć przed atakami ARP z sieci LAN.

Konfiguracja na przełączniku wymaga wykonania następujących kroków:

- 1) Skonfiguruj wiązanie IP-MAC. Wpisy wiązań dla użytkownika 1 i użytkownika 2 powinny być wiązaniami ręcznymi.
- 2) Skonfiguruj globalnie ARP Detection.

- 3) Skonfiguruj ARP Detection na portach. Ponieważ port 1/0/3 jest podłączony do routera będącego bramą sieciową, ustaw port 1/0/3 jako port trusted. Aby zapobiec atakom ARP flooding, ustaw limit częstotliwości otrzymywania pakietów ARP na wszystkich portach.

W poniższych podrozdziałach opisano dwa sposoby przeprowadzenia procedury konfiguracji: przez GUI oraz przez CLI.

### 5.1.3 Przez GUI

- 1) Wybierz z menu **SECURITY > IPv4 IMBP > IP-MAC Binding > Manual Binding** i kliknij **+ Add**, aby wyświetlić poniższą stronę. Wpisz nazwę hosta, adres IP, adres MAC i VLAN ID użytkownika 1, ustaw typ ochrony jako ARP Detection, i zaznacz na panelu port 1/0/1. Kliknij **Apply**.

Rys. 5-2 Wpis wiązania dla użytkownika 1

The screenshot shows the 'IPv4-MAC Binding' configuration page. The form contains the following fields:

- Host Name: User1 (20 characters maximum)
- IP Address: 192.168.0.31 (Format: 192.168.0.1)
- MAC Address: 74-D3-45-32-B6-8D (Format: 00-00-00-00-00-01)
- VLAN ID: 1 (1-4094)
- Protect Type: ARP Detection (dropdown menu)
- Port: 1/0/1 (Format: 1/0/1, input or choose below)

Below the form is a port selection panel for UNIT1 (ports 1-8) and LAGS (ports 9-10). Port 1 is selected. A legend shows Selected (blue), Unselected (white), and Not Available (grey). Buttons for Cancel and Apply are at the bottom right.

- 2) W ten sam sposób dodaj wpis wiązania dla użytkownika 2. Wpisz nazwę hosta, adres IP, adres MAC i VLAN ID użytkownika 2, ustaw typ ochrony jako ARP Detection, i zaznacz na panelu port 1/0/2. Kliknij **Apply**.



Rys. 5-3 Wpis wiązania dla użytkownika 2

IPv4-MAC Binding

Host Name:  (20 characters maximum)

IP Address:  (Format: 192.168.0.1)

MAC Address:  (Format: 00-00-00-00-00-01)

VLAN ID:  (1-4094)

Protect Type:  ▼

Port:  (Format: 1/0/1, input or choose below)

UNIT1      LAGS

1

2

3

4

5

6

7

8

9

10

Selected

Unselected

Not Available

Cancel

Apply

- 3) Wybierz z menu **SECURITY > IPv4 IMBP > ARP Detection > Global Config**, aby wyświetlić poniższą stronę. Włącz ARP Detect, Validate Source MAC, Validate Destination MAC oraz Validate IP i kliknij **Apply**. Zaznacz VLAN 1, zmień Status na Enabled i kliknij **Apply**.

Rys. 5-4 Włączanie ARP Detection

Global Config

ARP Detect:  Enable

Validate Source MAC:  Enable

Validate Destination MAC:  Enable

Validate IP:  Enable

Apply

VLAN Config

|                                     | VLAN ID | Status  | Log Status |
|-------------------------------------|---------|---------|------------|
| <input checked="" type="checkbox"/> | 1       | Enabled | Disabled   |

Total: 1      1 entry selected.

Cancel

Apply

- 4) Wybierz z menu **SECURITY > IPv4 IMBP > ARP Detection > Port Config**, aby wyświetlić poniższą stronę. Domyślnie wszystkie porty mają włączoną funkcję ARP Detection oraz

ochronę przed atakami ARP flooding. Ustaw port 1/0/3 jako prot trusted, a pozostałe parametry ochrony pozostaw domyślne. Kliknij **Apply**.


Rys. 5-5 Konfiguracja portów

Port Config

UNIT1 LAGS

| <input type="checkbox"/>            | Port   | Trust Status | Limit Rate<br>pps (0-300) | Current Speed<br>(pps) | Burst Interval<br>seconds (1-15) | Status | Operation | LAG |
|-------------------------------------|--------|--------------|---------------------------|------------------------|----------------------------------|--------|-----------|-----|
| <input type="checkbox"/>            | 1/0/1  | Disabled     | 100                       | 0                      | 1                                | Normal | ---       | --- |
| <input type="checkbox"/>            | 1/0/2  | Disabled     | 100                       | 0                      | 1                                | Normal | ---       | --- |
| <input checked="" type="checkbox"/> | 1/0/3  | Enabled      | 100                       | 0                      | 1                                | Normal | ---       | --- |
| <input type="checkbox"/>            | 1/0/4  | Disabled     | 100                       | 0                      | 1                                | Normal | ---       | --- |
| <input type="checkbox"/>            | 1/0/5  | Disabled     | 100                       | 0                      | 1                                | Normal | ---       | --- |
| <input type="checkbox"/>            | 1/0/6  | Disabled     | 100                       | 0                      | 1                                | Normal | ---       | --- |
| <input type="checkbox"/>            | 1/0/7  | Disabled     | 100                       | 0                      | 1                                | Normal | ---       | --- |
| <input type="checkbox"/>            | 1/0/8  | Disabled     | 100                       | 0                      | 1                                | Normal | ---       | --- |
| <input type="checkbox"/>            | 1/0/9  | Disabled     | 100                       | 0                      | 1                                | Normal | ---       | --- |
| <input type="checkbox"/>            | 1/0/10 | Disabled     | 100                       | 0                      | 1                                | Normal | ---       | --- |

Total: 10 1 entry selected. Cancel Apply

- 5) Kliknij  Save, aby zapisać ustawienia.

## 5.1.4 Przez CLI

- 1) Dodaj wpisy ręcznych wiązań dla użytkownika 1 i użytkownika 2.

```
Switch_A#configure
```

```
Switch_A(config)#ip source binding User1 192.168.0.31 74:d3:45:32:b6:8d vlan 1
interface gigabitEthernet 1/0/1 arp-detection
```

```
Switch_A(config)#ip source binding User1 192.168.0.32 88:a9:d4:54:fd:c3 vlan 1
interface gigabitEthernet 1/0/2 arp-detection
```

- 2) Włącz globalnie ARP Detection oraz w sieci VLAN 1.

```
Switch_A(config)#ip arp inspection
```

```
Switch_A(config)#ip arp inspection vlan 1
```

- 3) Ustaw prot 1/0/3 jako port trusted.

```
Switch_A(config)#interface gigabitEthernet 1/0/3
```

```
Switch_A(config-if)#ip arp inspection trust
```

```
Switch_A(config-if)#end
```

```
Switch_A#copy running-config startup-config
```

## Sprawdzanie konfiguracji

Sprawdzanie wpisów wiązań IP-MAC:

Switch\_A#show ip source binding

| U | Host  | IP-Addr      | MAC-Addr          | VID | Port    | ACL   | SOURCE |
|---|-------|--------------|-------------------|-----|---------|-------|--------|
| - | ----  | -----        | -----             | --- | ----    | ---   | -----  |
| 1 | User1 | 192.168.0.31 | 74:d3:45:32:b6:8d | 1   | Gi1/0/1 | ARP-D | Manual |
| 1 | User2 | 192.168.0.33 | 88:a9:d4:54:fd:c3 | 1   | Gi1/0/2 | ARP-D | Manual |

Notice:

1.Here, 'ARP-D' for 'ARP-Detection',and'IP-V-S' for 'IP-Verify-Source'.

Sprawdzanie globalnej konfiguracji ARP Detection:

Switch\_A#show ip arp inspection

Global Status: Enable

Verify SMAC: Enable

Verify DMAC: Enable

Verify IP: Enable

Sprawdzanie konfiguracji ARP Detection w sieci VLAN:

Switch\_A#show ip arp inspection vlan

| VID  | Enable status | Log Status |
|------|---------------|------------|
| ---- | -----         | -----      |
| 1    | Enable        | Disable    |

Sprawdzanie konfiguracji ARP Detection na portach:

Switch\_A#show ip arp inspection interface

| Interface | Trust state | limit Rate(pps) | Current speed(pps) | Burst Interval | Status | LAG |
|-----------|-------------|-----------------|--------------------|----------------|--------|-----|
| -----     | -----       | -----           | -----              | -----          | -----  | --- |
| Gi1/0/1   | Disable     | 100             | 0                  | 1              | ---    | N/A |
| Gi1/0/2   | Disable     | 100             | 0                  | 1              | ---    | N/A |
| Gi1/0/3   | Enable      | 100             | 0                  | 1              | ---    | N/A |

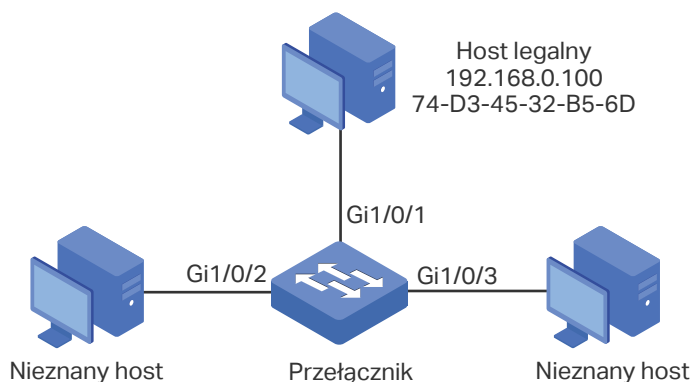
...

## 5.2 Przykład dla IP Source Guard

### 5.2.1 Wymagania sieciowe

Jak pokazano poniżej, the host legalny łączy się z przełącznikiem poprzez port 1/0/1 i należy do domyślnej sieci VLAN 1. Wymaga się, aby tylko host legalny miał dostęp do sieci poprzez port 1/0/1, a inne hosty będą blokowane starając się o dostęp do sieci poprzez porty 1/0/1-3.

Rys. 5-6 Topologia sieci



### 5.2.2 Schemat konfiguracji

Aby spełnić ten warunek, należy skorzystać z wiązania IP-MAC oraz funkcji IP Source Guard w celu filtrowania pakietów odbieranych od hostów nieznanymi. Konfiguracja na przełączniku wymaga wykonania następujących kroków:

- 1) Powiąż adres MAC, adres IP, numer podłączonego portu i VLAN ID hosta legalnego poprzez wiązanie IP-MAC.
- 2) Włącz IP Source Guard na portach 1/0/1-3.

W poniższych podrozdziałach opisano dwa sposoby przeprowadzenia procedury konfiguracji: przez GUI oraz przez CLI.

### 5.2.3 Przez GUI

- 1) Wybierz z menu **SECURITY > IPv4 IMPB > IP-MAC Binding > Manual Binding** i kliknij **+ Add**, aby wyświetlić poniższą stronę. Wprowadź nazwę hosta, adres IP, adres MAC i VLAN ID hosta legalnego, ustaw typ ochrony jako SIP+MAC i zaznacz na panelu port 1/0/1. Kliknij **Apply**.

Rys. 5-7 Wiązanie ręczne

### IPv4-MAC Binding

|               |                   |                                        |
|---------------|-------------------|----------------------------------------|
| Host Name:    | LegalHost         | (20 characters maximum)                |
| IP Address:   | 192.168.0.100     | (Format: 192.168.0.1)                  |
| MAC Address:  | 74-D3-45-32-B5-6D | (Format: 00-00-00-00-00-01)            |
| VLAN ID:      | 1                 | (1-4094)                               |
| Protect Type: | IP Source Guard ▼ |                                        |
| Port:         | 1/0/1             | (Format: 1/0/1, input or choose below) |

UNIT1
LAGS

Cancel
Apply

- 2) Wybierz z menu **SECURITY > IPv4 IMPB > IPv4 Source Guard**, aby wyświetlić poniższą stronę. Włącz IPv4 Source Guard Logging, aby przełącznik generował dzienniki po odebraniu nielegalnych pakietów i kliknij **Apply**. Zaznacz porty 1/0/1-3, ustaw Security Type jako SIP+MAC i kliknij **Apply**.

Rys. 5-8 IPv4 Source Guard

Global Config

IPv4 Source Guard Logging:  Enable Apply

Port Config

UNIT1 LAGS

| <input type="checkbox"/>            | Port   | Security Type | LAG |
|-------------------------------------|--------|---------------|-----|
| <input checked="" type="checkbox"/> | 1/0/1  | SIP+SMAC      | --  |
| <input checked="" type="checkbox"/> | 1/0/2  | SIP+SMAC      | --  |
| <input checked="" type="checkbox"/> | 1/0/3  | SIP+SMAC      | --  |
| <input type="checkbox"/>            | 1/0/4  | Disable       | --  |
| <input type="checkbox"/>            | 1/0/5  | Disable       | --  |
| <input type="checkbox"/>            | 1/0/6  | Disable       | --  |
| <input type="checkbox"/>            | 1/0/7  | Disable       | --  |
| <input type="checkbox"/>            | 1/0/8  | Disable       | --  |
| <input type="checkbox"/>            | 1/0/9  | Disable       | --  |
| <input type="checkbox"/>            | 1/0/10 | Disable       | --  |

Total: 10 3 entries selected. Cancel Apply

- 3) Kliknij  Save, aby zapisać ustawienia.

## 5.2.4 Przez CLI

- 1) Powiąż ręcznie adres IP, adres MAC, VLAN ID i numer podłączonego portu hosta legalnego, a następnie zastosuj ten wpis do funkcji IP Source Guard.

```
Switch#configure
```

```
Switch(config)#ip source binding legal-host 192.168.0.100 74:d3:45:32:b5:6d vlan 1
interface gigabitEthernet 1/0/1 ip-verify-source
```

- 2) Włącz funkcję dzienników oraz IP Source Guard na portach 1/0/1-3.

```
Switch(config)# ip verify source logging
```

```
Switch(config)# interface range gigabitEthernet 1/0/1-3
```

```
Switch(config-if-range)#ip verify source sip+mac
```

```
Switch(config-if-range)#end
```

```
Switch#copy running-config startup-config
```

### Sprawdzanie konfiguracji

Sprawdzanie wpisu wiązania:

```
Switch#show ip source binding
```

| U | Host  | IP-Addr       | MAC-Addr          | VID | Port    | ACL    | SOURCE |
|---|-------|---------------|-------------------|-----|---------|--------|--------|
| - | ----  | -----         | -----             | --- | ----    | ---    | -----  |
| 1 | User1 | 192.168.0.100 | 74:d3:45:32:b5:6d | 1   | Fa1/0/1 | IP-V-S | Manual |

Notice:

1. Here, 'ARP-D' for 'ARP-Detection', and 'IP-V-S' for 'IP-Verify-Source'.

Sprawdzanie konfiguracji IP Source Guard:

```
Switch#show ip verify source
```

```
IP Source Guard log: Enabled
```

| Port    | Security-Type | LAG |
|---------|---------------|-----|
| Gi1/0/1 | SIP+MAC       | N/A |
| Gi1/0/2 | SIP+MAC       | N/A |
| Gi1/0/3 | SIP+MAC       | N/A |

...

# Część 25

## Konfiguracja IMPB IPv6

### ROZDZIAŁY

1. IMPB IPv6
2. Konfiguracja wiązania IPv6-MAC
3. Konfiguracja funkcji ND Detection
4. Konfiguracja funkcji IPv6 Source Guard
5. Przykłady konfiguracji



# 1 IMPB IPv6

## 1.1 Overview

IMPB (IP-MAC-Port Binding) IPv6 służy do wiązania adresu IPv6, adresu MAC, VLAN ID i numeru połączonego portu określonego hosta. W oparciu o tablicę wiązań przełącznik może zapobiegać atakom ND za pomocą funkcji ND Detection i filtrować pakiety, które nie pasują do wpisów wiązań za pomocą funkcji IPv6 Source Guard.

## 1.2 Obsługiwane funkcje

### Wiązanie IPv6-MAC

Funkcja służy do dodawania wpisów wiązania. Wpisy wiązania mogą być konfigurowane ręcznie lub wyuczone przez funkcje ND Snooping lub DHCPv6 snooping. ND Detection i IPv6 Source Guard bazują na wpisach wiązania IPv6-MAC.

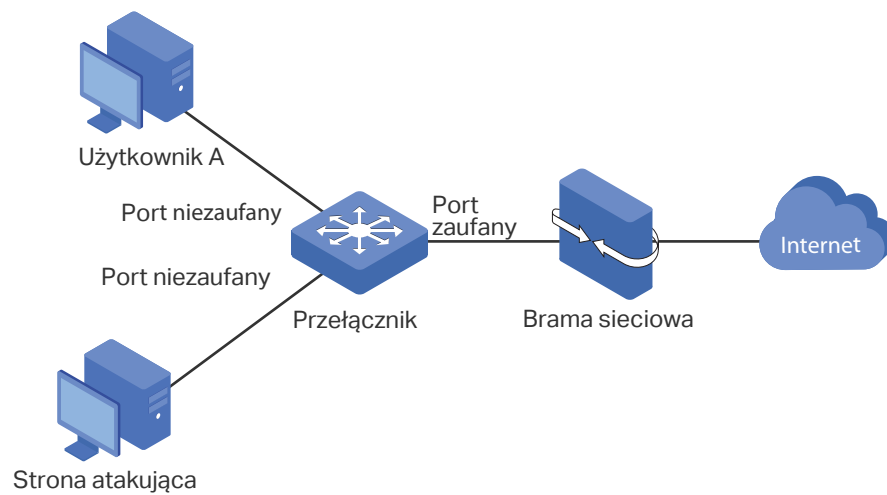
### ND Detection

Ze względu na brak mechanizmu zabezpieczającego, protokół IPv6 ND (Neighbor Discovery) może być z łatwością wykorzystywany przez podmiot atakujący. Funkcja ND detection wykorzystuje wpisy z tablicy wiązania IPv6-MAC do filtrowania sfałszowanych pakietów ND i zapobiegania atakom ND.

Topologia wdrażania ND Detection zaprezentowana jest na poniższym schemacie. Port podłączony do bramy powinien być skonfigurowany jako zaufany, pozostałe porty nie powinny mieć ustawionego trybu zaufania. Poniżej przedstawiono zasady przekierowywania pakietów ND:

- Wszystkie pakiety ND odebrane na porcie zaufanym będą przekierowywane bez sprawdzania.
- Pakiety RS (Router Solicitation) i NS (Neighbor Solicitation) bez wyznaczonych adresów IPv6, jak np. pakiet RS do żądania adresu IPv6 i pakiet NS do wykrywania podwójnych adresów, nie będą sprawdzane na żadnym z dwóch typów portów.
- Pakiety RA (Router Advertisement) i RR (Router Redirect) odebrane na porcie niezaufanym będą bezpośrednio odrzucane. Pozostałe pakiety ND będą sprawdzane. Przełącznik użyje tablicy wiązania IPv6-MAC do porównania adresu IPv6, adresu MAC, VLAN ID i portu odbierającego między wpisem i pakietem ND. W przypadku znalezienia dopasowania, pakiet ND uznawany jest za legalny, pakiet zostanie więc przekierowany. W przypadku braku dopasowania, pakiet ND uznawany jest za nielegalny; pakiet zostanie więc odrzucony.

Rys. 1-1 Topologia sieci ND Detection



### IPv6 Source Guard

Funkcja IPv6 Source Guard służy do filtrowania pakietów IPv6 w oparciu o tablicę wiązania IPv6-MAC. Przekierowywane są jedynie pakiety zgodne z regułami wiązania.

## 2 Konfiguracja wiązania IPv6-MAC

Wpisy wiązania IPv6-MAC można dodawać trzema sposobami:

- poprzez wiązanie ręczne;
- poprzez ND Snooping;
- poprzez DHCPv6 Snooping.

Dodatkowo można wyświetlać, wyszukiwać i edytować wpisy na tablicy wiązania (Binding Table).

### 2.1 Przez GUI

#### 2.1.1 Ręczne wiązanie wpisów

Możesz ręcznie powiązać adres IPv6, adres MAC, VLAN ID i numer portu pod warunkiem, że posiadasz szczegółowe dane hostów.

Wybierz z menu **SECURITY > IPv6 IMPB > IPv6-MAC Binding > Manual Binding** i kliknij **+ Add**, aby wyświetlić poniższą stronę.

Rys. 2-1 Wiązanie ręczne

IP-MAC Binding

Host Name:  (20 characters maximum)

IPv6 Address:  (Format: 2001::1)

MAC Address:  (Format: 00-00-00-00-00-01)

VLAN ID:  (1-4094)

Protect Type: None ▼

Port:  (Format: 1/0/1, input or choose below)

**UNIT1**                      **LAGS**

1

2

3

4

5

6

7

8

9

10

Wykonaj poniższe kroki, aby ręcznie utworzyć wiązanie IPv6-MAC:

- 1) Wprowadź następujące informacje, aby określić hosta.

|              |                                                    |
|--------------|----------------------------------------------------|
| Host Name    | Wprowadź nazwę, aby umożliwić identyfikację hosta. |
| IPv6 Address | Wprowadź adres IPv6.                               |
| MAC Address  | Wprowadź adres MAC.                                |
| VLAN ID      | Wprowadź VLAN ID.                                  |

- 2) Wybierz typ ochrony wpisu.

|              |                                                                                                                                                                                                                                                                                                                                                                                                                        |
|--------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Protect Type | <p>Wybierz typ ochrony wpisu. Wpis będzie zastosowany do wybranej funkcji. Dostępne są następujące opcje:</p> <p><b>None:</b> Wpis nie będzie zastosowany do żadnej funkcji.</p> <p><b>ND Detection:</b> Wpis zostanie zastosowany do funkcji ND Detection.</p> <p><b>IPv6 Source Guard:</b> Wpis zostanie zastosowany do funkcji IPv6 Source Guard.</p> <p><b>Both:</b> Wpis zostanie zastosowany do obu funkcji.</p> |
|--------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

- 3) Wpisz lub wybierz port podłączony do tego hosta.

- 4) Kliknij **Apply**.

## 2.1.2 Wiązanie wpisów poprzez ND Snooping

Przy włączonej funkcji ND Snooping przełącznik monitoruje pakiety ND i zapisuje adresy IPv6, adresy MAC, VLAN ID i numery portów połączonych z hostami IPv6. Możesz dogodnie powiązać wpisy.

### Uwaga:

Przed włączeniem tej funkcji upewnij się, że sieć jest bezpieczna, i że aktualnie nie występują ataki ND na hosty. W przeciwnym wypadku możesz uzyskać błędne wpisy wiązania IPv6-MAC. Jeżeli sieć jest atakowana, zaleca się przeprowadzenie ręcznego wiązania wpisów.

Wybierz z menu **SECURITY > IPv6 IMPB > IPv6-MAC Binding > ND Snooping**, aby wyświetlić poniższą stronę.

Rys. 2-2 ND Snooping

### ND Snooping

ND Snooping:  Enable Apply

---

### VLAN Config

Filter by VLAN: From  To  Apply

| <input type="checkbox"/>            | VLAN ID | Status   |
|-------------------------------------|---------|----------|
| <input checked="" type="checkbox"/> | 1       | Disabled |
| <input type="checkbox"/>            | 6       | Disabled |

Total: 2 1 entry selected. Cancel Apply

---

### Port Config

UNIT1

LAGS

| <input type="checkbox"/>            | Port   | Maximum Entries | LAG |
|-------------------------------------|--------|-----------------|-----|
| <input checked="" type="checkbox"/> | 1/0/1  | 512             | --- |
| <input type="checkbox"/>            | 1/0/2  | 512             | --- |
| <input type="checkbox"/>            | 1/0/3  | 512             | --- |
| <input type="checkbox"/>            | 1/0/4  | 512             | --- |
| <input type="checkbox"/>            | 1/0/5  | 512             | --- |
| <input type="checkbox"/>            | 1/0/6  | 512             | --- |
| <input type="checkbox"/>            | 1/0/7  | 512             | --- |
| <input type="checkbox"/>            | 1/0/8  | 512             | --- |
| <input type="checkbox"/>            | 1/0/9  | 512             | --- |
| <input type="checkbox"/>            | 1/0/10 | 512             | --- |

Total: 10 1 entry selected. Cancel Apply

Wykonaj poniższe kroki, aby skonfigurować wiązanie IPv6-MAC poprzez ND Snooping:

- 1) W sekcji **ND Snooping** włącz ND Snooping i kliknij **Apply**.
- 2) W sekcji **VLAN Config** wybierz co najmniej jeden VLAN i włącz ND Snooping. Kliknij **Apply**.

VLAN ID                      Informacja o VLAN ID.

Status                        Włącz lub wyłącz ND Snooping w sieci VLAN.

- 3) W sekcji **Port Config** skonfiguruj maks. liczbę wpisów, których port może wyuczyć się przez ND snooping. Kliknij **Apply**.

Port                            Informacja o numerze portu.

|                 |                                                                                   |
|-----------------|-----------------------------------------------------------------------------------|
| Maximum Entries | Skonfiguruj maks. liczbę wpisów, których port może wyuczyc się przez ND Snooping. |
| LAG             | Informacja o grupie LAG, do której należy port.                                   |

- 4) Wyuczone wpisy będą wyświetlane na tablicy wiązań. Aby wyświetlić lub edytować wpisy, idź do **SECURITY > IPv6 IMPB > IPv6-MAC Binding > Binding Table**.

### 2.1.3 Wiązanie wpisów przez DHCPv6 Snooping

Przy włączonej funkcji DHCPv6 Snooping przełącznik może monitorować proces przyjmowania przez host adresu IPv6 i zarejestrować adres IP, adres MAC, VLAN ID i numer podłączonego portu hosta.

Wybierz z menu **SECURITY > IPv6 IMPB > IPv6-MAC Binding > DHCPv6 Snooping**, aby wyświetlić poniższą stronę.

Rys. 2-3 DHCPv6 Snooping

Global Config

DHCPv6 Snooping:  Enable Apply

---

VLAN Config

Filter by VLAN: From  To  Apply

| <input type="checkbox"/>            | VLAN ID | Status   |
|-------------------------------------|---------|----------|
| <input checked="" type="checkbox"/> | 1       | Disabled |
| <input type="checkbox"/>            | 6       | Disabled |

Total: 2 1 entry selected. Cancel Apply

---

Port Config

**UNIT1** | LAGS

| <input type="checkbox"/>            | Port   | Maximum Entries | LAG |
|-------------------------------------|--------|-----------------|-----|
| <input checked="" type="checkbox"/> | 1/0/1  | 512             | --- |
| <input type="checkbox"/>            | 1/0/2  | 512             | --- |
| <input type="checkbox"/>            | 1/0/3  | 512             | --- |
| <input type="checkbox"/>            | 1/0/4  | 512             | --- |
| <input type="checkbox"/>            | 1/0/5  | 512             | --- |
| <input type="checkbox"/>            | 1/0/6  | 512             | --- |
| <input type="checkbox"/>            | 1/0/7  | 512             | --- |
| <input type="checkbox"/>            | 1/0/8  | 512             | --- |
| <input type="checkbox"/>            | 1/0/9  | 512             | --- |
| <input type="checkbox"/>            | 1/0/10 | 512             | --- |

Total: 10 1 entry selected. Cancel Apply

Wykonaj poniższe kroki, aby skonfigurować wiązanie IPv6-MAC poprzez DHCPv6 Snooping:

- 1) W sekcji **Global Config** włącz DHCPv6 Snooping globalnie. Kliknij **Apply**.
- 2) W sekcji **VLAN Config** włącz DHCPv6 Snooping w sieci VLAN lub w kilku sieciach VLAN. Kliknij **Apply**.

|         |                                                |
|---------|------------------------------------------------|
| VLAN ID | Informacja o VLAN ID.                          |
| Status  | Włącz lub wyłącz DHCPv6 Snooping w sieci VLAN. |

- 3) W sekcji **Port Config** skonfiguruj maks. liczbę wpisów wiązania, których może nauczyć się port przez DHCPv6 Snooping. Kliknij **Apply**.

|                 |                                                                                                |
|-----------------|------------------------------------------------------------------------------------------------|
| Port            | Informacja o numerze portu.                                                                    |
| Maximum Entries | Skonfiguruj maks. liczbę wpisów wiązania, których może nauczyć się port przez DHCPv6 Snooping. |
| LAG             | Informacja o grupie LAG, do której należy port.                                                |

- 4) Wyuczony wpis będą wyświetlane na tablicy wiązań. Aby wyświetlić lub edytować wpisy, idź do **SECURITY > IPv6 IMPB > IP-MAC Binding > Binding Table**.

## 2.1.4 Wyświetlanie wpisów wiązania

Na tablicy wiązań możesz wyświetlić, wyszukać lub edytować wybrane wpisy wiązania.

Wybierz z menu **SECURITY > IPv6 IMPB > IPv6-MAC Binding > Binding Table**, aby wyświetlić poniższą stronę.

Rys. 2-4 Binding Table

Binding Table

Source:

IP Address:  (Format: 2001::1)

| <input checked="" type="checkbox"/> | Host Name | IP Address | MAC Address       | VLAN ID | Port  | Protect Type | Source |
|-------------------------------------|-----------|------------|-------------------|---------|-------|--------------|--------|
| <input checked="" type="checkbox"/> | host1     | 2001::3    | aa-bb-cc-dd-ee-ff | 1       | 1/0/2 | ND Detection | Manual |

1 entry selected.

Możesz ustawić kryteria wyszukiwania wpisów.

|        |                                                                                                                                                                                                                                                                                                                                                              |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Source | Wybierz źródło wpisu i kliknij <b>Search</b> .<br><br><b>All:</b> Wyświetlanie wpisów ze wszystkich źródeł.<br><br><b>Manual Binding:</b> Wyświetlanie wpisów powiązanych ręcznie.<br><br><b>ND Snooping:</b> Wyświetlanie wpisów wiązania wyuczonych z ND Snooping.<br><br><b>DHCPv6 Snooping:</b> Wyświetlanie wpisów wiązania wyuczonych z DHCP Snooping. |
| IP     | Wpisz adres IP i kliknij <b>Search</b> , aby wyszukać konkretny wpis.                                                                                                                                                                                                                                                                                        |

Dodatkowo wybierz co najmniej jeden wpis, aby edytować nazwę hosta i typ ochrony. Kliknij **Apply**.

|              |                                                                                                                                                                                                                                                                                                                                                                                                                              |
|--------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Host Name    | Wpisz nazwę, aby umożliwić identyfikację hosta.                                                                                                                                                                                                                                                                                                                                                                              |
| IP Address   | Informacja o adresie IPv6.                                                                                                                                                                                                                                                                                                                                                                                                   |
| MAC Address  | Informacja o adresie MAC.                                                                                                                                                                                                                                                                                                                                                                                                    |
| VLAN ID      | Informacja o VLAN ID.                                                                                                                                                                                                                                                                                                                                                                                                        |
| Port         | Informacja o numerze portu.                                                                                                                                                                                                                                                                                                                                                                                                  |
| Protect Type | Wybierz typ ochrony wpisu. Wpis będzie zastosowany do wybranej funkcji. Dostępne są następujące opcje:<br><br><b>None (żadna):</b> Wpis nie będzie zastosowany do żadnej funkcji.<br><br><b>ND Detection:</b> Wpis zostanie zastosowany do funkcji ND Detection.<br><br><b>IPv6 Source Guard:</b> Wpis zostanie zastosowany do funkcji IP Source Guard.<br><br><b>Both (obie):</b> Wpis zostanie zastosowany do obu funkcji. |
| Source       | Informacja o źródle wpisu.                                                                                                                                                                                                                                                                                                                                                                                                   |

## 2.2 Przez CLI

Poniższe sekcje prezentują, jak powiązać wpisy ręcznie, przez ND Snooping i przez DHCP Snooping, oraz jak wyświetlać wpisy wiązania.

### 2.2.1 Ręczne wiązanie wpisów

Możesz ręcznie powiązać adres IPv6, adres MAC, VLAN ID i numer portu pod warunkiem, że posiadasz szczegółowe dane hostów.

Wykonaj poniższe kroki, aby ręcznie powiązać wpisy:



|        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Krok 1 | <b>configure</b><br>Uruchom tryb konfiguracji globalnej.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Krok 2 | <b>ipv6 source binding</b> <i>hostname ipv6-addr mac-addr vlan vlan-id interface { fastEthernet port   gigabitEthernet port   ten-gigabitEthernet port   port-channel port-channel-id } { none   nd-detection   ipv6-verify-source   both }</i><br><br>Ręcznie powiąż nazwę hosta, adres IP, adres MAC, VLAN ID i numer portu hosta oraz skonfiguruj typ ochrony hosta.<br><br><i>hostname</i> : Wyznacz nazwę hosta, składającą się z maks. 20 znaków.<br><br><i>ipv6-addr</i> : Wpisz adres IPv6 hosta.<br><br><i>mac-addr</i> : Wpisz adres MAC hosta w formacie xx:xx:xx:xx:xx:xx.<br><br><i>vlan-id</i> : Wpisz VLAN ID hosta.<br><br><i>port</i> : Wpisz numer portu, do którego podłączony jest host.<br><br><i>none   nd-detection   ipv6-verify-source   both</i> : Wyznacz typ ochrony wpisu. „None” oznacza, że wpis nie będzie zastosowany do żadnej funkcji; „nd-detection” oznacza, że wpis zostanie zastosowany do funkcji ND Detection; „ipv6-verify-source” oznacza, że wpis zostanie zastosowany do IP Source Guard; „Both” oznacza, że wpis będzie zastosowany do obu funkcji |
| Krok 3 | <b>show ip source binding</b><br>Sprawdź wpis wiązania.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Krok 4 | <b>end</b><br>Powróć do trybu privileged EXEC.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Krok 5 | <b>copy running-config startup-config</b><br>Zapisz ustawienia w pliku konfiguracyjnym.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |

Poniższy przykład prezentuje wiązanie wpisu z nazwą hosta host1, adresem IPv6 2001:0:9d38:90d5::34, adresem MAC AA-BB-CC-DD-EE-FF, VLAN ID 10, portem numer 1/0/5 i włączanie dla wpisu funkcji ND Detection.

### Switch#configure

```
Switch(config)#ipv6 source binding host1 2001:0:9d38:90d5::34 aa:bb:cc:dd:ee:ff vlan 10
interface gigabitEthernet 1/0/5 nd-detection
```

### Switch(config)#show ipv6 source binding

| U | Host  | IP-Addr              | MAC-Addr          | VID | Port    | ACL  | Source |
|---|-------|----------------------|-------------------|-----|---------|------|--------|
| - | ----  | -----                | -----             | --- | ----    | ---  | -----  |
| 1 | host1 | 2001:0:9d38:90d5::34 | aa:bb:cc:dd:ee:ff | 10  | Gi1/0/5 | ND-D | Manual |

### Switch(config)#end

### Switch#copy running-config startup-config

## 2.2.2 Wiązanie wpisów poprzez ND Snooping

Wykonaj poniższe kroki, aby powiązać wpisy poprzez ND Snooping:

|        |                                                                                                                                                                                                                                                                                                                                              |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Krok 1 | <b>configure</b><br>Uruchom tryb konfiguracji globalnej.                                                                                                                                                                                                                                                                                     |
| Krok 2 | <b>ipv6 nd snooping</b><br>Włącz ND Snooping globalnie.                                                                                                                                                                                                                                                                                      |
| Krok 3 | <b>ipv6 nd snooping vlan <i>vlan-range</i></b><br>Włącz ND Snooping w wyznaczonym VLAN.<br><br><i>vlan-range</i> : Wpisz zakres VLAN w formacie 1-3, 5.                                                                                                                                                                                      |
| Krok 4 | <b>interface { fastEthernet <i>port</i>   range fastEthernet <i>port-list</i>   gigabitEthernet <i>port</i>   range gigabitEthernet <i>port-list</i>   ten-gigabitEthernet <i>port</i>   range ten-gigabitEthernet <i>port-list</i> }</b><br>Wejdź w tryb konfiguracji interfejsu.                                                           |
| Krok 5 | <b>ipv6 nd snooping max-entries <i>value</i></b><br>Skonfiguruj maks. liczbę wpisów wiązania ND, których port może nauczyć się przez ND snooping.<br><br><i>value</i> : Wpisz maks. dopuszczalną liczbę wpisów wiązania ND, których port może nauczyć się przez ND snooping. Wartość powinna wynosić od 0 do 1024, wartość domyślna to 1024. |
| Krok 6 | <b>show ipv6 nd snooping</b><br>Sprawdź konfigurację globalną IPv6 ND Snooping                                                                                                                                                                                                                                                               |
| Krok 7 | <b>show ipv6 nd snooping interface { fastEthernet <i>port</i>   gigabitEthernet <i>port</i>   ten-gigabitEthernet <i>port</i> }</b><br>Sprawdź konfigurację IPv6 ND Snoopinga w wyznaczonym porcie.                                                                                                                                          |
| Krok 8 | <b>end</b><br>Powróć do trybu privileged EXEC.                                                                                                                                                                                                                                                                                               |
| Krok 9 | <b>copy running-config startup-config</b><br>Zapisz ustawienia w pliku konfiguracyjnym.                                                                                                                                                                                                                                                      |

Poniższy przykład prezentuje globalne włączanie ND Snooping we VLAN 1.

```
Switch#configure
```

```
Switch(config)#ipv6 nd snooping
```

```
Switch(config)#ipv6 nd snooping vlan 1
```

```
Switch(config)#show ipv6 nd snooping
```

```
Global Status: Enable
```

VLAN ID: 1

**Switch(config)#end**

**Switch#copy running-config startup-config**

Poniższy przykład przedstawia sposób konfiguracji maksymalnej liczby wpisów zapamiętywanych na porcie 1/0/1:

**Switch#configure**

**Switch(config)#interface gigabitEthernet 1/0/1**

**Switch(config-if)#ipv6 nd snooping max-entries 1000**

**Switch(config-if)#show ipv6 nd snooping interface gigabitEthernet 1/0/1**

```
Interface max-entries LAG
----- -
Gi1/0/1 1000 N/A
```

**Switch(config-if)#end**

**Switch#copy running-config startup-config**

## 2.2.3 Wiązanie wpisów poprzez DHCPv6 Snooping

Wykonaj poniższe kroki, aby powiązać wpisy poprzez DHCPv6 Snooping:

|        |                                                                                                                                                                                                                                                                                                                                                                                               |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Krok 1 | <b>configure</b><br>Uruchom tryb konfiguracji globalnej.                                                                                                                                                                                                                                                                                                                                      |
| Krok 2 | <b>ipv6 dhcp snooping</b><br>Włącz DHCPv6 Snooping globalnie.                                                                                                                                                                                                                                                                                                                                 |
| Krok 3 | <b>ipv6 dhcp snooping vlan <i>vlan-range</i></b><br>Włącz DHCPv6 Snooping w wyznaczonym VLAN.<br><br><i>vlan-range</i> : Wpisz zakres VLAN w formacie 1-3, 5.                                                                                                                                                                                                                                 |
| Krok 4 | <b>interface { fastEthernet <i>port</i>   range fastEthernet <i>port-list</i>   gigabitEthernet <i>port</i>   range gigabitEthernet <i>port-list</i>   ten-gigabitEthernet <i>port</i>   range ten-gigabitEthernet <i>port-list</i>   interface port-channel <i>port-channel-id</i>   interface range port-channel <i>port-channel-id-list</i> }</b><br>Wejdź w tryb konfiguracji interfejsu. |
| Krok 5 | <b>ipv6 dhcp snooping max-entries <i>value</i></b><br>Skonfiguruj maks. liczbę wpisów wiązania, których port może nauczyć się przez DHCPv6 snooping.<br><br><i>value</i> : Wpisz maks. dopuszczalną liczbę wpisów. Wartość powinna wynosić od 0 do 512.                                                                                                                                       |

---

|        |                                                                                         |
|--------|-----------------------------------------------------------------------------------------|
| Krok 6 | <b>show ip dhcp snooping</b><br>Sprawdź konfigurację globalną DHCPv6 Snooping.          |
| Krok 7 | <b>end</b><br>Powróć do trybu privileged EXEC.                                          |
| Krok 8 | <b>copy running-config startup-config</b><br>Zapisz ustawienia w pliku konfiguracyjnym. |

---

Poniższy przykład prezentuje globalne włączenie DHCPv6 Snooping we VLAN 5 i ustawianie maks. liczby wpisów wiązania, których może nauczyć się port 1/0/1 przez DHCPv6 Snooping na 100:

**Switch#configure**

**Switch(config)#ipv6 dhcp snooping**

**Switch(config)#ipv6 dhcp snooping vlan 5**

**Switch(config)#interface gigabitEthernet 1/0/1**

**Switch(config-if)#ipv6 dhcp snooping max-entries 100**

**Switch(config-if)#show ipv6 dhcp snooping**

Global Status: Enable

VLAN ID: 5

**Switch(config-if)#show ipv6 dhcp snooping interface gigabitEthernet 1/0/1**

Interface max-entries LAG

```
----- ----- ---
Gi1/0/1 100 N/A
```

**Switch(config-if)#end**

**Switch#copy running-config startup-config**

## 2.2.4 Wyświetlanie wpisów wiązania

W trybie privileged EXEC, tak jak i w każdym innym trybie konfiguracji, możesz wyświetlać wpisy wiązania, korzystając z poniższego polecenia:

**show ipv6 source binding**

Wyświetl dane wpisów wiązania (nazwa hosta, adres IP, adres MAC, VLAN ID, numer portu, typ ochrony).

---

# 3 Konfiguracja funkcji ND Detection

Aby przeprowadzić konfigurację funkcji ND Detection, wykonaj poniższe kroki:

- 1) Dodaj wpisy wiązania IPv6-MAC.
- 2) Włącz ND Detection.
- 3) Skonfiguruj ND Detection na portach.
- 4) Sprawdź statystyki ND.

## 3.1 Przez GUI

### 3.1.1 Dodawanie wpisów wiązania IPv6-MAC

Funkcja ND Detection polega na wykrywaniu przez przełącznik pakietów ND w oparciu o wpisy wiązania na tablicy wiązania IPv6-MAC (IP-MAC Binding Table) i filtrowaniu nielegalnych pakietów ND. Przed konfiguracją funkcji ND Detection należy przeprowadzić konfigurację wiązania IPv6-MAC. Więcej informacji na ten temat znajdziesz w części *Konfiguracja wiązania IPv6-MAC*.

### 3.1.2 Włączanie funkcji ND Detection

Wybierz z menu **SECURITY > IPv6 IMPB > ND Detection > Global Config**, aby wyświetlić poniższą stronę.

Rys. 3-1 Globalna konfiguracja ND Detection

Global Config

---

ND Detection:  Enable Apply

VLAN Config

|                                     | VLAN ID | Status            | Log Status                                                                                                                                                                                        |
|-------------------------------------|---------|-------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <input checked="" type="checkbox"/> | 1       | Disabled          | Disabled                                                                                                                                                                                          |
| <input type="checkbox"/>            | 8       | Disabled          | Disabled                                                                                                                                                                                          |
| Total: 2                            |         | 1 entry selected. | <span style="border: 1px solid #00a651; padding: 2px 10px; color: white;">Cancel</span> <span style="border: 1px solid #00a651; padding: 2px 10px; color: white; margin-left: 10px;">Apply</span> |

Wykonaj poniższe kroki, aby włączyć ND Detection:

- 1) W sekcji **Global Config** włącz ND Detection i skonfiguruj powiązane parametry. Kliknij **Apply**.

---

ND Detection      Włącz lub wyłącz ND Detection globalnie.

---

- 2) W sekcji **VLAN Config** włącz ND Detection w wybranych sieciach VLAN. Kliknij **Apply**.

|            |                                                                                                                                                                               |
|------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| VLAN ID    | Informacja o VLAN ID.                                                                                                                                                         |
| Status     | Włącz lub wyłącz ND Detection w sieci VLAN.                                                                                                                                   |
| Log Status | Włącz lub wyłącz w sieci VLAN Log Feature (funkcja rejestru zdarzeń). Jeżeli funkcja jest włączona, przełącznik po odrzuceniu nielegalnego pakietu ND będzie generował zapis. |

### 3.1.3 Konfiguracja funkcji ND Detection na portach

Wybierz z menu **SECURITY > IPv6 IMPB > ND Detection > Port Config**, aby wyświetlić poniższą stronę.

Rys. 3-2 ND Detection na portach

The screenshot shows the 'Port Config' window with two tabs: 'UNIT1' and 'LAGS'. Below the tabs is a table with columns: 'Port', 'Trust Status', and 'LAG'. The table lists ports 1/0/1 through 1/0/10. Port 1/0/1 is selected with a checked checkbox. All 'Trust Status' values are 'Disabled'. The 'LAG' column contains dashes. At the bottom, there is a summary bar showing 'Total: 10' and '1 entry selected.', along with 'Cancel' and 'Apply' buttons.

| Port                                      | Trust Status | LAG |
|-------------------------------------------|--------------|-----|
| <input checked="" type="checkbox"/> 1/0/1 | Disabled     | --- |
| <input type="checkbox"/> 1/0/2            | Disabled     | --- |
| <input type="checkbox"/> 1/0/3            | Disabled     | --- |
| <input type="checkbox"/> 1/0/4            | Disabled     | --- |
| <input type="checkbox"/> 1/0/5            | Disabled     | --- |
| <input type="checkbox"/> 1/0/6            | Disabled     | --- |
| <input type="checkbox"/> 1/0/7            | Disabled     | --- |
| <input type="checkbox"/> 1/0/8            | Disabled     | --- |
| <input type="checkbox"/> 1/0/9            | Disabled     | --- |
| <input type="checkbox"/> 1/0/10           | Disabled     | --- |

Wykonaj poniższe kroki, aby skonfigurować ND Detection na portach:

- 1) Wybierz co najmniej jeden port i skonfiguruj odpowiednie parametry.

|              |                                                                                                                                                                                                                                              |
|--------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Port         | Informacja o numerze portu.                                                                                                                                                                                                                  |
| Trust Status | Włącz lub wyłącz dla tego portu status portu zaufanego. Na porcie zaufanym pakiety ARP przekierowywane są bezpośrednio, bez sprawdzania. Zaleca się ustawienie portów niektórych typów, np. portów uplink czy portów routingu, jako zaufane. |
| LAG          | Informacja o grupie LAG, do której należy port..                                                                                                                                                                                             |

- 2) Kliknij **Apply**.

### 3.1.4 Wyświetlanie statystyk ND

Możesz zobaczyć liczbę nielegalnych pakietów ND otrzymanych na każdym porcie. Ułatwi to zlokalizowanie przyczyny wadliwego działania sieci i podjęcie odpowiednich środków dla zabezpieczenia sieci..

Wybierz z menu **SECURITY > IPv6 IMPB > ND Detection > ND Statistics**, aby wyświetlić poniższą stronę.

Rys. 3-3 Statystyki ND

**Auto Refresh**

---

Auto Refresh:  Enable Apply

**Illegal ND Packets**

↻ Refresh ✕ Clear

| VLAN ID  | Forwarded | Dropped |
|----------|-----------|---------|
| 1        | 0         | 0       |
| 8        | 0         | 0       |
| Total: 2 |           |         |

W sekcji **Auto Refresh** możesz włączyć funkcję automatycznego odświeżania i wyznaczyć odstęp czasu, w którym strona internetowa będzie automatycznie odświeżana.

W sekcji **Illegal ND Packet** możesz sprawdzić liczbę nielegalnych pakietów ND w każdej sieci VLAN.

|           |                                                                 |
|-----------|-----------------------------------------------------------------|
| VLAN ID   | Informacja o VLAN ID.                                           |
| Forwarded | Informacja o liczbie przekazanych pakietów ND w tej sieci VLAN. |
| Dropped   | Informacja o liczbie odrzuconych pakietów ND w tej sieci VLAN.  |

## 3.2 Przez CLI

### 3.2.1 Dodawanie wpisów wiązania IPv6-MAC

Funkcja ND Detection polega na wykrywaniu przez przełącznik pakietów ND w oparciu o wpisy wiązania na tablicy wiązania IPv6-MAC (IP-MAC Binding Table) i filtrowaniu nielegalnych pakietów ND. Przed konfiguracją funkcji ND Detection należy przeprowadzić konfigurację wiązania IPv6-MAC. Więcej informacji na ten temat znajdziesz w części *Konfiguracja wiązania IPv6-MAC*.

## 3.2.2 Włączanie funkcji ND Detection

Wykonaj poniższe kroki, aby włączyć ND Detection:

|        |                                                                                                                                                                                                                                                                      |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Krok 1 | <b>configure</b><br>Uruchom tryb konfiguracji globalnej.                                                                                                                                                                                                             |
| Krok 2 | <b>ipv6 nd detection</b><br>Włącz funkcję ND Detection globalnie.                                                                                                                                                                                                    |
| Krok 3 | <b>ipv6 nd detection vlan <i>vlan-range</i></b><br>Włącz ND Detection w wybranej sieci VLAN.<br><br><i>vlan-range</i> : Wpisz zakres VLAN w formacie 1-3, 5.                                                                                                         |
| Krok 4 | <b>ipv6 nd detection vlan <i>vlan-range</i> logging</b><br>(Opcjonalnie) Włącz funkcję Log feature (funkcja rejestru zdarzeń, aby przełącznik po odrzuceniu nielegalnego pakietu ND generował zapis.<br><br><i>vlan-range</i> : Wpisz zakres VLAN w formacie 1-3, 5. |
| Krok 5 | <b>show ipv6 nd detection</b><br>Sprawdź ustawienia globalne ND Detection.                                                                                                                                                                                           |
| Krok 6 | <b>end</b><br>Powróć do trybu privileged EXEC.                                                                                                                                                                                                                       |
| Krok 7 | <b>copy running-config startup-config</b><br>Zapisz ustawienia w pliku konfiguracyjnym.                                                                                                                                                                              |

Poniższy przykład prezentuje globalne włączanie ND Detection we VLAN 1:

```
Switch#configure
```

```
Switch(config)#ipv6 nd detection
```

```
Switch(config)#ipv6 nd detection vlan 1
```

```
Switch(config)#show ipv6 nd detection
```

```
Global Status: Enable
```

```
Switch(config)#show ipv6 nd detection vlan
```

```
VID Enable status Log Status
```

```
---- -
```

```
1 Enable Disable
```

```
Switch(config)#end
```

```
Switch#copy running-config startup-config
```



### 3.2.3 Konfiguracja funkcji ND Detection na portach

Wykonaj poniższe kroki, aby skonfigurować ND Detection na portach:

|        |                                                                                                                                                                                                                                                                                    |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Krok 1 | <b>configure</b><br>Uruchom tryb konfiguracji globalnej.                                                                                                                                                                                                                           |
| Krok 2 | <b>interface { fastEthernet <i>port</i>   range fastEthernet <i>port-list</i>   gigabitEthernet <i>port</i>   range gigabitEthernet <i>port-list</i>   ten-gigabitEthernet <i>port</i>   range ten-gigabitEthernet <i>port-list</i> }</b><br>Uruchom tryb konfiguracji interfejsu. |
| Krok 3 | <b>ipv6 nd detection trust</b><br>Ustaw port jako zaufany, który nie będzie objęty działaniem funkcji ND Detection. Zaleca się ustawienie portów niektórych typów, np. portów uplink czy portów routingu, jako zaufane.                                                            |
| Krok 4 | <b>show ipv6 nd detection interface { fastEthernet <i>port</i>   gigabitEthernet <i>port</i>   ten-gigabitEthernet <i>port</i>   port-channel <i>port-channel-id</i> }</b><br>Sprawdź globalną konfigurację ND Detection na porcie.                                                |
| Krok 5 | <b>end</b><br>Powróć do trybu privileged EXEC.                                                                                                                                                                                                                                     |
| Krok 6 | <b>copy running-config startup-config</b><br>Zapisz ustawienia w pliku konfiguracyjnym.                                                                                                                                                                                            |

Poniższy przykład prezentuje konfigurację portu 1/0/1 jako zaufanego:

```
Switch#configure
```

```
Switch(config)#interface gigabitEthernet 1/0/1
```

```
Switch(config-if)#ipv6 nd detection trust
```

```
Switch(config-if)#show ipv6 nd detection interface gigabitEthernet 1/0/1
```

```
Interface Trusted LAG
```

```

```

```
Gi1/0/1 Enable N/A
```

```
Switch(config-if)#end
```

```
Switch#copy running-config startup-config
```

### 3.2.4 Wyświetlanie statystyk ND

W trybie użytkownika uprzywilejowanego (privileged EXEC mode), tak jak i w każdym innym trybie konfiguracji, możesz wyświetlać wpisy wiązania, korzystając z poniższego polecenia:

**show ipv6 nd detection statistics**

Wyświetl statystyki ND dla każdego portu (liczba przekazanych pakietów ND, liczba odrzuconych pakietów ND).

---

# 4 Konfiguracja funkcji IPv6 Source Guard

Aby przeprowadzić konfigurację IPv6 Source Guard, wykonaj poniższe kroki:

- 1) Dodaj wpisy wiązania IP-MAC.
- 2) Skonfiguruj funkcję IPv6 Source Guard.

## 4.1 Przez GUI

### 4.1.1 Dodawanie wpisów wiązania IPv6-MAC

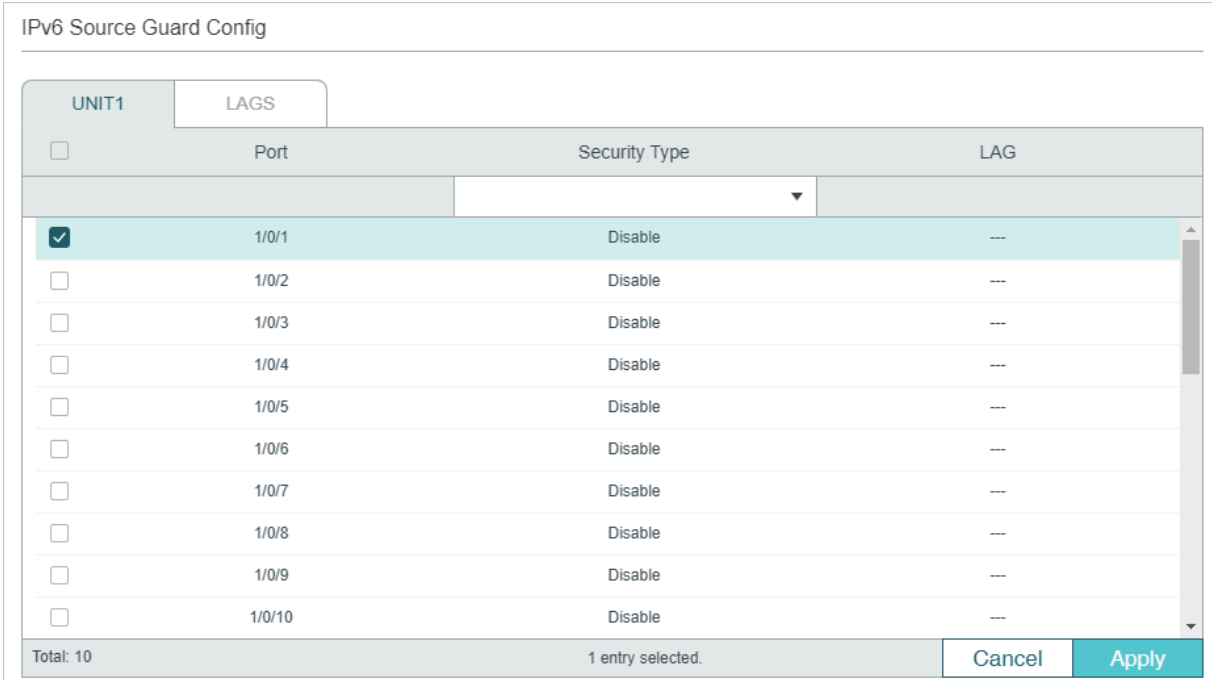
Funkcja ND Detection polega na wykrywaniu przez przełącznik pakietów ND w oparciu o wpisy wiązania na tablicy wiązania IPv6-MAC (IP-MAC Binding Table) i filtrowaniu nielegalnych pakietów ND. Przed konfiguracją funkcji ND Detection należy przeprowadzić konfigurację wiązania IPv6-MAC. Więcej informacji na ten temat znajdziesz w części *Konfiguracja wiązania IPv6-MAC*.

### 4.1.2 Konfiguracja funkcji IPv6 Source Guard

Przed konfiguracją funkcji IPv6 Source Guard należy skonfigurować szablon (SDM template) jako EnterpriseV6.

Wybierz z menu **SECURITY > IPv6 IMPB > IPv6 Source Guard**, aby wyświetlić poniższą stronę.

Rys. 4-1 Konfiguracja IPv6 Source Guard



| <input type="checkbox"/>            | Port   | Security Type | LAG |
|-------------------------------------|--------|---------------|-----|
| <input checked="" type="checkbox"/> | 1/0/1  | Disable       | --- |
| <input type="checkbox"/>            | 1/0/2  | Disable       | --- |
| <input type="checkbox"/>            | 1/0/3  | Disable       | --- |
| <input type="checkbox"/>            | 1/0/4  | Disable       | --- |
| <input type="checkbox"/>            | 1/0/5  | Disable       | --- |
| <input type="checkbox"/>            | 1/0/6  | Disable       | --- |
| <input type="checkbox"/>            | 1/0/7  | Disable       | --- |
| <input type="checkbox"/>            | 1/0/8  | Disable       | --- |
| <input type="checkbox"/>            | 1/0/9  | Disable       | --- |
| <input type="checkbox"/>            | 1/0/10 | Disable       | --- |

Total: 10      1 entry selected.

Wykonaj poniższe kroki, aby skonfigurować IPv6 Source Guard:

- 1) Wybierz co najmniej jeden port i skonfiguruj typ ochrony.

|               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|---------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Port          | Informacja o numerze portu.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Security Type | <p>Wybierz tryb ochrony na porcie dla pakietów IPv6. Dostępne są następujące opcje:</p> <p><b>Disable (wył.):</b> Funkcja IP Source Guard jest wyłączona na porcie.</p> <p><b>SIP+MAC:</b> Przetwarzane mogą być jedynie pakiety ze źródłowym adresem IPv6, źródłowym adresem MAC i numerem portu dopasowanym do reguł wiązania IPv6-MAC. Pozostałe pakiety będą odrzucane.</p> <p><b>SIP:</b> Przetwarzane mogą być jedynie pakiety ze źródłowym adresem IPv6 i numerem portu dopasowanym do reguł wiązania IPv6-MAC. Pozostałe pakiety będą odrzucane.</p> |
| LAG           | Informacja o grupie LAG, do której należy port.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |

- 2) Kliknij **Apply**.

## 4.2 Przez CLI

### 4.2.1 Dodawanie wpisów wiązania IPv6-MAC

Funkcja ND Detection polega na wykrywaniu przez przełącznik pakietów ND w oparciu o wpisy wiązania na tablicy wiązania IPv6-MAC (IP-MAC Binding Table) i filtrowaniu nielegalnych pakietów ND. Przed konfiguracją funkcji ND Detection należy przeprowadzić konfigurację wiązania IPv6-MAC. Więcej informacji na ten temat znajdziesz w części *Konfiguracja wiązania IPv6-MAC*.

### 4.2.2 Konfiguracja funkcji IPv6 Source Guard

Przed konfiguracją funkcji IPv6 Source Guard należy skonfigurować szablon (SDM template) jako EnterpriseV6.

Wykonaj poniższe kroki, aby skonfigurować IPv6 Source Guard:

|        |                                                                                                                                                                                                                                                     |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Krok 1 | <p><b>configure</b></p> <p>Uruchom tryb konfiguracji globalnej.</p>                                                                                                                                                                                 |
| Krok 2 | <p><b>interface { fastEthernet port   range fastEthernet port-list   gigabitEthernet port   range gigabitEthernet port-list   ten-gigabitEthernet port   range ten-gigabitEthernet port-list }</b></p> <p>Uruchom tryb konfiguracji interfejsu.</p> |

- 
- Krok 3      **ipv6 verify source { sipv6+mac | sipv6 }**  
 Włącz IP Source Guard dla pakietów IPv6.  
 sipv6+mac: Przetwarzane mogą być jedynie pakiety ze źródłowym adresem IPv6, źródłowym adresem MAC i numerem portu dopasowanym do reguł wiązania IPv6-MAC. Pozostałe pakiety będą odrzucane.
- 
- Krok 4      **show ipv6 verify source [ interface { fastEthernet port | gigabitEthernet port | ten-gigabitEthernet port | port-channel port-channel-id } ]**  
 Sprawdź konfigurację IP Source Guard dla pakietów IPv6.
- 
- Krok 5      **end**  
 Powróć do trybu privileged EXEC.
- 
- Krok 6      **copy running-config startup-config**  
 Zapisz ustawienia w pliku konfiguracyjnym.
- 

Poniższy przykład prezentuje włączanie funkcji IPv6 Source Guard na porcie 1/0/1:

**Switch#configure**

**Switch(config)#interface gigabitEthernet 1/0/1**

**Switch(config-if)#ipv6 verify source sipv6+mac**

**Switch(config-if)#show ipv6 verify source interface gigabitEthernet 1/0/1**

| Port    | Security-Type | LAG  |
|---------|---------------|------|
| ----    | -----         | ---- |
| Gi1/0/1 | SIPv6+MAC     | N/A  |

**Switch(config-if)#end**

**Switch#copy running-config startup-config**

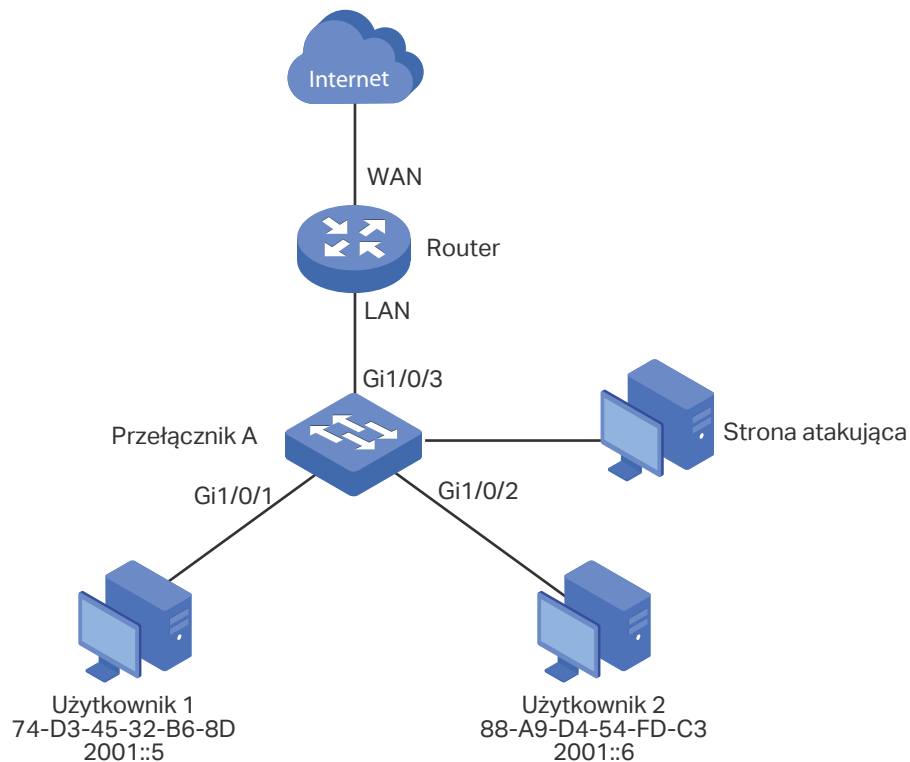
# 5 Przykłady konfiguracji

## 5.1 Przykład dla ND Detection

### 5.1.1 Wymagania sieciowe

Jak pokazano poniżej, użytkownik 1 i użytkownik 2 to legalni użytkownicy IPv6 w sieci LAN, podłączeni do portów 1/0/1 i 1/0/2. Obaj są w domyślnej sieci VLAN 1. Na routerze skonfigurowana została funkcja zabezpieczająca, aby zapobiegać atakom z sieci WAN. Administrator sieci planuje także skonfigurować przełącznik A, aby zapobiegać atakom ND z sieci LAN.

Rys. 5-1 Topologia sieci



### 5.1.2 Schemat konfiguracji

Aby spełnić powyższy warunek, należy skonfigurować ND Detection, aby chronić sieć przed atakami ND z sieci LAN.

Konfiguracja na przełączniku wymaga wykonania następujących kroków:

- 1) Skonfiguruj wiązanie IPv6-MAC. Wpisy wiązań dla użytkownika 1 i użytkownika 2 powinny być wiązaniami ręcznymi.
- 2) Skonfiguruj globalnie ND Detection.

- 3) Skonfiguruj ND Detection na portach. Ponieważ port 1/0/3 jest podłączony do routera będącego bramą sieciową, ustaw port 1/0/3 jako port trusted.

W poniższych podrozdziałach opisano dwa sposoby przeprowadzenia procedury konfiguracji: przez GUI oraz przez CLI.

### 5.1.3 Przez GUI

- 1) Wybierz z menu **SECURITY > IPv6 IMBP > IPv6-MAC Binding > Manual Binding** i kliknij **+ Add** aby wyświetlić poniższą stronę. Wpisz nazwę hosta, adres IPv6, adres MAC i VLAN ID użytkownika 1, ustaw typ ochrony jako ND Detection, i zaznacz na panelu port 1/0/1. Kliknij **Apply**.

Rys. 5-2 Wpis wiązania dla użytkownika 1

The screenshot shows the 'IPv6-MAC Binding' configuration page. The form contains the following fields:

- Host Name: User1 (20 characters maximum)
- IPv6 Address: 2001::5 (Format: 2001::1)
- MAC Address: 74-D3-45-32-B6-8D (Format: 00-00-00-00-00-01)
- VLAN ID: 1 (1-4094)
- Protect Type: ND Detection
- Port: 1/0/1 (Format: 1/0/1, input or choose below)

Below the form, there is a port selection panel for 'UNIT1' and 'LAGS'. The 'UNIT1' section shows ports 1 through 10. Port 1 is selected (highlighted in blue). A legend below the panel indicates that a blue icon means 'Selected', a white icon means 'Unselected', and a grey icon means 'Not Available'. At the bottom right, there are 'Cancel' and 'Apply' buttons.

- 2) W ten sam sposób dodaj wpis wiązania dla użytkownika 2. Wpisz nazwę hosta, adres IPv6, adres MAC i VLAN ID użytkownika 2, ustaw typ ochrony jako ND Detection, i zaznacz na panelu port 1/0/2. Kliknij **Apply**.

Rys. 5-3 Wpis wiązania dla użytkownika 2

**IPv6-MAC Binding**

Host Name:  (20 characters maximum)

IPv6 Address:  (Format: 2001::1)

MAC Address:  (Format: 00-00-00-00-00-01)

VLAN ID:  (1-4094)

Protect Type:  ▼

Port:  (Format: 1/0/1, input or choose below)

UNIT1:  1  2  3  4  5  6  7  8  9  10

LAGS:

Selected  Unselected  Not Available

- 3) Wybierz z menu **SECURITY > IPv6 IMBP > ND Detection > Global Config** aby wyświetlić poniższą stronę. Włącz ND Detection i kliknij **Apply**. Zaznacz VLAN 1, zmień Status na Enabled i kliknij **Apply**.

Rys. 5-4 Włączanie ND Detection

**Global Config**

ND Detection:  Enable

**VLAN Config**

| <input checked="" type="checkbox"/> | VLAN ID | Status  | Log Status |
|-------------------------------------|---------|---------|------------|
| <input checked="" type="checkbox"/> | 1       | Enabled | Disabled   |

Total: 1 1 entry selected.

- 4) Wybierz z menu **SECURITY > IPv6 IMBP > ND Detection > Port Config** aby wyświetlić poniższą stronę. Domyślnie wszystkie porty mają włączoną funkcję ND Detection. Ponieważ port 1/0/3 jest podłączony do routera będącego bramą sieciową, ustaw port 1/0/3 jako port trusted. Kliknij **Apply**.




Rys. 5-5 Konfiguracja portów

The screenshot shows the 'Port Config' window with two tabs: 'UNIT1' and 'LAGS'. The 'UNIT1' tab is active, displaying a table of ports. The 'Trust Status' column for port 1/0/3 is highlighted in a red box and set to 'Enable'. The 'Apply' button at the bottom right is also highlighted in a red box.

| <input type="checkbox"/>            | Port   | Trust Status | LAG |
|-------------------------------------|--------|--------------|-----|
| <input type="checkbox"/>            | 1/0/1  | Disabled     | --- |
| <input type="checkbox"/>            | 1/0/2  | Disabled     | --- |
| <input checked="" type="checkbox"/> | 1/0/3  | Enabled      | --- |
| <input type="checkbox"/>            | 1/0/4  | Disabled     | --- |
| <input type="checkbox"/>            | 1/0/5  | Disabled     | --- |
| <input type="checkbox"/>            | 1/0/6  | Disabled     | --- |
| <input type="checkbox"/>            | 1/0/7  | Disabled     | --- |
| <input type="checkbox"/>            | 1/0/8  | Disabled     | --- |
| <input type="checkbox"/>            | 1/0/9  | Disabled     | --- |
| <input type="checkbox"/>            | 1/0/10 | Disabled     | --- |

Total: 10      1 entry selected.     

- 5) Kliknij  Save, aby zapisać ustawienia.

## 5.1.4 Przez CLI

- 1) Dodaj wpisy ręcznych wiązań dla użytkownika 1 i użytkownika 2.

```
Switch_A#configure
```

```
Switch_A(config)#ipv6 source binding User1 2001::5 74:d3:45:32:b6:8d vlan 1 interface
gigabitEthernet 1/0/1 nd-detection
```

```
Switch_A(config)#ip source binding User1 2001::6 88:a9:d4:54:fd:c3 vlan 1 interface
gigabitEthernet 1/0/2 nd-detection
```

- 2) Włącz globalnie ND Detection oraz w sieci VLAN 1.

```
Switch_A(config)#ipv6 nd detection vlan 1
```

- 3) Ustaw prot 1/0/3 jako port trusted.

```
Switch_A(config)#interface gigabitEthernet 1/0/3
```

```
Switch_A(config-if)#ipv6 nd detection trust
```

```
Switch_A(config-if)#end
```

```
Switch_A#copy running-config startup-config
```

## Sprawdzanie konfiguracji

Sprawdzanie wpisów wiązań IPv6-MAC:

```
Switch_A#show ipv6 source binding
```

```
U Host IP-Addr MAC-Addr VID Port ACL SOURCE
```

```

- ---- -
1 User1 2001::5 74:d3:45:32:b6:8d 1 Fa1/0/1 ND-D Manual
1 User2 2001::6 88:a9:d4:54:fd:c3 1 Fa1/0/2 ND-D Manual

```

Notice:

1. Here, 'ND-D' for 'ND-Detection', and 'IP-V-S' for 'IP-Verify-Source'.

Sprawdzanie globalnej konfiguracji ND Detection:

```
Switch_A#show ipv6 nd detection
```

```
Global Status: Enable
```

Sprawdzanie konfiguracji ND Detection w sieci VLAN:

```
Switch_A#show ipv6 nd detection vlan
```

```

VID Enable status Log Status
---- -
1 Enable Disable

```

Sprawdzanie konfiguracji ND Detection na portach:

```
Switch_A#show ipv6 nd detection interface
```

```

Interface Trusted LAG
----- -
Gi1/0/1 Disable N/A
Gi1/0/2 Disable N/A
Gi1/0/3 Enable N/A
...

```

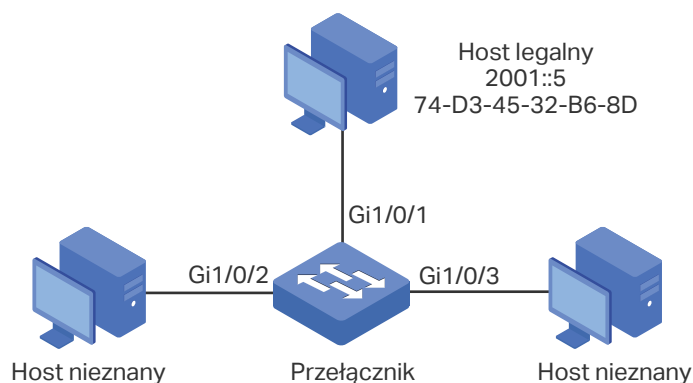
## 5.2 Przykład dla IPv6 Source Guard

### 5.2.1 Wymagania sieciowe

Jak pokazano poniżej, the host legalny łączy się z przełącznikiem poprzez port 1/0/1 i należy do domyślnej sieci VLAN 1. Wymaga się, aby tylko host legalny miał dostęp do sieci

poprzez port 1/0/1, a inne hosty będą blokowane starając się o dostęp do sieci poprzez porty 1/0/1-3.

Rys. 5-6 Topologia sieci



## 5.2.2 Schemat konfiguracji

Aby spełnić ten warunek, należy skorzystać z wiązania IPv6-MAC oraz funkcji IPv6 Source Guard w celu filtrowania pakietów odbieranych od hostów nieznanych. Konfiguracja na przełączniku wymaga wykonania następujących kroków:

- 1) Powiąż adres MAC, adres IPv6, numer podłączonego portu i VLAN ID hosta legalnego poprzez wiązanie IPv6-MAC.
- 2) Włącz IPv6 Source Guard na portach 1/0/1-3.

W poniższych podrozdziałach opisano dwa sposoby przeprowadzenia procedury konfiguracji: przez GUI oraz przez CLI.

## 5.2.3 Przez GUI

- 1) Wybierz z menu **SECURITY > IPv6 IMPB > IPv6-MAC Binding > Manual Binding** i kliknij **+ Add**, aby wyświetlić poniższą stronę. Wprowadź nazwę hosta, adres IPv6, adres MAC i VLAN ID hosta legalnego, ustaw typ ochrony jako SIP+MAC i zaznacz na panelu port 1/0/1. Kliknij **Apply**.

Rys. 5-7 Wiązanie ręczne

### IPv6-MAC Binding

Host Name:  (20 characters maximum)

IPv6 Address:  (Format: 2001::1)

MAC Address:  (Format: 00-00-00-00-00-01)

VLAN ID:  (1-4094)

Protect Type:

Port:  (Format: 1/0/1, input or choose below)

**UNIT1**

**LAGS**

Selected

Unselected

Not Available

- 2) Wybierz z menu **SECURITY > IPv6 IMPB > IPv6 Source Guard**, aby wyświetlić poniższą stronę. Zaznacz porty 1/0/1-3, ustaw Security Type jako SIP+MAC i kliknij **Apply**.

Rys. 5-8 IPv6 Source Guard

#### IPv6 Source Guard Config

UNIT1
LAGS

| <input type="checkbox"/>            | Port   | Security Type | LAG |
|-------------------------------------|--------|---------------|-----|
| <input checked="" type="checkbox"/> | 1/0/1  | SIP+MAC       | --- |
| <input checked="" type="checkbox"/> | 1/0/2  | SIP+SMAC      | --- |
| <input checked="" type="checkbox"/> | 1/0/3  | SIP+SMAC      | --- |
| <input type="checkbox"/>            | 1/0/4  | Disable       | --- |
| <input type="checkbox"/>            | 1/0/5  | Disable       | --- |
| <input type="checkbox"/>            | 1/0/6  | Disable       | --- |
| <input type="checkbox"/>            | 1/0/7  | Disable       | --- |
| <input type="checkbox"/>            | 1/0/8  | Disable       | --- |
| <input type="checkbox"/>            | 1/0/9  | Disable       | --- |
| <input type="checkbox"/>            | 1/0/10 | Disable       | --- |

Total: 10
3 entries selected.

- 3) Kliknij **Save**, aby zapisać ustawienia.

## 5.2.4 Przez CLI

- 1) Powiąż ręcznie adres IPv6, adres MAC, VLAN ID i numer podłączonego portu hosta legalnego, a następnie zastosuj ten wpis do funkcji IPv6 Source Guard.

```
Switch#configure
```

```
Switch(config)#ipv6 source binding legal-host 2001::5 74:d3:45:32:b6:8d vlan 1
interface gigabitEthernet 1/0/1 ipv6-verify-source
```

- 2) Włącz funkcję IPv6 Source Guard na portach 1/0/1-3.

```
Switch(config)# ipv6 verify source
```

```
Switch(config)# interface range gigabitEthernet 1/0/1-3
```

```
Switch(config-if-range)#ipv6 verify source sipv6+mac
```

```
Switch(config-if-range)#end
```

```
Switch#copy running-config startup-config
```

### Sprawdzanie konfiguracji

Sprawdzanie wpisu wiązania:

```
Switch#show ip source binding
```

| U | Host       | IP-Addr | MAC-Addr          | VID | Port    | ACL    | SOURCE |
|---|------------|---------|-------------------|-----|---------|--------|--------|
| - | ----       | -----   | -----             | --- | ----    | ---    | -----  |
| 1 | legal-host | 2001::5 | 74:d3:45:32:b6:8d | 1   | Fa1/0/1 | IP-V-S | Manual |

Notice:

1. Here, 'ND-D' for 'ND-Detection', and 'IP-V-S' for 'IP-Verify-Source'.

Sprawdzanie konfiguracji IPv6 Source Guard:

```
Switch#show ipv6 verify source
```

| Port    | Security-Type | LAG |
|---------|---------------|-----|
| Gi1/0/1 | SIP+MAC       | N/A |
| Gi1/0/2 | SIP+MAC       | N/A |
| Gi1/0/3 | SIP+MAC       | N/A |

.....

# Część 26

## Konfiguracja filtrowania DHCP

### ROZDZIAŁY

1. Filtrowanie DHCP
2. Konfiguracja filtrowania DHCPv4
3. Konfiguracja filtrowania DHCPv6
4. Przykłady konfiguracji

# 1 Filtrowanie DHCP

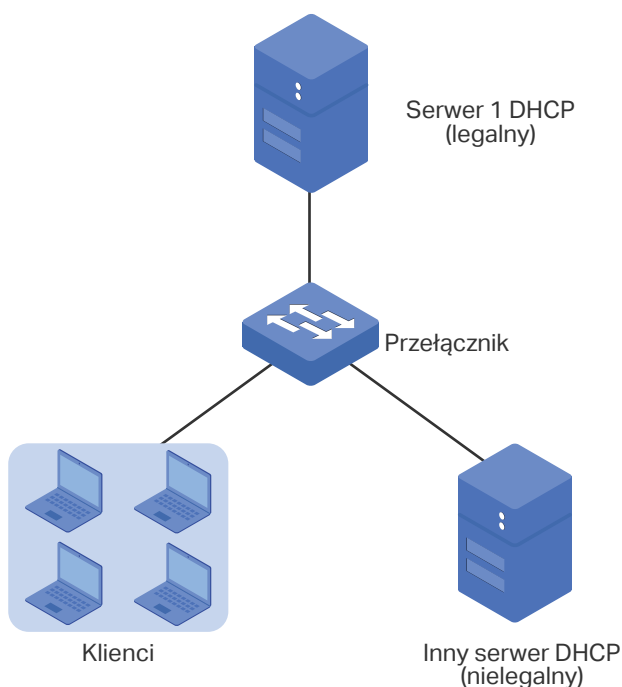
## 1.1 Informacje ogólne

Funkcjonowanie DHCP nie uwzględnia mechanizmu uwierzytelniania pomiędzy serwerem DHCP a klientami. Jeśli w sieci jest kilka serwerów DHCP, może to powodować zakłócenia sieci i problemy z jej bezpieczeństwem. Funkcja filtrowania DHCP rozwiązuje ten problem.

Po skonfigurowaniu funkcji filtrowania DHCP przełącznik może sprawdzać, czy odbierane pakiety DHCP są legalne i odrzucać te, które nie są. W ten sposób filtrowanie DHCP zapewnia użytkownikom otrzymywanie adresów IP tylko z legalnego serwera DHCP i zwiększa bezpieczeństwo sieci.

Jak pokazano na poniższym schemacie, w sieci są zarówno legalne, jak i nielegalne serwery DHCP. Aby ustawić serwer 1 DHCP jako legalny serwer DHCP, należy podać adres IP i numer portu serwera 1 DHCP. Po odebraniu pakietów respond DHCP przełącznik prześle pakiety z legalnego serwera DHCP.

Rys. 1-1 Topologia sieci



Ponadto można także ustawić limit szybkości przesyłania pakietów DHCP na każdym porcie.

## 1.2 Obsługiwane funkcje

Przełącznik obsługuje filtrowanie DHCPv4 oraz filtrowanie DHCPv6.

**Filtrowanie DHCPv4**

Filtrowanie DHCPv4 stosuje się w przypadku serwerów DHCPv4 i klientów IPv4.

**Filtrowanie DHCPv6**

Filtrowanie DHCPv6 stosuje się w przypadku serwerów DHCPv6 i klientów IPv6.



## 2 Konfiguracja filtrowania DHCPv4

Aby przeprowadzić konfigurację filtrowania DHCPv4, wykonaj poniższe kroki:

- 1) Skonfiguruj podstawowe parametry filtrowania DHCPv4.
- 2) Skonfiguruj legalne serwery DHCPv4.

### 2.1 Przez GUI

#### 2.1.1 Konfiguracja podstawowych parametrów filtrowania DHCPv4

Wybierz z menu **SECURITY > DHCP Filter > DHCPv4 Filter > Basic Config**, aby wyświetlić poniższą stronę.

Rys. 2-1 Podstawowa konfiguracja filtrowania DHCPv4

**Global Config**

DHCPv4 Filter:  Enable Apply

---

**Port Config**

UNIT1

LAGS

| <input type="checkbox"/>            | Port   | Status   | MAC Verify | Rate Limit | Decline Protect | LAG |
|-------------------------------------|--------|----------|------------|------------|-----------------|-----|
| <input checked="" type="checkbox"/> | 1/0/1  | Disabled | Disabled   | Disabled   | Disabled        | --- |
| <input type="checkbox"/>            | 1/0/2  | Disabled | Disabled   | Disabled   | Disabled        | --- |
| <input type="checkbox"/>            | 1/0/3  | Disabled | Disabled   | Disabled   | Disabled        | --- |
| <input type="checkbox"/>            | 1/0/4  | Disabled | Disabled   | Disabled   | Disabled        | --- |
| <input type="checkbox"/>            | 1/0/5  | Disabled | Disabled   | Disabled   | Disabled        | --- |
| <input type="checkbox"/>            | 1/0/6  | Disabled | Disabled   | Disabled   | Disabled        | --- |
| <input type="checkbox"/>            | 1/0/7  | Disabled | Disabled   | Disabled   | Disabled        | --- |
| <input type="checkbox"/>            | 1/0/8  | Disabled | Disabled   | Disabled   | Disabled        | --- |
| <input type="checkbox"/>            | 1/0/9  | Disabled | Disabled   | Disabled   | Disabled        | --- |
| <input type="checkbox"/>            | 1/0/10 | Disabled | Disabled   | Disabled   | Disabled        | --- |

Total: 10
1 entry selected.

Cancel
Apply

Wykonaj poniższe kroki, aby skonfigurować podstawowe ustawienia filtrowania DHCPv4:

- 1) W sekcji **Global Config** włącz globalnie DHCPv4.
- 2) W sekcji **Port Config** wybierz co najmniej jeden port i skonfiguruj jego parametry.

---

|      |              |
|------|--------------|
| Port | Numer portu. |
|------|--------------|

---

|                 |                                                                                                                                                                                                                                                                                                                                                                      |
|-----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Status          | Włącz lub wyłącz funkcję filtrowania DHCPv4 na porcie.                                                                                                                                                                                                                                                                                                               |
| MAC Verify      | <p>Włącz lub wyłącz funkcję weryfikacji adresów MAC. Pakiet DHCPv4 składa się z dwóch pól, które zawierają adres MAC hosta. Weryfikacja adresów MAC polega na porównaniu dwóch pól pakietu DHCPv4 i odrzuceniu pakietu, których pola się od siebie różnią.</p> <p>Zapobiega to wyczerpywaniu się źródła adresów IP na serwerze DHCPv4 przez fałszywe adresy MAC.</p> |
| Rate Limit      | Zaznacz, aby włączyć funkcję ograniczania przesyłu pakietów i ustalić maksymalną liczbę pakietów DHCPv4, które mogą być przesyłane na porcie na sekundę. Pakiety, które przekraczają ten limit będą odrzucane.                                                                                                                                                       |
| Decline Protect | Zaznacz, aby włączyć tę funkcję i ustalić maksymalną liczbę odrzuconych pakietów DHCPv4, które mogą być przesyłane na porcie na sekundę. Pakiety, które przekraczają ten limit będą odrzucane.                                                                                                                                                                       |
| LAG             | LAG, do którego należy port.                                                                                                                                                                                                                                                                                                                                         |

### 3) Kliknij **Apply**.

---

 **Uwaga:**

Port należący do LAG (Link Aggregation Group) korzysta z ustawień LAG, a nie ustawień własnych. Port może skorzystać ze swoich ustawień dopiero po opuszczeniu LAG.

---

## 2.1.2 Konfiguracja legalnych serwerów DHCPv4

Wybierz z menu **SECURITY > DHCP Filter > DHCPv4 Filter > Legal DHCPv4 Servers** i kliknij **+ Add**, aby wyświetlić poniższą stronę.

Rys. 2-2 Dodawanie legalnego serwera DHCPv4

Wykonaj poniższe kroki, aby dodać legalny serwer DHCPv4:

1) Skonfiguruj poniższe parametry:

|                    |                                                                                                                     |
|--------------------|---------------------------------------------------------------------------------------------------------------------|
| Server IP Address  | Podaj adres IP legalnego serwera DHCPv4.                                                                            |
| Client MAC Address | (Opcjonalnie) Podaj adres MAC klienta DHCP. Pozostawienie tego pola pustego oznacza wybór wszystkich klientów DHCP. |
| Server Port        | Wybierz port, z którym legalny serwer DHCPv4 jest połączony.                                                        |

2) Kliknij **Create**.

## 2.2 Przez CLI

### 2.2.1 Konfiguracja podstawowych parametrów filtrowania DHCPv4

Wykonaj poniższe kroki, aby skonfigurować podstawowe parametry filtrowania DHCPv4:

|        |                                                          |
|--------|----------------------------------------------------------|
| Krok 1 | <b>configure</b><br>Uruchom tryb konfiguracji globalnej. |
|--------|----------------------------------------------------------|

---

|         |                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|---------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Krok 2  | <b>ip dhcp filter</b><br>Włącz globalnie filtrowanie DHCPv4.                                                                                                                                                                                                                                                                                                                                                                                            |
| Krok 3  | <b>interface { fastEthernet <i>port</i>   range fastEthernet <i>port-list</i>   gigabitEthernet <i>port</i>   range gigabitEthernet <i>port-list</i>   ten-gigabitEthernet <i>port</i>   range ten-gigabitEthernet <i>port-list</i>   interface port-channel <i>port-channel-id</i>   interface range port-channel <i>port-channel-id-list</i> }</b><br>Uruchom tryb konfiguracji interfejsu.                                                           |
| Krok 4  | <b>ip dhcp filter</b><br>Włącz filtrowanie DHCPv4 na porcie.                                                                                                                                                                                                                                                                                                                                                                                            |
| Krok 5  | <b>ip dhcp filter mac-verify</b><br>Włącz funkcję weryfikacji adresów MAC. Pakiet DHCPv4 składa się z dwóch pól, które zawierają adres MAC hosta. Weryfikacja adresów MAC polega na porównaniu dwóch pól pakietu DHCPv4 i odrzuceniu pakietu, których pola się od siebie różnią. Zapobiega to wyczerpywaniu się źródła adresów IP na serwerze DHCPv4 przez fałszywe adresy MAC.                                                                         |
| Krok 6  | <b>ip dhcp filter limit rate <i>value</i></b><br>Włącz funkcję ograniczania przesyłu pakietów i ustal maksymalną liczbę pakietów DHCPv4, które mogą być przesyłane na porcie na sekundę. Pakiety, które przekraczają ten limit będą odrzucane.<br><br><i>value</i> : Podaj wartość limitu przesyłanych pakietów. Dostępne są następujące opcje: 0, 5,10,15,20,25 i 30 (pakietów/s). Domyślną wartością jest 0, co oznacza, że funkcja jest wyłączona.   |
| Krok 7  | <b>ip dhcp filter decline rate <i>value</i></b><br>Włącz funkcję limitu odrzucania pakietów i ustal maksymalną liczbę odrzuconych pakietów, które mogą być przesyłane na porcie na sekundę. Pakiety, które przekraczają ten limit będą odrzucane.<br><br><i>value</i> : Podaj wartość limitu odrzucanych pakietów. Dostępne są następujące opcje: 0, 5,10,15,20,25 i 30 (pakietów/s). Domyślną wartością jest 0, co oznacza, że funkcja jest wyłączona. |
| Krok 8  | <b>show ip dhcp filter</b><br>Przejrzyj globalną konfigurację filtrowania DHCPv4.                                                                                                                                                                                                                                                                                                                                                                       |
| Krok 9  | <b>show ip dhcp filter interface [ fastEthernet <i>port</i>   gigabitEthernet <i>port</i>   ten-gigabitEthernet <i>port</i>   port-channel <i>port-channel-id</i> ]</b><br>Przejrzyj konfigurację filtrowania DHCPv4 na porcie.                                                                                                                                                                                                                         |
| Krok 10 | <b>end</b><br>Powróć do trybu privileged EXEC.                                                                                                                                                                                                                                                                                                                                                                                                          |
| Krok 11 | <b>copy running-config startup-config</b><br>Zapisz ustawienia w pliku konfiguracyjnym.                                                                                                                                                                                                                                                                                                                                                                 |

---

 **Uwaga:**

Port należący do LAG (Link Aggregation Group) korzysta z ustawień LAG, a nie ustawień własnych. Port może skorzystać ze swoich ustawień dopiero po opuszczeniu LAG.

Poniższy schemat przedstawia przykładowy sposób globalnego włączania filtrowania DHCPv4, włączania filtrowania DHCPv4, funkcji weryfikacji adresów MAC, ustawiania limitu przesyłanych pakietów jako 10 p/s i odrzucanych pakietów jako 20 p/s na porcie 1/0/1:

```
Switch#configure
```

```
Switch(config)#ip dhcp filter
```

```
Switch(config)#interface gigabitEthernet 1/0/1
```

```
Switch(config-if)#ip dhcp filter
```

```
Switch(config-if)#ip dhcp filter mac-verify
```

```
Switch(config-if)#ip dhcp filter limit rate 10
```

```
Switch(config-if)#ip dhcp filter decline rate 20
```

```
Switch(config-if)##show ip dhcp filter
```

```
Global Status: Enable
```

```
Switch(config-if)#show ip dhcp filter interface gigabitEthernet 1/0/1
```

| Interface | state  | MAC-Verify | Limit-Rate | Dec-rate | LAG |
|-----------|--------|------------|------------|----------|-----|
| -----     | -----  | -----      | -----      | -----    | --- |
| Gi1/0/1   | Enable | Enable     | 10         | 20       | N/A |

```
Switch(config-if)#end
```

```
Switch#copy running-config startup-config
```

## 2.2.2 Konfiguracja legalnych serwerów DHCPv4

Wykonaj poniższe kroki, aby skonfigurować legalne serwery DHCPv4:

|        |                                      |
|--------|--------------------------------------|
| Krok 1 | <b>configure</b>                     |
|        | Uruchom tryb konfiguracji globalnej. |

- 
- Krok 2      **ip dhcp filter server permit-entry server-ip *ipAddr* client-mac *macAddr* interface { fastEthernet *port-list* | gigabitEthernet *port-list* | ten-gigabitEthernet *port-list* | port-channel *port-channel-id* }**
- Utwórz wpis dla legalnego serwera DHCPv4.
- ipAddr*: Podaj adres IP legalnego serwera DHCPv4.
- macAddr* : Podaj adres MAC klienta DHCP. Wartość "all" oznacza wszystkie adresy MAC klientów.
- port-list* | *port-channel-id*: Określ port, z którym legalny serwer DHCPv4 jest połączony.
- 
- Krok 3      **show ip dhcp filter server permit-entry**
- Przejrzyj ustawienia legalnego serwera DHCPv4.
- 
- Krok 4      **end**
- Powróć do trybu uprzywilejowanego (privileged EXEC mode).
- 
- Krok 5      **copy running-config startup-config**
- Zapisz ustawienia w pliku konfiguracyjnym.
- 

Poniższy schemat przedstawia przykładowy sposób tworzenia wpisu dla legalnego serwera DHCPv4, którego adres IP wynosi 192.168.0.100, a numerem połączonego portu jest 1/0/1 bez przydzielonego adresu MAC klienta:

### Switch#configure

```
Switch(config)#ip dhcp filter server permit-entry server-ip 192.168.0.100 client-mac all
interface gigabitEthernet 1/0/1
```

### Switch(config)#show ip dhcp filter server permit-entry

| Server IP     | Client MAC | Interface |
|---------------|------------|-----------|
| -----         | -----      | -----     |
| 192.168.0.100 | all        | Gi1/0/1   |

### Switch(config)#end

### Switch#copy running-config startup-config

# 3 Konfiguracja filtrowania DHCPv6

Aby przeprowadzić konfigurację filtrowania DHCPv6, wykonaj poniższe kroki:

- 1) Skonfiguruj podstawowe parametry filtrowania DHCPv6.
- 2) Skonfiguruj legalne serwery DHCPv6.

## 3.1 Przez GUI

### 3.1.1 Konfiguracja podstawowych parametrów filtrowania DHCPv6

Wybierz z menu **SECURITY > DHCP Filter > DHCPv6 Filter > Basic Config**, aby wyświetlić poniższą stronę.

Rys. 3-1 Podstawowa konfiguracja filtrowania DHCPv6

Global Config

DHCPv6 Filter:  Enable Apply

Port Config

| <input type="checkbox"/>            | Port   | Status   | Rate Limit | Decline Protect | LAG |
|-------------------------------------|--------|----------|------------|-----------------|-----|
| <input checked="" type="checkbox"/> | 1/0/1  | Disabled | Disabled   | Disabled        | --  |
| <input type="checkbox"/>            | 1/0/2  | Disabled | Disabled   | Disabled        | --  |
| <input type="checkbox"/>            | 1/0/3  | Disabled | Disabled   | Disabled        | --  |
| <input type="checkbox"/>            | 1/0/4  | Disabled | Disabled   | Disabled        | --  |
| <input type="checkbox"/>            | 1/0/5  | Disabled | Disabled   | Disabled        | --  |
| <input type="checkbox"/>            | 1/0/6  | Disabled | Disabled   | Disabled        | --  |
| <input type="checkbox"/>            | 1/0/7  | Disabled | Disabled   | Disabled        | --  |
| <input type="checkbox"/>            | 1/0/8  | Disabled | Disabled   | Disabled        | --  |
| <input type="checkbox"/>            | 1/0/9  | Disabled | Disabled   | Disabled        | --  |
| <input type="checkbox"/>            | 1/0/10 | Disabled | Disabled   | Disabled        | --  |

Total: 10 1 entry selected. Cancel Apply

Wykonaj poniższe kroki, aby skonfigurować podstawowe ustawienia filtrowania DHCPv6:

- 3) W sekcji **Global Config** włącz globalnie DHCPv6.
- 4) W sekcji **Port Config** wybierz co najmniej jeden port i skonfiguruj jego parametry.

---

Port                      Numer portu.

---


|                 |                                                                                                                                                                                                                |
|-----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Status          | Włącz lub wyłącz funkcję filtrowania DHCPv6 na porcie.                                                                                                                                                         |
| Rate Limit      | Zaznacz, aby włączyć funkcję ograniczania przesyłu pakietów i ustalić maksymalną liczbę pakietów DHCPv6, które mogą być przesyłane na porcie na sekundę. Pakiety, które przekraczają ten limit będą odrzucane. |
| Decline Protect | Zaznacz, aby włączyć tę funkcję i ustalić maksymalną liczbę odrzuconych pakietów DHCPv6, które mogą być przesyłane na porcie na sekundę. Pakiety, które przekraczają ten limit będą odrzucane.                 |
| LAG             | LAG, do którego należy port.                                                                                                                                                                                   |

### 5) Kliknij **Apply**.

#### Uwaga:

Port należący do LAG (Link Aggregation Group) korzysta z ustawień LAG, a nie ustawień własnych. Port może skorzystać ze swoich ustawień dopiero po opuszczeniu LAG.

## 3.1.2 Konfiguracja legalnych serwerów DHCPv6

Wybierz z menu **SECURITY > DHCP Filter > DHCPv6 Filter > Legal DHCPv6 Servers** i kliknij  **Add**, aby wyświetlić poniższą stronę.

Rys. 3-1 Dodawanie legalnego serwera DHCPv6

Add Legal DHCPv6 Server

Server IPv6 Address:  (Format: 2001::1)

Server Port:  Cancel (Format: 1/0/1, input or choose below)

**UNIT1**                      **LAGS**

1

2

3

4

5


6


7


8

9

10

 **Selected**

 **Unselected**

 **Not Available**

Cancel

Create

Wykonaj poniższe kroki, aby dodać legalny serwer DHCPv6:

### 1) Skonfiguruj poniższe parametry:

|                     |                                          |
|---------------------|------------------------------------------|
| Server IPv6 Address | Podaj adres IP legalnego serwera DHCPv6. |
|---------------------|------------------------------------------|

Configuration Guide ■ 745



---

|             |                                                              |
|-------------|--------------------------------------------------------------|
| Server Port | Wybierz port, z którym legalny serwer DHCPv6 jest połączony. |
|-------------|--------------------------------------------------------------|

---

2) Kliknij **Create**.

## 3.2 Przez CLI

### 3.2.1 Konfiguracja podstawowych parametrów filtrowania DHCPv6

Wykonaj poniższe kroki, aby skonfigurować podstawowe parametry filtrowania DHCPv6:

|        |                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Krok 1 | <b>configure</b><br>Uruchom tryb konfiguracji globalnej.                                                                                                                                                                                                                                                                                                                                                                                               |
| Krok 2 | <b>ipv6 dhcp filter</b><br>Włącz filtrowanie DHCPv6 globalnie.                                                                                                                                                                                                                                                                                                                                                                                         |
| Krok 3 | <b>interface { fastEthernet port   range fastEthernet port-list   gigabitEthernet port   range gigabitEthernet port-list   ten-gigabitEthernet port   range ten-gigabitEthernet port-list   interface port-channel port-channel-id   interface range port-channel port-channel-id-list }</b><br>Uruchom tryb konfiguracji interfejsu.                                                                                                                  |
| Krok 4 | <b>ipv6 dhcp filter</b><br>Włącz filtrowanie DHCPv6 na porcie.                                                                                                                                                                                                                                                                                                                                                                                         |
| Krok 5 | <b>ipv6 dhcp filter limit rate value</b><br>Włącz funkcję ograniczania przesyłu pakietów i ustal maksymalną liczbę pakietów DHCPv4, które mogą być przesyłane na porcie na sekundę. Pakiety, które przekraczają ten limit będą odrzucane.<br><br><i>value</i> : Podaj wartość limitu przesyłanych pakietów. Dostępne są następujące opcje: 0, 5, 10, 15, 20, 25 i 30 (pakietów/s). Domyślną wartością jest 0, co oznacza, że funkcja jest wyłączona.   |
| Krok 6 | <b>ipv6 dhcp filter decline rate value</b><br>Włącz funkcję limitu odrzucania pakietów i ustal maksymalną liczbę odrzuconych pakietów, które mogą być przesyłane na porcie na sekundę. Pakiety, które przekraczają ten limit będą odrzucane.<br><br><i>value</i> : Podaj wartość limitu odrzucanych pakietów. Dostępne są następujące opcje: 0, 5, 10, 15, 20, 25 i 30 (pakietów/s). Domyślną wartością jest 0, co oznacza, że funkcja jest wyłączona. |
| Krok 7 | <b>show ipv6 dhcp filter</b><br>Przejrzyj globalną konfigurację filtrowania DHCPv6.                                                                                                                                                                                                                                                                                                                                                                    |
| Krok 8 | <b>show ipv6 dhcp filter interface [ fastEthernet port   gigabitEthernet port   ten-gigabitEthernet port   port-channel port-channel-id ]</b><br>Przejrzyj konfigurację filtrowania DHCPv6 na porcie.                                                                                                                                                                                                                                                  |

---

Krok 9      **end**  
Powróć do trybu privileged EXEC.

Krok 10     **copy running-config startup-config**  
Zapisz ustawienia w pliku konfiguracyjnym.

 **Uwaga:**

Port należący do LAG (Link Aggregation Group) korzysta z ustawień LAG, a nie ustawień własnych. Port może skorzystać ze swoich ustawień dopiero po opuszczeniu LAG.

Poniższy schemat przedstawia przykładowy sposób globalnego włączania filtrowania DHCPv6, włączania filtrowania DHCPv6, ustawiania limitu przesyłanych pakietów jako 10 p/s i odrzucanych pakietów jako 20 p/s na porcie 1/0/1:

**Switch#configure**

**Switch(config)#ipv6 dhcp filter**

**Switch(config)#interface gigabitEthernet 1/0/1**

**Switch(config-if)#ipv6 dhcp filter**

**Switch(config-if)#ipv6 dhcp filter limit rate 10**

**Switch(config-if)#ipv6 dhcp filter decline rate 20**

**Switch(config-if)##show ipv6 dhcp filter**

Global Status: Enable

**Switch(config-if)#show ip dhcp filter interface gigabitEthernet 1/0/1**

| Interface | state  | Limit-Rate | Dec-rate | LAG |
|-----------|--------|------------|----------|-----|
| -----     | -----  | -----      | -----    | --- |
| Gi1/0/1   | Enable | 10         | 20       | N/A |

**Switch(config-if)#end**

**Switch#copy running-config startup-config**

### 3.2.2 Konfiguracja legalnych serwerów DHCPv6

Wykonaj poniższe kroki, aby skonfigurować legalne serwery DHCPv6:

Krok 1      **configure**  
Uruchom tryb konfiguracji globalnej.

Krok 2      **ipv6 dhcp filter server permit-entry server-ip *ipAddr* interface { fastEthernet *port-list* | gigabitEthernet *port-list* | ten-gigabitEthernet *port-list* | port-channel *port-channel-id* }**

Utwórz wpis dla legalnego serwera DHCPv6.

*ipAddr*: Podaj adres IP legalnego serwera DHCPv6.

*port-list* | *port-channel-id*: Określ port, z którym legalny serwer DHCPv6 jest połączony.

Krok 3      **show ip dhcp filter server permit-entry**

Przejrzyj ustawienia legalnego serwera DHCPv6.

Krok 4      **end**

Powróć do trybu privileged EXEC.

Krok 5      **copy running-config startup-config**

Zapisz ustawienia w pliku konfiguracyjnym.

Poniższy schemat przedstawia przykładowy sposób tworzenia wpisu dla legalnego serwera DHCPv4, którego adresem IP jest 2001::54, a numerem połączonego portu 1/0/1:

**Switch#configure**

**Switch(config)#ipv6 dhcp filter server permit-entry server-ip 2001::54 interface gigabitEthernet 1/0/1**

**Switch(config)#show ipv6 dhcp filter server permit-entry**

| Server IP | Interface |
|-----------|-----------|
| -----     | -----     |
| 2001::54  | Gi1/0/1   |

**Switch(config)#end**

**Switch#copy running-config startup-config**

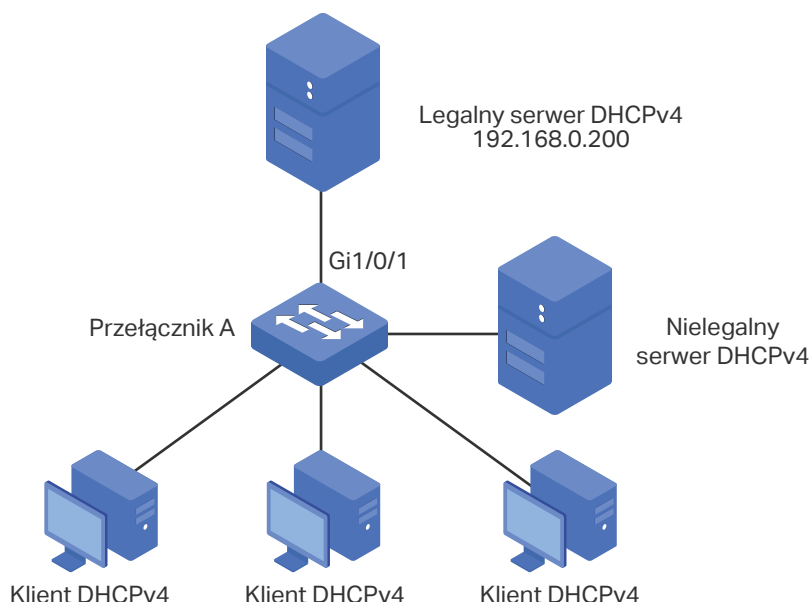
# 4 Przykłady konfiguracji

## 4.1 Przykład dla filtrowania DHCPv4

### 4.1.1 Wymagania sieciowe

Jak pokazano poniżej, wszyscy klienci DHCPv4 pobierają adresy IP z legalnego serwera DHCPv4 i żaden z serwerów DHCPv4 w sieci LAN nie jest uznawany za nielegalny. Wymaga się, aby wyłącznie serwer DHCPv4 mógł przydzielać adresy IP klientom.

Rys. 4-1 Topologia sieci



### 4.1.2 Schemat konfiguracji

Aby spełnić ten wymóg, należy skonfigurować funkcję filtrowania DHCPv4 w celu filtrowania pakietów DHCPv4 pochodzących z nielegalnego serwera DHCPv4.

Konfiguracja wymaga wykonania następujących kroków:

- 1) Włącz filtrowanie DHCPv4 globalnie i na wszystkich portach.
- 2) Utwórz wpis dla legalnego serwera DHCPv4.

W poniższych podrozdziałach opisano dwa sposoby przeprowadzenia procedury konfiguracji: przez GUI oraz przez CLI.

### 4.1.3 Przez GUI

- Wybierz z menu **SECURITY > DHCP Filter > DHCPv4 Filter > Basic Config**, aby wyświetlić poniższą stronę. Włącz globalnie filtrowanie DHCPv4 i kliknij **Apply**. Zaznacz wszystkie porty, zmień opcję Status na Enable i kliknij **Apply**.

Rys. 4-2 Podstawowa konfiguracja

Global Config

DHCPv4 Filter:  Enable **Apply**


Port Config

| UNIT1                               |        | LAGS    |            |            |                 |     |  |
|-------------------------------------|--------|---------|------------|------------|-----------------|-----|--|
| <input checked="" type="checkbox"/> | Port   | Status  | MAC Verify | Rate Limit | Decline Protect | LAG |  |
|                                     |        | Enable  |            |            |                 |     |  |
| <input checked="" type="checkbox"/> | 1/0/1  | Enabled | Disabled   | Disabled   | Disabled        | --- |  |
| <input checked="" type="checkbox"/> | 1/0/2  | Enabled | Disabled   | Disabled   | Disabled        | --- |  |
| <input checked="" type="checkbox"/> | 1/0/3  | Enabled | Disabled   | Disabled   | Disabled        | --- |  |
| <input checked="" type="checkbox"/> | 1/0/4  | Enabled | Disabled   | Disabled   | Disabled        | --- |  |
| <input checked="" type="checkbox"/> | 1/0/5  | Enabled | Disabled   | Disabled   | Disabled        | --- |  |
| <input checked="" type="checkbox"/> | 1/0/6  | Enabled | Disabled   | Disabled   | Disabled        | --- |  |
| <input checked="" type="checkbox"/> | 1/0/7  | Enabled | Disabled   | Disabled   | Disabled        | --- |  |
| <input checked="" type="checkbox"/> | 1/0/8  | Enabled | Disabled   | Disabled   | Disabled        | --- |  |
| <input checked="" type="checkbox"/> | 1/0/9  | Enabled | Disabled   | Disabled   | Disabled        | --- |  |
| <input checked="" type="checkbox"/> | 1/0/10 | Enabled | Disabled   | Disabled   | Disabled        | --- |  |

Total: 10 28 entries selected. **Cancel** **Apply**

- Wybierz z menu **SECURITY > DHCP Filter > DHCPv4 Filter > Legal DHCPv4 Servers** i kliknij **+ Add**, aby wyświetlić poniższą stronę. Podaj adres IP i numer podłączonego port legalnego serwera DHCPv4. Kliknij **Create**.

Rys. 4-3 Tworzenie wpisu dla legalnego serwera DHCPv4

- 3) Kliknij  , aby zapisać ustawienia.

#### 4.1.4 Przez CLI

- 1) Włącz filtrowanie DHCPv4 globalnie i na wszystkich portach:

```
Switch_A#configure
```

```
Switch_A(config)#ip dhcp filter
```

```
Switch_A(config)#interface range gigabitEthernet 1/0/1-10
```

```
Switch_A(config-if-range)#exit
```

- 2) Utwórz wpis dla legalnego serwera DHCPv4:

```
Switch_A(config)#ip dhcp filter server permit-entry server-ip 192.168.0.200 client-mac all interface fastEthernet 1/0/1
```

```
Switch_A(config)#end
```

```
Switch_A#copy running-config startup-config
```

#### Sprawdzanie konfiguracji

Sprawdanie globalnej konfiguracji filtrowania DHCPv4:

```
Switch_A#show ip dhcp filter
```

```
Global Status: Enable
```

Sprawdzanie konfiguracji filtrowania DHCPv4 na portach:

```
Switch_A#show ip dhcp filter interface
```

| Interface | state  | MAC-Verify | Limit-Rate | Dec-rate | LAG |
|-----------|--------|------------|------------|----------|-----|
| -----     | -----  | -----      | -----      | -----    | --- |
| Gi1/0/1   | Enable | Disable    | Disable    | Disable  | N/A |
| Gi1/0/2   | Enable | Disable    | Disable    | Disable  | N/A |
| Gi1/0/3   | Enable | Disable    | Disable    | Disable  | N/A |
| Gi1/0/4   | Enable | Disable    | Disable    | Disable  | N/A |
| .....     |        |            |            |          |     |

Sprawdzanie konfiguracji legalnego serwera DHCPv4:

```
Switch_A#show ip dhcp filter server permit-entry
```

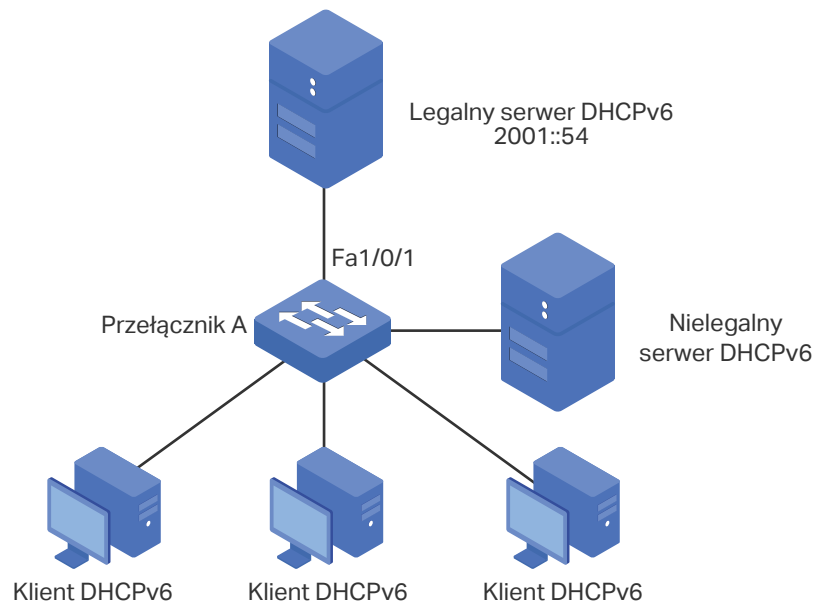
| Server IP     | Client MAC | Interface |
|---------------|------------|-----------|
| -----         | -----      | -----     |
| 192.168.0.200 | all        | Fa1/0/1   |

## 4.2 Przykład dla filtrowania DHCPv6

### 4.2.1 Wymagania sieciowe

Jak pokazano poniżej, wszyscy klienci DHCPv6 pobierają adresy IP z legalnego serwera DHCPv6 i żaden z serwerów DHCPv6 w sieci LAN nie jest uznawany za nielegalny. Wymaga się, aby wyłącznie serwer DHCPv6 mógł przydzielać adresy IP klientom.

Rys. 4-4 Topologia sieci



## 4.2.2 Schemat konfiguracji

Aby spełnić ten wymóg, należy skonfigurować funkcję filtrowania DHCPv6 w celu filtrowania pakietów DHCPv6 pochodzących z nielegalnego serwera DHCPv6.

Konfiguracja wymaga wykonania następujących kroków:

- 1) Włącz filtrowanie DHCPv6 globalnie i na wszystkich portach.
- 2) Utwórz wpis dla legalnego serwera DHCPv6.

W poniższych podrozdziałach opisano dwa sposoby przeprowadzenia procedury konfiguracji: przez GUI oraz przez CLI.

## 4.2.3 Przez GUI

- 1) Wybierz z menu **SECURITY > DHCP Filter > DHCPv6 Filter > Basic Config**, aby wyświetlić poniższą stronę. Włącz globalnie filtrowanie DHCPv6 i kliknij **Apply**. Zaznacz wszystkie porty, zmień opcję Status na Enable i kliknij **Apply**.



Rys. 4-5 Podstawowa konfiguracja

Global Config

DHCPv6 Filter:  Enable Apply

Port Config

| UNIT1                               | LAGS | Port   | Status  | MAC Verify | Rate Limit | Decline Protect | LAG |
|-------------------------------------|------|--------|---------|------------|------------|-----------------|-----|
| <input checked="" type="checkbox"/> |      |        | Enable  |            |            |                 |     |
| <input checked="" type="checkbox"/> |      | 1/0/1  | Enabled | Disabled   | Disabled   | Disabled        | --- |
| <input checked="" type="checkbox"/> |      | 1/0/2  | Enabled | Disabled   | Disabled   | Disabled        | --- |
| <input checked="" type="checkbox"/> |      | 1/0/3  | Enabled | Disabled   | Disabled   | Disabled        | --- |
| <input checked="" type="checkbox"/> |      | 1/0/4  | Enabled | Disabled   | Disabled   | Disabled        | --- |
| <input checked="" type="checkbox"/> |      | 1/0/5  | Enabled | Disabled   | Disabled   | Disabled        | --- |
| <input checked="" type="checkbox"/> |      | 1/0/6  | Enabled | Disabled   | Disabled   | Disabled        | --- |
| <input checked="" type="checkbox"/> |      | 1/0/7  | Enabled | Disabled   | Disabled   | Disabled        | --- |
| <input checked="" type="checkbox"/> |      | 1/0/8  | Enabled | Disabled   | Disabled   | Disabled        | --- |
| <input checked="" type="checkbox"/> |      | 1/0/9  | Enabled | Disabled   | Disabled   | Disabled        | --- |
| <input checked="" type="checkbox"/> |      | 1/0/10 | Enabled | Disabled   | Disabled   | Disabled        | --- |

Total: 10 28 entries selected. Cancel Apply

- 2) Wybierz z menu **SECURITY > DHCP Filter > DHCPv6 Filter > Legal DHCPv6 Servers** i kliknij **+ Add**, aby wyświetlić poniższą stronę. Podaj adres IP i numer podłączonego port legalnego serwera DHCPv6. Kliknij **Create**.

Rys. 4-6 Tworzenie wpisu dla legalnego serwera DHCPv6

Add Legal DHCPv6 Server

Server IPv6 Address:  (Format: 2001::1)

Server Port:  Cancel (Format: 1/0/1, input or choose below)

UNIT1                      LAGS

1

2

3

4

5

6

7

8

9


10

Selected

Unselected

Not Available

Cancel Create

- 3) Kliknij  **Save**, aby zapisać ustawienia.

## 4.2.4 Przez CLI

- 1) Włącz filtrowanie DHCPv6 globalnie i na wszystkich portach:

```
Switch_A#configure
Switch_A(config)#ipv6 dhcp filter
Switch_A(config)#interface range gigabitEthernet 1/0/1-10
Switch_A(config-if-range)#exit
```

- 2) Utwórz wpis dla legalnego serwera DHCPv6:

```
Switch_A(config)#ipv6 dhcp filter server permit-entry server-ip 2001::54 interface
gigabitEthernet 1/0/1
Switch_A(config)#end
Switch_A#copy running-config startup-config
```

### Sprawdzanie konfiguracji

Sprawdzanie globalnej konfiguracji filtrowania DHCPv6:

```
Switch_A#show ipv6 dhcp filter
Global Status: Enable
```

Sprawdzanie konfiguracji filtrowania DHCPv6 na portach:

```
Switch_A#show ipv6 dhcp filter interface
```

| Interface | state  | Limit-Rate | Dec-rate | LAG |
|-----------|--------|------------|----------|-----|
| -----     | -----  | -----      | -----    | --- |
| Gi1/0/1   | Enable | Disable    | Disable  | N/A |
| Gi1/0/2   | Enable | Disable    | Disable  | N/A |
| Gi1/0/3   | Enable | Disable    | Disable  | N/A |
| Gi1/0/4   | Enable | Disable    | Disable  | N/A |
| .....     |        |            |          |     |

Sprawdzanie konfiguracji legalnego serwera DHCPv6:

```
Switch_A#show ipv6 dhcp filter server permit-entry
```

| Server IP | Interface |
|-----------|-----------|
| -----     | -----     |
| 2001::54  | Gi1/0/1   |

# Część 27

## Konfiguracja DoS Defend

### ROZDZIAŁY

1. Informacje ogólne
2. Konfiguracja DoS Defend

# 1 Informacje ogólne

Funkcja DoS (Denial of Service) Defend zapewnia ochronę przed atakami DoS, które złośliwie zajmują przepustowość sieci poprzez wysyłanie wielu żądań usług do hostów. Występowanie ataków DoS skutkuje nieprawidłowym działaniem lub awarią sieci.

Z funkcją DoS Defend przełącznik może analizować określone pola adresu IP pakietów, wykrywać pakiety wysyłane w wyniku ataku DoS i od razu je odrzucać. Funkcja ta pozwala także na ograniczanie częstotliwości przesyłania pakietów legalnych. Gdy liczba legalnych pakietów przekracza ustawiony próg i istnieje ryzyko awarii sieci, przełącznik zaczyna odrzucać pakiety.

# 2 Konfiguracja DoS Defend

## 2.1 Przez GUI

Wybierz z menu **SECURITY > DoS Defend**, aby wyświetlić poniższą stronę.

Rys. 2-1 DoS Defend

Wykonaj poniższe kroki, aby skonfigurować DoS Defend:

- 1) W sekcji **DoS Defend** włącz DoS Protection i kliknij **Apply**.
- 2) W sekcji **DoS Defend Config** wybierz jeden lub kilka typów ochrony, stosownie do wymagań, i kliknij **Apply**. Poniższa tabela zawiera wszystkie typy ataków DoS.

|             |                                                                                                                                                                                                                                                                                    |
|-------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Land Attack | Strona atakująca wysyła określony fałszywy pakiet SYN (synchroniczny) do hosta docelowego. Ponieważ zarówno źródłowy adres IP, jak i docelowy adres IP pakietu SYN mają pełnić rolę adresu IP hosta, host bezskutecznie będzie starać się nawiązać połączenie ze stroną atakującą. |
| Scan SYNFIN | Strona atakująca wysyła pakiet z ustawioną flagą SYN oraz flagą FIN o wartości 1. Flaga SYN wysyła do hosta żądanie nawiązania połączenia, natomiast flaga FIN żąda przerwania połączenia. Zatem pakiet tego typu jest nielegalny.                                                 |
| Xmascan     | Strona atakująca wysyła nielegalny pakiet z indeksem TCP oraz flagami FIN, URG i PSH o wartości 1.                                                                                                                                                                                 |

|                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| NULL Scan            | Strona atakująca wysyła nielegalny pakiet ze swoim indeksem TCP i wszystkimi polami kontrolnymi ustawionymi do wartości 0. Podczas trwającego połączenia TCP oraz transmisji danych wszystkie pola kontrolne o wartości 0 są klasyfikowane jako nielegalne.                                                                                                                                                                                                             |
| SYN sPort less 1024  | Strona atakująca wysyła nielegalne pakiety z ustawionymi flagami TCP SYN o wartości 1 oraz portem źródłowym o numerze niższym niż 1024.                                                                                                                                                                                                                                                                                                                                 |
| Blat Attack          | Strona atakująca wysyła nielegalny pakiet z tym samym portem źródłowym i docelowym w warstwie 4 oraz flagą URG o wartości 1. Podobnie jak w przypadku Land Attack, działanie systemu atakowanego hosta jest ograniczone, ponieważ host bezskutecznie stara się nawiązać połączenie ze stroną atakującą.                                                                                                                                                                 |
| Ping Flooding        | Strona atakująca przeciąża system docelowy wysyłanymi pakietami ping, tworząc burzę broadcastową, która uniemożliwia systemowi poprawną komunikację.                                                                                                                                                                                                                                                                                                                    |
| SYN/SYN-ACK Flooding | Strona atakująca korzysta ze sfałszowanego adresu IP do wysyłania pakietów żądań TCP do serwera. Po otrzymaniu pakietów żądań serwer odpowiada poprzez pakiety SYN-ACK. Ze względu na to, że adres IP jest sfałszowany, serwer nie otrzyma żadnej odpowiedzi. Dlatego serwer będzie kontynuować wysyłanie pakietów SYN-ACK. Jeżeli strona atakująca przeciąży zasoby sieciowe wysyłaniem sfałszowanych pakietów żądań, także żądania legalnych klientów będą odrzucane. |
| WinNuke Attack       | Ze względu na to, że system operacyjny z błędami nie może poprawnie przetwarzać flagi URG (Urgent Pointer) pakietów TCP, strona atakująca wysyła ten typ pakietów do portu 139 (NetBIOS) hosta z błędami systemu operacyjnego, co skutkuje zawieszeniem systemu i wyświetleniem niebieskiego ekranu.                                                                                                                                                                    |
| Ping of Death        | Strona atakująca wysyła nieprawidłowe pakiety ping, większe niż 65535 bajtów, aby spowodować awarię systemu komputera docelowego.                                                                                                                                                                                                                                                                                                                                       |
| Smurf Attack         | Smurf attack to rozproszony atak DoS, w którym duża liczba pakietów ICMP (Internet Control Message Protocol) ze sfałszowanym adresem IP jest przesyłana na adres rozgłoszeniowy sieci. Większość urządzeń w sieci będzie domyślnie wysyłała odpowiedzi na źródłowy adres IP atakowanej ofiary. Jeżeli liczba urządzeń, które wysyłają odpowiedzi na te pakiety jest duża, łącze atakowanego komputera zostanie przeciążone.                                             |

3) Kliknij **Apply**.

## 2.2 Przez CLI

Wykonaj poniższe kroki, aby skonfigurować DoS Defend:

|        |                                                              |
|--------|--------------------------------------------------------------|
| Krok 1 | <b>configure</b><br>Uruchom tryb konfiguracji globalnej.     |
| Krok 2 | <b>ip dos-prevent</b><br>Włącz globalnie funkcję DoS Defend. |

## Krok 3

**ip dos-prevent type { land | scan-synfin | xma-scan | null-scan | port-less-1024 | blat | ping-flood | syn-flood | win-nuke | ping-of-death | smurf }**

Skonfiguruj jeden lub kilka typów ochrony, stosownie do wymagań. Poniżej znajdują się objaśnienia wszystkich typów ataków DoS.

**land:** Strona atakująca wysyła określony fałszywy pakiet SYN (synchroniczny) do hosta docelowego. Ponieważ zarówno źródłowy adres IP, jak i docelowy adres IP pakietu SYN mają pełnić rolę adresu IP hosta, host bezskutecznie będzie starać się nawiązać połączenie ze stroną atakującą.

**scan-synfin:** Strona atakująca wysyła pakiet z ustawioną flagą SYN oraz flagą FIN o wartości 1. Flaga SYN wysyła do hosta żądanie nawiązania połączenia, natomiast flaga FIN żąda przerwania połączenia. Zatem pakiet tego typu jest nielegalny.

**xma-scan:** Strona atakująca wysyła nielegalny pakiet z indeksem TCP oraz flagami FIN, URG i PSH o wartości 1.

**null-scan:** Strona atakująca wysyła nielegalny pakiet ze swoim indeksem TCP i wszystkimi polami kontrolnymi ustawionymi do wartości 0. Podczas trwającego połączenia TCP oraz transmisji danych wszystkie pola kontrolne o wartości 0 są klasyfikowane jako nielegalne.

**port-less-1024:** Strona atakująca wysyła nielegalne pakiety z ustawionymi flagami TCP SYN o wartości 1 oraz portem źródłowym o numerze niższym niż 1024.

**blat:** Strona atakująca wysyła nielegalny pakiet z tym samym portem źródłowym i docelowym w warstwie 4 oraz flagą URG o wartości 1. Podobnie jak w przypadku Land Attack, działanie systemu atakowanego hosta jest ograniczone, ponieważ host bezskutecznie stara się nawiązać połączenie ze stroną atakującą.

**ping-flood:** Strona atakująca przeciąża system docelowy wysyłanymi pakietami ping, tworząc burzę broadcastową, która uniemożliwia systemowi poprawną komunikację.

**syn-flood:** Strona atakująca korzysta ze sfałszowanego adresu IP do wysyłania pakietów żądań TCP do serwera. Po otrzymaniu pakietów żądań serwer odpowiada poprzez pakiety SYN-ACK. Adres IP jest sfałszowany, stąd serwer nie otrzyma żadnej odpowiedzi i serwer będzie kontynuować wysyłanie pakietów SYN-ACK. Jeżeli strona atakująca przeciąży zasoby sieciowe fałszywymi pakietami żądań, żądania legalnych klientów będą odrzucane.

**win-nuke:** Ze względu na to, że system operacyjny z błędami nie może poprawnie przetwarzać flagi URG (Urgent Pointer) pakietów TCP, strona atakująca wysyła ten typ pakietów do portu 139 (NetBIOS) hosta z błędami systemu operacyjnego, co skutkuje zawieszeniem systemu i wyświetleniem niebieskiego ekranu.

**ping-of-death:** Strona atakująca wysyła nieprawidłowe pakiety ping, większe niż 65535 bajtów, aby spowodować awarię systemu komputera docelowego.

**smurf:** Smurf attack to rozproszony atak DoS, w którym duża liczba pakietów ICMP (Internet Control Message Protocol) ze sfałszowanym adresem IP jest przesyłana na adres rozgłoszeniowy sieci. Większość urządzeń w sieci będzie domyślnie wysyłała odpowiedzi na źródłowy adres IP atakowanej ofiary. Jeżeli liczba urządzeń, które wysyłają odpowiedzi na te pakiety jest duża, łącze atakowanego komputera zostanie przeciążone.

## Krok 4

**show ip dos-prevent**

Przejrzyj ustawienia DoS Defend.



---

Krok 5      **end**  
Powróć do trybu privileged EXEC.

---

Krok 6      **copy running-config startup-config**  
Zapisz ustawienia w pliku konfiguracyjnym.

---

Poniższy schemat przedstawia przykładowy sposób włączania typu ochrony DoS o nazwie land:

**Switch#configure**

**Switch(config)#ip dos-prevent**

**Switch(config)#ip dos-prevent type land**

**Switch(config)#show ip dos-prevent**

DoS Prevention State:    Enabled

| Type | Status |
|------|--------|
|------|--------|

|      |       |
|------|-------|
| ---- | ----- |
|------|-------|

|             |         |
|-------------|---------|
| Land Attack | Enabled |
|-------------|---------|

|             |          |
|-------------|----------|
| Scan SYNFIN | Disabled |
|-------------|----------|

|         |          |
|---------|----------|
| Xmascan | Disabled |
|---------|----------|

|           |          |
|-----------|----------|
| NULL Scan | Disabled |
|-----------|----------|

|                     |          |
|---------------------|----------|
| SYN sPort less 1024 | Disabled |
|---------------------|----------|

|             |          |
|-------------|----------|
| Blat Attack | Disabled |
|-------------|----------|

|               |          |
|---------------|----------|
| Ping Flooding | Disabled |
|---------------|----------|

|                      |          |
|----------------------|----------|
| SYN/SYN-ACK Flooding | Disabled |
|----------------------|----------|

|                |          |
|----------------|----------|
| WinNuke Attack | Disabled |
|----------------|----------|

|              |          |
|--------------|----------|
| Smurf Attack | Disabled |
|--------------|----------|

|               |          |
|---------------|----------|
| Ping Of Death | Disabled |
|---------------|----------|

**Switch(config)#end**

**Switch#copy running-config startup-config**

# Część 28

## Monitorowanie systemu

### ROZDZIAŁY

1. Informacje ogólne
2. Monitorowanie procesora
3. Monitorowanie pamięci

# 1 Informacje ogólne

Z funkcją monitorowania systemu możesz:

- monitorować wykorzystanie procesora przełącznika.
- monitorować wykorzystanie pamięci przełącznika.

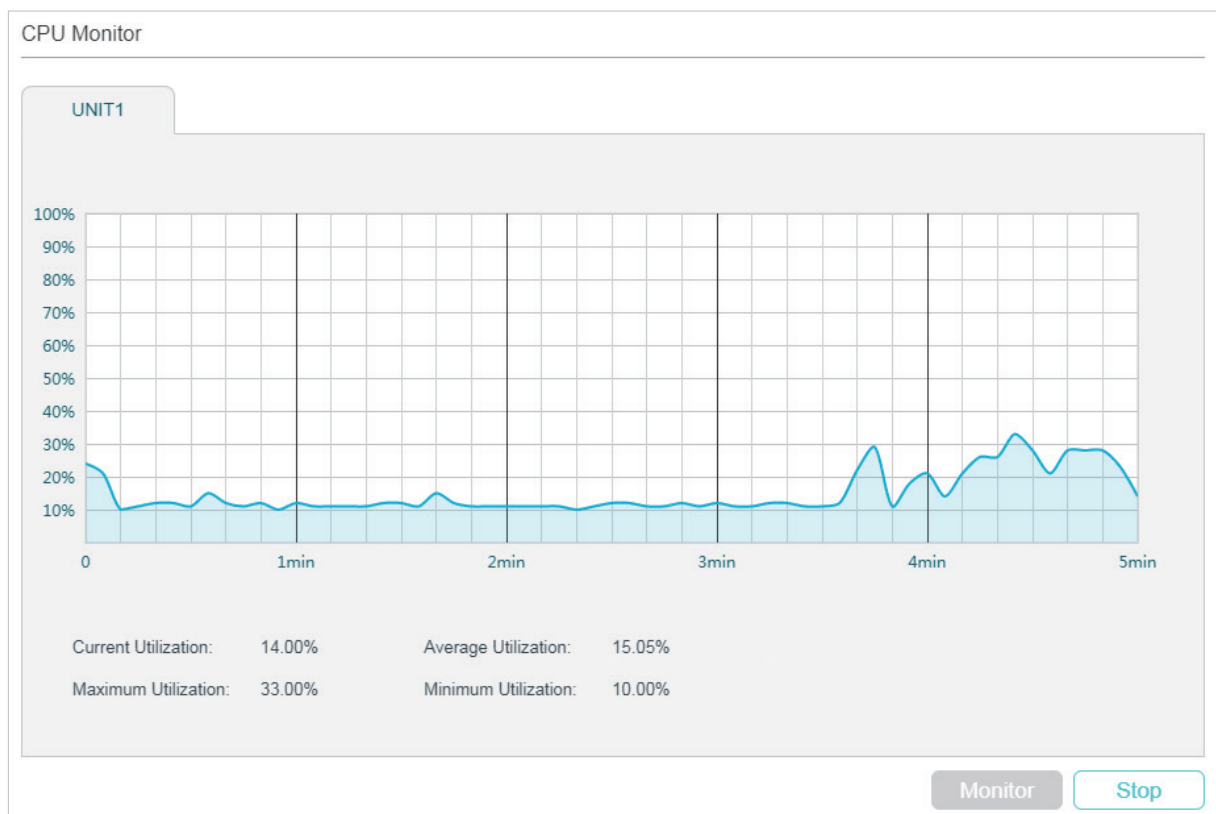
Wykorzystanie procesora nie powinno przekraczać 80%. Zbyt duże zużycie może skutkować nieprawidłowym działaniem przełącznika, np. brakiem odpowiedzi na żądania kontroli (ICMP ping, przekroczenie czasu odpowiedzi SNMP, wolne połączenie Telnet lub sesja SSH). Funkcja monitorowania systemu umożliwia identyfikację problemów ze stanem procesora.

# 2 Monitorowanie procesora

## 2.1 Przez GUI

Wybierz z menu **MAINTENANCE > System Monitor > CPU Monitor**, aby wyświetlić poniższą stronę.

Rys. 2-1 Monitorowanie procesora



Kliknij **Monitor**, aby włączyć na przełączniku monitorowanie i wyświetlanie co 5 sekund stopnia wykorzystania procesora.

## 2.2 Przez CLI

Korzystając z poniższego polecenia w trybie privileged EXEC mode lub w każdym innym trybie konfiguracji możesz wyświetlić wykorzystanie procesora:

```
show cpu-utilization
```

Zobacz wykorzystanie procesora przełącznika sprzed ostatnich 5 sekund, 1 minuty i 5 minut.

Poniższy schemat przedstawia przykładowy sposób monitorowania procesora:

**Switch#show cpu-utilization**

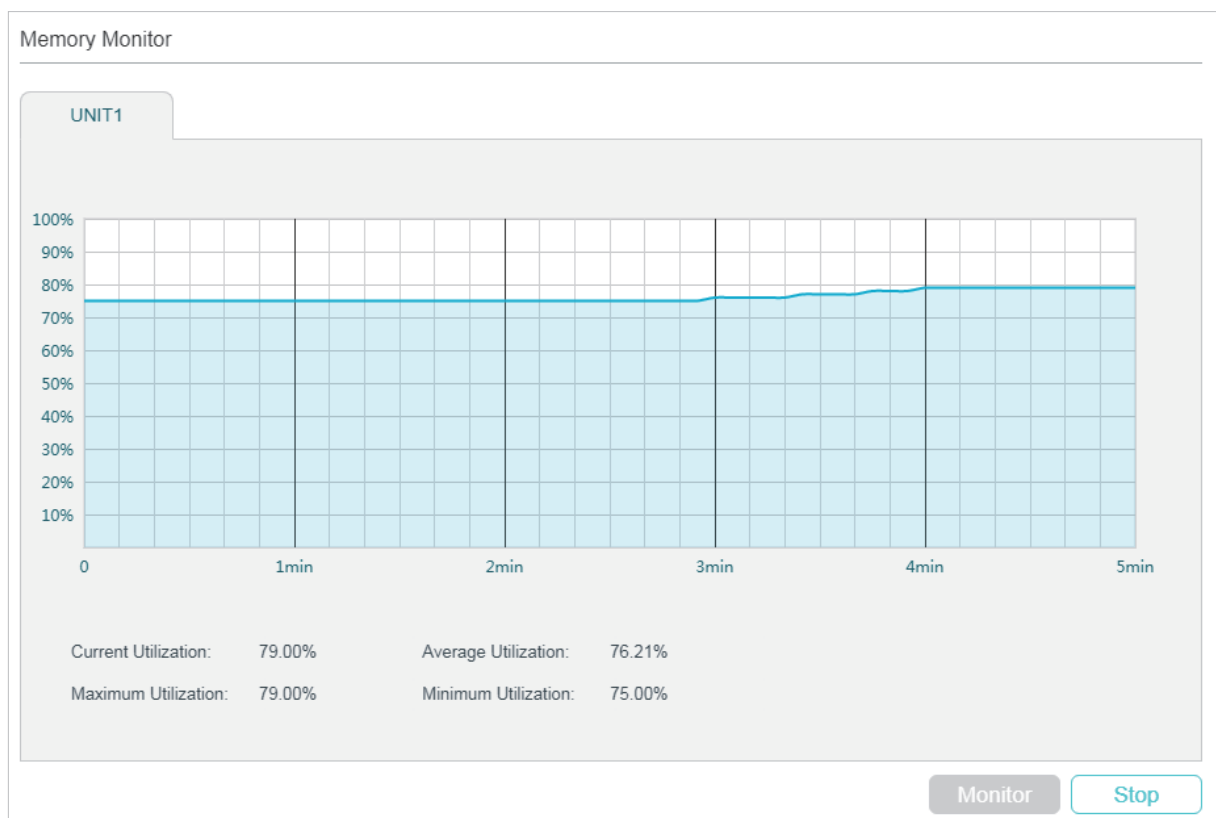
| Unit        | CPU Utilization |            |              |
|-------------|-----------------|------------|--------------|
| No.         | Five-Seconds    | One-Minute | Five-Minutes |
| -----+----- |                 |            |              |
| 1           | 13%             | 13%        | 13%          |

# 3 Monitorowanie pamięci

## 3.1 Przez GUI

Wybierz z menu **MAINTENANCE > System Monitor > Memory Monitor**, aby wyświetlić poniższą stronę.

Rys. 3-1 Monitorowanie pamięci



Kliknij **Monitor**, aby włączyć na przełączniku monitorowanie i wyświetlanie co 5 sekund stopnia wykorzystania pamięci.

## 3.2 Przez CLI

Korzystając z poniższego polecenia w trybie privileged EXEC lub w każdym innym trybie konfiguracji możesz wyświetlić wykorzystanie pamięci:

```
show memory-utilization
```

Zobacz aktualne wykorzystanie pamięci przełącznika.

Poniższy schemat przedstawia przykładowy sposób monitorowania pamięci:

```
Switch#show memory-utilization
```

Unit | Current Memory Utilization

-----+-----

1 | 74%

# Część 29

## Monitorowanie ruchu

### ROZDZIAŁY

#### 1. Monitorowanie ruchu



# 1 Monitorowanie ruchu

Funkcja monitorowania ruchu umożliwia analizę ruchu na każdym porcie poprzez dostęp do dokładnych zestawień i statystyk ruchu danych.

## 1.1 Przez GUI

Wybierz z menu **MAINTENANCE > Traffic Monitor**, aby wyświetlić poniższą stronę.

Rys. 1-1 Podsumowanie ruchu danych

**Traffic Summary**

Auto Refresh:  Enable Apply

UNIT1

LAGS

Refresh
 Clear

| <input type="checkbox"/> | Port   | Packets Rx | Packets Tx | Octets Rx | Octets Tx | Statistics                 |
|--------------------------|--------|------------|------------|-----------|-----------|----------------------------|
| <input type="checkbox"/> | 1/0/1  | 0          | 0          | 0         | 0         | <a href="#">Statistics</a> |
| <input type="checkbox"/> | 1/0/2  | 0          | 0          | 0         | 0         | <a href="#">Statistics</a> |
| <input type="checkbox"/> | 1/0/3  | 0          | 0          | 0         | 0         | <a href="#">Statistics</a> |
| <input type="checkbox"/> | 1/0/4  | 0          | 0          | 0         | 0         | <a href="#">Statistics</a> |
| <input type="checkbox"/> | 1/0/5  | 0          | 0          | 0         | 0         | <a href="#">Statistics</a> |
| <input type="checkbox"/> | 1/0/6  | 0          | 0          | 0         | 0         | <a href="#">Statistics</a> |
| <input type="checkbox"/> | 1/0/7  | 0          | 0          | 0         | 0         | <a href="#">Statistics</a> |
| <input type="checkbox"/> | 1/0/8  | 1490744    | 118053     | 156482855 | 35085375  | <a href="#">Statistics</a> |
| <input type="checkbox"/> | 1/0/9  | 0          | 0          | 0         | 0         | <a href="#">Statistics</a> |
| <input type="checkbox"/> | 1/0/10 | 0          | 0          | 0         | 0         | <a href="#">Statistics</a> |
| Total: 10                |        |            |            |           |           |                            |

Wykonaj poniższe kroki, aby zobaczyć zestawienia ruchu sieciowego dla każdego portu:

- 1) Włącz automatyczne odświeżanie (**Auto Refresh**) lub kliknij **Refresh**, aby na bieżąco analizować zestawienia ruchu.

**Auto Refresh:** Włączenie tej opcji umożliwia przełącznikowi automatyczne odświeżanie zestawień ruchu sieciowego.

**Refresh Interval:** Podaj interwał odświeżania przez przełącznik zestawień ruchu sieciowego.

- 2) W sekcji **Traffic Summary** kliknij **UNIT1**, aby zobaczyć informacje o portach fizycznych, a następnie kliknij **LAGS**, aby wyświetlić informacje o grupach agregacji łączy (LAG).

**Packets Rx:** Liczba pakietów odebranych na porcie. Błędne pakiety nie są uwzględniane.

|             |                                                                            |
|-------------|----------------------------------------------------------------------------|
| Packets Tx: | Liczba pakietów przesłanych na porcie. Błędne pakiety nie są uwzględniane. |
| Octets Rx:  | Liczba oktetów odebranych na porcie. Błędne oktety są uwzględniane.        |
| Octets Tx:  | Liczba oktetów przesyłanych na porcie. Błędne oktety są uwzględniane.      |

Aby wyświetlić szczegółowe statystyki danych dla portu, kliknij **Statistics** po prawej stronie pozycji.

Rys. 1-1 Statystyki ruchu

| Statistics <span style="float: right;">✕</span> |           |                    |          |
|-------------------------------------------------|-----------|--------------------|----------|
| Port1/0/8                                       |           |                    |          |
| Received                                        |           | Sent               |          |
| Broadcast:                                      | 1205990   | Broadcast:         | 0        |
| Multicast:                                      | 179749    | Multicast:         | 11511    |
| Unicast:                                        | 105266    | Unicast:           | 106552   |
| Jumbo:                                          | 0         | Jumbo:             | 0        |
| Alignment Errors:                               | 0         | Pkts:              | 118063   |
| Undersize Packets:                              | 0         | Bytes:             | 35087903 |
| 64-Octets Packets:                              | 1170083   | Collisions Errors: | 0        |
| 65-to-127-Octets Packets:                       | 65762     |                    |          |
| 128-to-255-Octets Packets:                      | 106624    |                    |          |
| 256-to-511-Octets Packets:                      | 130504    |                    |          |
| 512-to-1023-Octets Packets:                     | 18004     |                    |          |
| 1024-to-1518-Octets Packets:                    | 28        |                    |          |
| Pkts:                                           | 1491005   |                    |          |
| Bytes:                                          | 156503887 |                    |          |

---

|                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Received:</b> | Szczegółowe informacje o odebranych pakietach.<br><br>Broadcast: Liczba prawidłowych pakietów broadcast odebranych na porcie. Błędne ramki nie są uwzględniane.<br><br>Multicast: Liczba prawidłowych pakietów multicast odebranych na porcie. Błędne ramki nie są uwzględniane.<br><br>Unicast: Liczba prawidłowych pakietów unicast odebranych na porcie. Błędne ramki nie są uwzględniane.<br><br>Jumbo: Liczba prawidłowych pakietów jumbo odebranych na porcie. Błędne ramki nie są uwzględniane.<br><br>Alignment Errors: Liczba odebranych pakietów, których FCS (Frame Check Sequence) ma niezintegrowany oktet (Alignment Error). Rozmiar pakietu musi mieścić się w przedziale 64 - 1518 bajtów.<br><br>Undersize Packets: Liczba odebranych pakietów (z wykluczeniem pakietów błędnych), krótszych niż 64 bajty.<br><br>64-Octets Packets: Liczba odebranych pakietów (z wykluczeniem pakietów błędnych) o rozmiarze 64 bajtów.<br><br>65-to-127-Octets Packets: Liczba odebranych pakietów (łącznie z pakietami błędnymi), które mają od 65 do 127 bajtów długości.<br><br>128-to-255-Octets Packets: Liczba odebranych pakietów (łącznie z pakietami błędnymi), które mają od 128 do 255 bajtów długości.<br><br>256-to-511-Octets Packets: Liczba odebranych pakietów (łącznie z pakietami błędnymi), które mają od 256 do 511 bajtów długości.<br><br>512-to-1023-Octets Packets: Liczba odebranych pakietów (łącznie z pakietami błędnymi), które mają od 512 do 1023 bajtów długości.<br><br>1023-to-1518-Octets Packets: Liczba odebranych pakietów (łącznie z pakietami błędnymi), które mają od 512 do 1023 bajtów długości.<br><br>Pkts: Liczba pakietów odebranych na porcie. Błędne pakiety nie są uwzględniane.<br><br>Bytes: Liczba bajtów odebranych na porcie. Błędne pakiety nie są uwzględniane. |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

---

|              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|--------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Sent:</b> | Szczegółowe informacje o pakietach wysłanych.<br><br>Broadcast: Liczba prawidłowych pakietów broadcast przesłanych na porcie. Błędne ramki nie są uwzględniane.<br><br>Multicast: Liczba prawidłowych pakietów multicast przesłanych na porcie. Błędne ramki nie są uwzględniane.<br><br>Unicast: Liczba prawidłowych pakietów unicast przesłanych na porcie. Błędne ramki nie są uwzględniane.<br><br>Pkts: Liczba pakietów przesłanych na porcie. Błędne pakiety nie są uwzględniane.<br><br>Bytes: Liczba bajtów przesłanych na porcie. Błędne pakiety nie są uwzględniane.<br><br>Collisions: Liczba kolizji na porcie w trybie półduplexu podczas przesyłania pakietów. |
|--------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

---

## 1.2 Przez CLI

Korzystając z poniższego polecenia w trybie uprzywilejowanym (privileged EXEC mode) lub w każdym innym trybie konfiguracji możesz wyświetlić informacje o ruchu na każdym porcie lub w grupie agregacji łączy (LAG):

```
show interface counters [fastEthernet port | gigabitEthernet port | ten-gigabitEthernet port | port-channel port-channel-id]
```

*port-channel-id* : Numer grupy LAG.

Jeżeli nie podasz żadnego numeru portu, ani numeru grupy, wyświetlą się informacje o wszystkich portach i grupach.

Te informacje uwzględniają:

Tx Collisions: Liczba kolizji na porcie podczas przesyłania pakietów.

Tx Ucast / Tx Mcast / Tx Bcast / Tx Jumbo: Liczba prawidłowych pakietów unicast / multicast / broadcast / jumbo przesłanych na porcie. Błędne ramki nie są uwzględniane.

Tx Pkts: Liczba pakietów przesłanych na porcie. Błędne pakiety nie są uwzględniane.

Rx Bytes: Liczba bajtów przesłanych na porcie. Błędne pakiety nie są uwzględniane.

Rx Ucast / Rx Mcast / Rx Bcast / Rx Liczba prawidłowych pakietów unicast / multicast / broadcast / jumbo odebranych na porcie. Błędne ramki nie są uwzględniane.

Rx Alignment: Liczba odebranych pakietów, których FCS (Frame Check Sequence) ma niezintegrowany oktet (Alignment Error). Rozmiar pakietu musi mieścić się w przedziale 64 - 1518 bajtów.

Rx UnderSize: Liczba odebranych pakietów (z wykluczeniem pakietów błędnych), krótszych niż 64 bajty.

Rx 64Pkts: Liczba odebranych pakietów (z wykluczeniem pakietów błędnych) o rozmiarze 64 bajtów.

Rx 65-127Pkts: Liczba odebranych pakietów (łącznie z pakietami błędnymi), które mają od 65 do 127 bajtów długości.

Rx 128-255Pkts: Liczba odebranych pakietów (łącznie z pakietami błędnymi), które mają od 128 do 255 bajtów długości.

Rx 256-511Pkts: Liczba odebranych pakietów (łącznie z pakietami błędnymi), które mają od 256 do 511 bajtów długości.

Rx 512-1023Pkts: Liczba odebranych pakietów (łącznie z pakietami błędnymi), które mają od 512 do 1023 bajtów długości.

Rx 1024-1518Pkts: Liczba odebranych pakietów (łącznie z pakietami błędnymi), które mają od 512 do 1023 bajtów długości.

Rx Pkts: Liczba pakietów odebranych na porcie. Błędne pakiety nie są uwzględniane.

Rx Bytes: Liczba bajtów odebranych na porcie. Błędne pakiety nie są uwzględniane.

# Część 30

## Port Mirroring

### ROZDZIAŁY

1. Mirroring
2. Przykłady konfiguracji

# 1 Mirroring

Mirroring to funkcja do analizy ruchu sieciowego i rozwiązywania problemów występujących w sieci. Funkcja ta umożliwia przełącznikowi przesyłanie kopii ruchu przechodzącego przez określone źródła (porty, grupy LAG lub procesor) do portu docelowego. Nie ma natomiast wpływu na przełączanie ruchu sieciowego na portach źródłowych, w grupach LAG lub na procesorze.

## 1.1 Przez GUI

Wybierz z menu **MAINTENANCE > Mirroring**, aby wyświetlić poniższą stronę.

Rys. 1-1 Lista sesji Port Mirroring

| Port Mirroring Session List |                  |                                     |                   |                                            |
|-----------------------------|------------------|-------------------------------------|-------------------|--------------------------------------------|
| Session                     | Destination Port | Mode                                | Source Interfaces | Operation                                  |
| 1                           |                  | Ingress Only<br>Egress Only<br>Both |                   | <a href="#">Edit</a> <a href="#">Clear</a> |
| Total: 1                    |                  |                                     |                   |                                            |

Powyższa strona przedstawia sesję mirroring. Nie można utworzyć żadnej dodatkowej sesji. Kliknij **Edit**, aby skonfigurować tą sesję mirroring, tak jak na poniższej stronie.

Rys. 1-2 Konfiguracja sesji Mirroring

### Destination Port Config

UNIT1

1

2

3

4

5

6

7

8

9

10

Apply

---

### Source Interfaces Config

|                          | UNIT1  | LAGS     | CPU      |     |  |
|--------------------------|--------|----------|----------|-----|--|
| <input type="checkbox"/> | Port   | Ingress  | Egress   | LAG |  |
| <input type="checkbox"/> | 1/0/1  | Disabled | Disabled | --  |  |
| <input type="checkbox"/> | 1/0/2  | Disabled | Disabled | --  |  |
| <input type="checkbox"/> | 1/0/3  | Disabled | Disabled | --  |  |
| <input type="checkbox"/> | 1/0/4  | Disabled | Disabled | --  |  |
| <input type="checkbox"/> | 1/0/5  | Disabled | Disabled | --  |  |
| <input type="checkbox"/> | 1/0/6  | Disabled | Disabled | --  |  |
| <input type="checkbox"/> | 1/0/7  | Disabled | Disabled | --  |  |
| <input type="checkbox"/> | 1/0/8  | Disabled | Disabled | --  |  |
| <input type="checkbox"/> | 1/0/9  | Disabled | Disabled | --  |  |
| <input type="checkbox"/> | 1/0/10 | Disabled | Disabled | --  |  |

Total: 10

Wykonaj poniższe kroki, aby skonfigurować sesję mirroring:

- 1) W sekcji **Destination Port Config** wybierz port docelowy dla sesji mirroring i kliknij **Apply**.
- 2) W sekcji **Source Interfaces Config** wybierz interfejsy źródłowe i kliknij **Apply**. Ruch przesyłany przez interfejsy źródłowe będzie kopiowany do portu źródłowego. Dostępne są trzy typy interfejsów źródłowych: port, LAG i CPU. Wybierz jeden lub kilka typów, stosownie do swoich wymagań.

|                |                                                                                                                                                                     |
|----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>UNIT1</b>   | Ustaw interfejsy źródłowe, wybierając określone porty. Przełącznik prześle do portu docelowego kopię ruchu przechodzącego przez port.                               |
| <b>LAGS</b>    | Ustaw interfejsy źródłowe, wybierając określone grupy agregacji łącza. Przełącznik prześle do portu docelowego kopię ruchu przechodzącego przez LAG.                |
| <b>CPU</b>     | Jeżeli wybierzesz ten typ, przełącznik prześle do portu docelowego kopię ruchu przechodzącego przez procesor.                                                       |
| <b>Ingress</b> | Jeżeli włączysz tę opcję, pakiety odebrane przez odpowiedni interfejs (port, LAG lub CPU) zostaną skopiowane do portu docelowego. Domyślnie ta opcja jest włączona. |

|        |                                                                                                                                                                       |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Egress | Jeżeli włączysz tę opcję, pakiety przesłane przez odpowiedni interfejs (port, LAG lub CPU) zostaną skopiowane do portu docelowego. Domyślnie ta opcja jest wyłączona. |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|

 Uwaga:

- Porty przynależące do LAG nie mogą być portami docelowymi ani źródłowymi.
- Ten sam port nie może być równocześnie portem docelowym i źródłowym.

## 1.2 Przez CLI

Wykonaj poniższe kroki, aby skonfigurować funkcję Mirroring.

|        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Krok 1 | <b>configure</b><br>Uruchom tryb konfiguracji globalnej.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Krok 2 | <b>monitor session <i>session_num</i> destination interface { fastEthernet <i>port</i>   gigabitEthernet <i>port</i>   ten-gigabitEthernet <i>port</i> }</b><br>Włącz funkcję port mirror i ustaw port docelowy.<br><i>session_num</i> : Numer sesji monitorowania. Jedyną dozwoloną wartością jest 1.<br><i>port</i> : Numer portu docelowego. Dla sesji monitorowania można podać tylko jeden port docelowy.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Krok 3 | <b>monitor session <i>session_num</i> source { cpu <i>cpu_numbr</i>   interface { fastEthernet <i>port-list</i>   gigabitEthernet <i>port-list</i>   ten-gigabitEthernet <i>port-list</i>   port-channel <i>port-channel-id</i> } mode</b><br>Ustaw interfejsy monitorowania, wybierając określone porty lub grupy agregacji łącza.<br><i>session_num</i> : Numer sesji monitorowania. Jedyną dozwoloną wartością jest 1.<br><i>cpu_number</i> : Numer procesora. Jedyną dozwoloną wartością jest 1.<br><i>port-list</i> : Lista portów źródłowych. Można wybrać wiele opcji.<br><i>mode</i> : Tryb monitorowania. Dostępne są trzy opcje: <b>rx</b> , <b>tx</b> i <b>both</b> :<br><b>rx</b> : Pakiety przychodzące na port źródłowy będą kopiowane na port docelowy.<br><b>tx</b> : Pakiety wychodzące na porcie źródłowym będą kopiowane na port docelowy.<br><b>both</b> : Zarówno pakiety przychodzące, jak i wychodzące na porcie źródłowym mogą być skopiowane na port docelowy.<br><i>Note</i> :<br>Możesz skonfigurować dowolną liczbę typów interfejsów źródłowych (ports, LAGs i CPU), stosownie do wymagań. |
| Krok 4 | <b>show monitor session</b><br>Przejrzyj konfigurację Port Mirroring.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Krok 5 | <b>end</b><br>Powróć do trybu privileged EXEC.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Krok 6 | <b>copy running-config startup-config</b><br>Zapisz ustawienia w pliku konfiguracyjnym.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |



Poniższy schemat przedstawia przykładowy sposób kopiowania odebranych i wysłanych pakietów na porcie 1/0/1,2,3 i procesora CPU na port 1/0/10.

**Switch#configure****Switch(config)#monitor session 1 destination interface gigabitEthernet 1/0/10****Switch(config)#monitor session 1 source interface gigabitEthernet 1/0/1-3 both****Switch(config)#monitor session 1 source cpu 1 both****Switch(config)#show monitor session**

```
Monitor Session: 1
Destination Port: Gi1/0/10
Source Ports(Ingress): Gi1/0/1-3
Source Ports(Egress): Gi1/0/1-3
Source CPU(Ingress): cpu1
Source CPU(Egress): cpu1
```

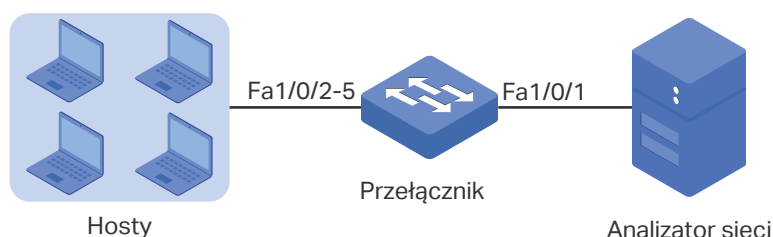
**Switch(config-if)#end****Switch#copy running-config startup-config**

# 2 Przykłady konfiguracji

## 2.1 Wymagania sieciowe

Jak pokazano poniżej, bezpośrednio do przełącznika podłączonych jest kilku hostów oraz analizator sieci. W celu zachowania bezpieczeństwa sieci i diagnozowania problemów administrator sieci musi korzystać z analizatora sieci, co pozwala mu na monitorowanie pakietów danych wysyłanych przez hosta końcowego.

Rys. 2-1 Topologia sieci



## 2.2 Schemat konfiguracji

Aby wdrożyć powyższe rozwiązanie, należy skorzystać z funkcji Mirroring, która pozwala na kopiowanie pakietów z portów 1/0/2-5 do portu 1/0/1. Konfiguracja wymaga wykonania następujących kroków:

- 1) Ustaw porty 1/0/2-5 jako porty źródłowe, co umożliwi przełącznikowi kopiowanie pakietów od hostów.
- 2) Ustaw port 1/0/1 jako port docelowy, co umożliwi analizatorowi sieci odbieranie skopiowanych pakietów od hostów.

W poniższych podrozdziałach opisano dwa sposoby przeprowadzenia procedury konfiguracji: przez GUI oraz przez CLI.

## 2.3 Przez GUI

- 1) Wybierz z menu **MAINTENANCE > Mirroring**, aby wyświetlić poniższą stronę. Znajdują się tutaj informacje o sesji mirroring.

Rys. 2-2 Lista sesji Mirror

| Port Mirroring Session List |                  |                                     |                   |                                            |
|-----------------------------|------------------|-------------------------------------|-------------------|--------------------------------------------|
| Session                     | Destination Port | Mode                                | Source Interfaces | Operation                                  |
| 1                           |                  | Ingress Only<br>Egress Only<br>Both |                   | <a href="#">Edit</a> <a href="#">Clear</a> |
| Total: 1                    |                  |                                     |                   |                                            |

- 2) Kliknij na powyższej stronie **Edit**, aby wyświetlić stronę poniższą. W sekcji **Destination Port Config** ustaw port 1/0/1 jako port docelowy i kliknij **Apply**.

Rys. 2-3 Konfiguracja portu docelowego

Destination Port Config

UNIT1

1

2

3

4

5

6

7

8

9

10

Apply

- 3) W sekcji **Source Interfaces Config** ustaw porty 1/0/2-5 jako porty źródłowe oraz włącz **Ingress** i **Egress**, aby zezwolić na kopiowanie pakietów odebranych i wysłanych do portu docelowego. Następnie kliknij **Apply**.

Rys. 2-4 Konfiguracja portu źródłowego

Source Interfaces Config

UNIT1

LAGS

CPU

| <input type="checkbox"/>            | Port   | Ingress                                         | Egress                                          | LAG |
|-------------------------------------|--------|-------------------------------------------------|-------------------------------------------------|-----|
|                                     |        | Enable <span style="font-size: small;">▼</span> | Enable <span style="font-size: small;">▼</span> |     |
| <input type="checkbox"/>            | 1/0/1  | Disabled                                        | Disabled                                        | --  |
| <input checked="" type="checkbox"/> | 1/0/2  | Enabled                                         | Enabled                                         | --  |
| <input checked="" type="checkbox"/> | 1/0/3  | Enabled                                         | Enabled                                         | --  |
| <input checked="" type="checkbox"/> | 1/0/4  | Enabled                                         | Enabled                                         | --  |
| <input checked="" type="checkbox"/> | 1/0/5  | Enabled                                         | Enabled                                         | --  |
| <input type="checkbox"/>            | 1/0/6  | Disabled                                        | Disabled                                        | --  |
| <input type="checkbox"/>            | 1/0/7  | Disabled                                        | Disabled                                        | --  |
| <input type="checkbox"/>            | 1/0/8  | Disabled                                        | Disabled                                        | --  |
| <input type="checkbox"/>            | 1/0/9  | Disabled                                        | Disabled                                        | --  |
| <input type="checkbox"/>            | 1/0/10 | Disabled                                        | Disabled                                        | --  |

Total: 10
4 entries selected.

Cancel

Apply

- 4) Kliknij  **Save**, aby zapisać ustawienia.

## 2.4 Przez CLI

```
Switch#configure
```

```
Switch(config)#monitor session 1 destination interface fastEthernet 1/0/1
```

```
Switch(config)#monitor session 1 source interface fastEthernet 1/0/2-5 both
```

```
Switch(config)#end
```

```
Switch#copy running-config startup-config
```

### Sprawdzanie konfiguracji

```
Switch#show monitor session 1
```

```
Monitor Session: 1
```

```
Destination Port: Fa1/0/1
```

```
Source Ports(Ingress): Fa1/0/2-5
```

```
Source Ports(Egress): Fa1/0/2-5
```

# Część 31

## Konfiguracja DLDP

### ROZDZIAŁY

1. Informacje ogólne
2. Konfiguracja DLDP

# 1 Informacje ogólne

DLDP (Device Link Detection Protocol) to protokół warstwy, który pozwala urządzeniom podłączonym za pomocą światłowodu lub skrętki Ethernetowej wykryć, czy istnieje łącze jednokierunkowe.

Łącze jednokierunkowe występuje, gdy ruch wysyłany przez urządzenie lokalne jest odbierany przez urządzenie równorzędne, ale ruch z urządzenia równorzędnego nie jest odbierany przez urządzenie lokalne.

Łącza jednokierunkowe mogą powodować różne problemy, w tym pętle topologii drzewa rozpinającego. Po wykryciu takiego łącza DLDP automatycznie wyłącza odpowiedni port lub wysyła powiadomienie do użytkowników.

# 2 Konfiguracja DLDP

## Wskazówki dotyczące konfiguracji

- Port obsługujący DLDP nie może wykryć łącza jednokierunkowego, jeżeli jest podłączony do portu nieobsługującego DLDP innego przełącznika.
- Aby wykrywać łącza jednokierunkowe, upewnij się, że technologia DLDP jest włączona po obu stronach łącza.

## 2.1 Przez GUI

Wybierz z menu **MAINTENANCE > DLDP**, aby wyświetlić poniższą stronę.

Rys. 2-1 Konfiguracja DLDP

Global Config

---

DLDP:  Enable

Advertisement Interval:  seconds (1-30)

Shut Mode:  Auto  Manual

Auto Refresh:  Enable

Refresh Interval:  seconds (1-100)

[Apply](#)

---

Port Config

UNIT1

|                                     | Port   | DLDP     | Protocol State | Link State | Neighbour State |
|-------------------------------------|--------|----------|----------------|------------|-----------------|
| <input checked="" type="checkbox"/> | 1/0/1  | Disabled | Initial        | Link-Down  | N/A             |
| <input type="checkbox"/>            | 1/0/2  | Disabled | Initial        | Link-Down  | N/A             |
| <input type="checkbox"/>            | 1/0/3  | Disabled | Initial        | Link-Down  | N/A             |
| <input type="checkbox"/>            | 1/0/4  | Disabled | Initial        | Link-Down  | N/A             |
| <input type="checkbox"/>            | 1/0/5  | Disabled | Initial        | Link-Down  | N/A             |
| <input type="checkbox"/>            | 1/0/6  | Disabled | Initial        | Link-Down  | N/A             |
| <input type="checkbox"/>            | 1/0/7  | Disabled | Initial        | Link-Down  | N/A             |
| <input type="checkbox"/>            | 1/0/8  | Disabled | Initial        | Link-Up    | N/A             |
| <input type="checkbox"/>            | 1/0/9  | Disabled | Initial        | Link-Down  | N/A             |
| <input type="checkbox"/>            | 1/0/10 | Disabled | Initial        | Link-Down  | N/A             |

Total: 10 1 entry selected.

[Cancel](#)
[Apply](#)

Wykonaj poniższe kroki, aby skonfigurować DLDP:

- 1) W sekcji **Global Config** włącz DLDP i skonfiguruj odpowiednie parametry. Kliknij **Apply**.

|                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DLDP State             | Włącz lub wyłącz globalnie DLDP.                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Advertisement Interval | Skonfiguruj interwał wysyłania pakietów powiadamiających. Prawidłowe wartości wahają się od 1 do 30 sekund, a wartością domyślną jest 5 sekund.                                                                                                                                                                                                                                                                                                          |
| Shut Mode              | Wybierz sposób zamknięcia portu, gdy wykryte zostanie łącze jednokierunkowe:<br><br><b>Auto:</b> Gdy na porcie zostanie wykryte łącze jednokierunkowe, DLDP wygeneruje dzienniki i pułapki, a następnie zamknie port, a DLDP na tym porcie wyłączy się.<br><br><b>Manual:</b> Gdy na porcie zostanie wykryte łącze jednokierunkowe, DLDP wygeneruje dzienniki i pułapki. Następnie użytkownicy będą mogli ręcznie zamknąć porty łącza jednokierunkowego. |
| Auto Refresh           | Po zaznaczeniu tej opcji przełącznik będzie automatycznie odświeżać informacje o DLDP.                                                                                                                                                                                                                                                                                                                                                                   |
| Refresh Interval       | Ustaw częstotliwość odświeżania informacji o DLDP. Prawidłowe wartości wahają się od 1 do 100 sekund, a wartością domyślną są 3 sekundy.                                                                                                                                                                                                                                                                                                                 |

- 2) W sekcji **Port Config** wybierz co najmniej jeden port, włącz DLDP i kliknij **Apply**. W tabeli pojawią się informacje o DLDP.

|                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DLDP           | Włącz lub wyłącz DLDP na porcie.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Protocol State | Stan protokołu DLDP.<br><br><b>Initial:</b> DLDP jest wyłączony.<br><br><b>Inactive:</b> DLDP jest włączony, ale łącze nie działa.<br><br><b>Active:</b> DLDP jest włączony i łącze działa lub wpisy o urządzeniach sąsiadujących na tym urządzeniu są puste.<br><br><b>Advertisement:</b> Nie wykryto łącza jednokierunkowego (urządzenie ustanowiło dwukierunkowe połączenia ze wszystkimi urządzeniami sąsiadującymi) lub DLDP pozostało w stanie Active dłużej niż 5 sekund.<br><br><b>Probe:</b> Po przejściu w ten stan urządzenie wyśle pakiety sondujące, aby sprawdzić czy łącze jest jednokierunkowe. Port wchodzi w ten stan ze stanu Active, jeżeli odbierze pakiet od nieznanego urządzenia sąsiadującego.<br><br><b>Disable:</b> Wykryto łącze jednokierunkowe. |
| Link State     | Stan łącza.<br><br><b>Link-Down:</b> Łącze nie jest aktywne.<br><br><b>Link-Up:</b> Łącze jest aktywne.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |



|                 |                                                                                                                                                                                                                                                                                                 |
|-----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Neighbour State | <p>Stan urządzenia sąsiadującego.</p> <p><b>Unknown:</b> Trwa wykrywanie łącza.</p> <p><b>Unidirectional:</b> Łącze pomiędzy portem a urządzeniem sąsiadującym jest jednokierunkowe.</p> <p><b>Bidirectional:</b> Połączenie pomiędzy portem a urządzeniem sąsiadującym jest dwukierunkowe.</p> |
|-----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## 2.2 Przez CLI

Wykonaj poniższe kroki, aby skonfigurować DLDP:

|        |                                                                                                                                                                                                                                                                                                                                                                                                                   |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Krok 1 | <p><b>configure</b></p> <p>Uruchom tryb konfiguracji globalnej.</p>                                                                                                                                                                                                                                                                                                                                               |
| Krok 2 | <p><b>dldp</b></p> <p>Włącz globalnie DLDP.</p>                                                                                                                                                                                                                                                                                                                                                                   |
| Krok 3 | <p><b>dldp interval <i>interval-time</i></b></p> <p>Skonfiguruj interwał wysyłania pakietów powiadamiających na portach, które są w stanie powiadomień.</p> <p><i>interval-time:</i> Podaj wartość interwału. Prawidłowe wartości wahają się od 1 do 30 sekund, a wartością domyślną jest 5 sekund.</p>                                                                                                           |
| Krok 3 | <p><b>dldp shut-mode { auto   manual }</b></p> <p>Skonfiguruj tryb wyłączenia DLDP po wykryciu łącza jednokierunkowego.</p> <p><b>auto:</b> Przełącznik automatycznie zamyka porty, gdy wykryte zostanie łącze jednokierunkowe.</p> <p><b>manual:</b> Przełącznik wysyła powiadomienie, gdy wykryte zostanie łącze jednokierunkowe. Następnie użytkownicy mogą ręcznie zamknąć porty łącza jednokierunkowego.</p> |
| Krok 4 | <p><b>interface {fastEthernet <i>port</i>   range fastEthernet <i>port-list</i>   gigabitEthernet <i>port</i>   range gigabitEthernet <i>port-list</i>   ten-gigabitEthernet <i>port</i>   range ten-gigabitEthernet <i>port-list</i>}</b></p> <p>Uruchom tryb konfiguracji globalnej.</p>                                                                                                                        |
| Krok 5 | <p><b>dldp</b></p> <p>Włącz DLDP na wybranym porcie.</p>                                                                                                                                                                                                                                                                                                                                                          |
| Krok 6 | <p><b>show dldp</b></p> <p>Przejrzyj globalną konfigurację DLDP.</p>                                                                                                                                                                                                                                                                                                                                              |
| Krok 7 | <p><b>show dldp interface</b></p> <p>Przejrzy konfigurację DLDP portów.</p>                                                                                                                                                                                                                                                                                                                                       |

---

|        |                                                                                         |
|--------|-----------------------------------------------------------------------------------------|
| Krok 8 | <b>end</b><br>Powróć do trybu privileged EXEC.                                          |
| Krok 9 | <b>copy running-config startup-config</b><br>Zapisz ustawienia w pliku konfiguracyjnym. |

---

Poniższy schemat przedstawia przykładowy sposób globalnego włączania DLDP, ustawiania interwału DLDP jako 10 sekund i trybu wyłączenia DLDP jako auto.

**Switch#configure**

**Switch(config)#dldp**

**Switch(config)#dldp interval 10**

**Switch(config)#dldp shut-mode auto**

**Switch(config)#show dldp**

DLDP Global State: Enable

DLDP Message Interval: 10

DLDP Shut Mode: Auto

**Switch(config)#end**

**Switch#copy running-config startup-config**

Poniższy schemat przedstawia przykładowy sposób włączania DLDP na porcie 1/0/1.

**Switch#configure**

**Switch(config)#interface gigabitEthernet 1/0/1**

**Switch(config-if)#dldp**

**Switch(config-if)#show dldp interface**

| Port    | DLDP State | Protocol State | Link State | Neighbor State |
|---------|------------|----------------|------------|----------------|
| ----    | -----      | -----          | -----      | -----          |
| Gi1/0/1 | Enable     | Inactive       | Link-Down  | N/A            |
| Gi1/0/2 | Disable    | Initial        | Link-Down  | N/A            |

...

**Switch(config-if)#end**

**Switch#copy running-config startup-config**

# Część 32

## Konfiguracja SNMP i RMON

### ROZDZIAŁY

1. SNMP
2. Konfiguracja SNMP
3. Konfiguracja powiadomień
4. RMON
5. Konfiguracja RMON
6. Przykład konfiguracji

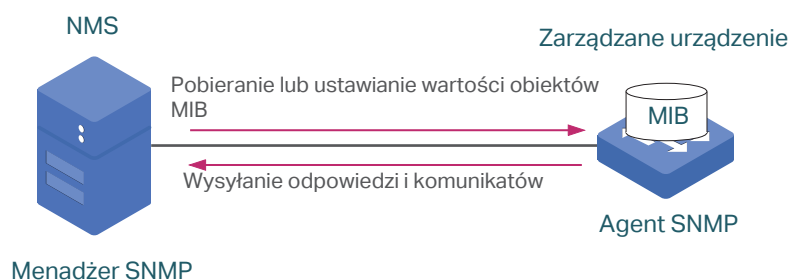
# 1 SNMP

## 1.1 Informacje ogólne

SNMP (Simple Network Management Protocol) to standardowy protokół zarządzania siecią, szeroko stosowany w sieciach TCP/IP. Umożliwia zarządzanie urządzeniami za pomocą oprogramowania NMS (Network Management System). Korzystając z SNMP, administratorzy sieci mogą przeglądać i modyfikować informacje o urządzeniach sieciowych, a także rozwiązywać na bieżąco problemy identyfikowane za pomocą komunikatów wysyłanych przez te urządzenia.

Jak pokazano na poniższym schemacie, system SNMP składa się z menadżera SNMP, agenta SNMP oraz MIB (Management Information Base). Menadżer SNMP może być częścią NMS, np. tpNMS. Agent i MIB znajdują się na zarządzanym urządzeniu, takim jak przełącznik, router, host lub drukarka sieciowa. Aby skonfigurować SNMP na przełączniku, konieczne jest określenie relacji pomiędzy menadżerem a agentem.

Rys. 1-1 System SNMP



## 1.2 Podstawowe założenia

Poniżej omówiono podstawowe dla SNMP pojęcia: menadżer SNMP, agent SNMP, MIB (Management Information Base), jednostka SNMP, silnik SNMP i wersja SNMP.

### SNMP Manager

Menadżer SNMP korzysta z SNMP do monitorowania i kontrolowania agentów SNMP, zapewniając administratorowi wygodny interfejs zarządzania urządzeniami sieciowymi. Może pozyskiwać wartości obiektów MIB od agenta lub zapisywać wartość obiektu MIB w agencie, a także otrzymywać od agentów komunikaty informujące o stanie sieci.

### SNMP Agent

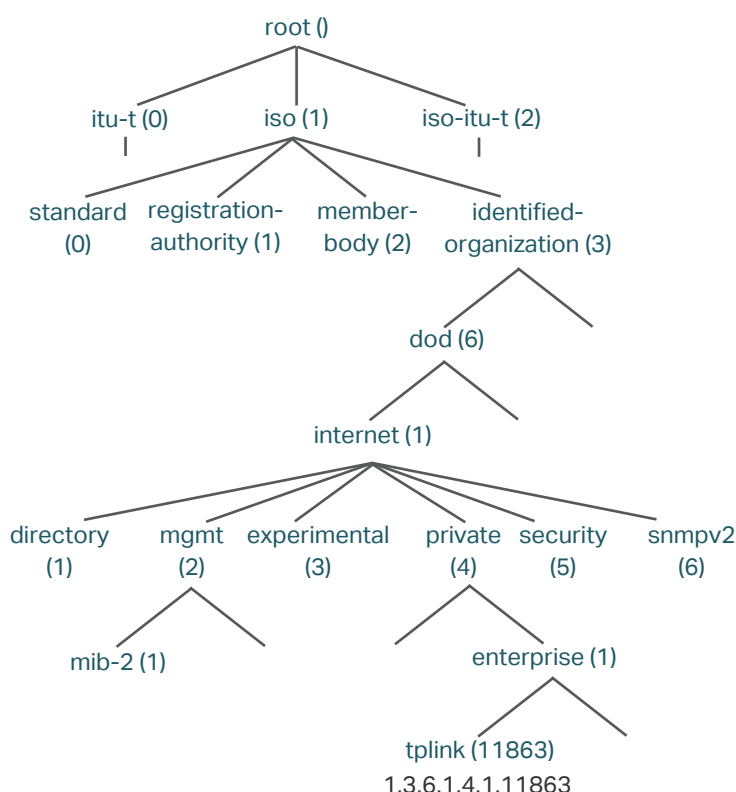
Agent SNMP jest to proces uruchamiany na zarządzanym urządzeniu. Zawiera obiekty MIB, których wartości menadżer SNMP może zarządzać lub zmieniać. Agent może wysyłać nieoczekiwane komunikaty trap w celu powiadomienia menadżera SNMP o istotnym zdarzeniu na agencie.

## MIB

MIB jest to zbiór zorganizowanych hierarchicznie obiektów zarządzanych. Obiekty definiują atrybuty zarządzanego urządzenia, w tym nazwy, stan, prawa dostępu i typy danych. Każdy obiekt może być adresowany za pomocą identyfikatora obiektu (OID).

Jak pokazano na poniższym schemacie, hierarchię MIB można przedstawić w formie drzewa strukturalnego, którego poziomy ustalane są przez różne organizacje. Identyfikatory obiektów MIB najwyższego poziomu należą do różnych organizacji normalizacyjnych, natomiast identyfikatory obiektów niższego poziomu ustalane są przez powiązane organizacje. Producenci mogą definiować dla swoich produktów prywatne gałęzie, które uwzględniają zarządzane obiekty.

Rys. 1-2 Drzewo MIB



Przełączniki TP-Link zapewniają prywatne bazy MIB, identyfikowane za pomocą OID 1.3.6.1.4.1.11863. Pliki MIB dostępne są na dołączonej do produktu płycie CD lub w zakładce "Do pobrania" na oficjalnej stronie TP-Link: <http://www.tp-link.com/pl/support/download/>.

Przełączniki TP-Link obsługują także poniższe publiczne bazy MIB:

- LLDP.mib
- LLDP-Ext-Dot1.mib
- LLDP-Ext-MED.mib
- RFC1213.mib
- RFC1493-Bridge.mib
- RFC1757-RMON.mib

- RFC2618-RADIUS-Auth-Client.mib
- RFC2620-RADIUS-Acc-Client.mib
- RFC2674-pBridge.mib
- RFC2674-qBridge.mib
- RFC2863-pBridge.mib
- RFC2925-Disman-Ping.mib
- RFC2925-Disman-Traceroute.mib

Szczegółowe informacje dotyczące obsługiwanych publicznych baz MIB znajdują się w instrukcji *Supported Public MIBs for TP-Link Switches*, która znajduje się w zakładce "Instrukcje konfiguracji" na stronie TP-Link:

<https://www.tp-link.com/pl/configuration-guide/>

## SNMP Entity

Jednostka SNMP jest to urządzenie obsługujące protokół SNMP. Zarówno menadżer SNMP, jak i agent SNMP to jednostki SNMP.

## SNMP Engine

Silnik SNMP to część jednostki SNMP. Każda jednostka SNMP ma tylko jeden silnik. Zapewnia możliwość kończenia i wysyłania komunikatów, ich uwierzytelniania i szyfrowania oraz kontrolowania dostępu do zarządzanych obiektów.

Silnik SNMP można identyfikować w ramach domeny administracyjnej za pomocą unikalnego ID. Ponieważ pomiędzy silnikami SNMP a jednostkami SNMP istnieje relacja one-to-one, ID silnika może także służyć do jednoznacznej identyfikacji jednostki SNMP w ramach tej domeny administracyjnej.

## SNMP Version

Urządzenie obsługuje trzy wersje SNMP: SNMPv1, SNMPv2c oraz SNMPv3. *Tabela 1-1* zawiera listę funkcji obsługiwanych w różnych wersjach SNMP, a *Tabela 1-2* przedstawia możliwe zastosowania poszczególnych wersji.

Tabela 1-1 Funkcje obsługiwane w różnych wersjach SNMP

| Funkcja                    | SNMPv1                                        | SNMPv2c                                       | SNMPv3                                                                                             |
|----------------------------|-----------------------------------------------|-----------------------------------------------|----------------------------------------------------------------------------------------------------|
| Access Control             | Zależy od hasła (SNMP Community) i widoku MIB | Zależy od hasła (SNMP Community) i widoku MIB | Zależy od użytkownika i grupy SNMP oraz widoku MIB                                                 |
| Authentication and Privacy | Zależy od nazwy społeczności                  | Zależy od nazwy społeczności                  | Obsługiwane tryby uwierzytelniania i szyfrowania:<br>Uwierzytelnianie: MD5/SHA<br>Szyfrowanie: DES |
| Trap                       | Obsługiwana                                   | Obsługiwana                                   | Obsługiwana                                                                                        |

| Funkcja | SNMPv1         | SNMPv2c     | SNMPv3      |
|---------|----------------|-------------|-------------|
| Inform  | Nieobsługiwana | Obsługiwana | Obsługiwana |

Tabela 1-2 Zastosowania poszczególnych wersji

| Wersja  | Zastosowania                                                                                                                                                                                                                                                                                                                                                |
|---------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| SNMPv1  | Ma zastosowanie w przypadku małych sieci o nieskomplikowanej topologii, niskich wymaganiach względem zabezpieczeń lub dobrej stabilności (takich jak sieci kampusowe i sieci w małych firmach).                                                                                                                                                             |
| SNMPv2c | Ma zastosowanie w przypadku średnich i dużych sieci o niskich wymaganiach względem zabezpieczeń oraz sieci dobrze chronionych (takich jak VPN), ale z zajętymi usługami, w których możliwe jest wystąpienie przeciążeń. Aby upewnić się, że administratorzy sieci otrzymują powiadomienia od zarządzanych urządzeń, należy skonfigurować komunikaty Inform. |
| SNMPv3  | Ma zastosowanie dla sieci o różnej skali, zwłaszcza dla tych, które mają wysokie wymagania względem zabezpieczeń i w których urządzeniami zarządzać muszą uwierzytelnieni administratorzy (np. gdy dane są przesyłane w sieciach publicznych).                                                                                                              |

# 2 Konfiguracja SNMP

Aby przeprowadzić proces konfiguracji SNMP, wybierz wersję SNMP zgodnie z wymaganiami sieci i obsługą oprogramowania NMS, a następnie wykonaj poniższe kroki:

- Wybierając SNMPv1 lub SNMPv2c

- 1) Włącz SNMP.
- 2) Utwórz widok SNMP dla zarządzanych obiektów.
- 3) Utwórz społeczność (community), wybierz widok dostępu i odpowiednie uprawnienia dostępu.

- Wybierając SNMPv3

- 1) Włącz SNMP.
- 2) Utwórz widok SNMP dla zarządzanych obiektów.
- 3) Utwórz grupę SNMP i określ prawa dostępu.
- 4) Utwórz użytkowników SNMP i skonfiguruj tryb uwierzytelniania, tryb ochrony prywatności i odpowiednia hasła.

## 2.1 Przez GUI

### 2.1.1 Włączanie SNMP

Wybierz z menu **MAINTENANCE > SNMP > Global Config**, aby wyświetlić poniższą stronę.

Rys. 2-1 Konfiguracja globalna

| Port Config                         |        |            |          |     |
|-------------------------------------|--------|------------|----------|-----|
| <input type="checkbox"/>            | Port   | DDM Status | Shutdown | LAG |
| <input checked="" type="checkbox"/> | 1/0/9  | Enabled    | None     | --  |
| <input type="checkbox"/>            | 1/0/10 | Enabled    | None     | --  |

Wykonaj poniższe kroki, aby skonfigurować globalnie SNMP:

- 1) W sekcji **Global Config** włącz SNMP i skonfiguruj lokalny i zdalny engine ID.

|      |                                  |
|------|----------------------------------|
| SNMP | Włącz lub wyłącz globalnie SNMP. |
|------|----------------------------------|



**Local Engine ID** Ustaw engine ID lokalnego agenta SNMP (przełącznika) używając od 10 do 64 znaków szesnastkowych. Domyślnie przełącznik generuje engine ID korzystając z PEN firmy TP-Link (80002e5703) i własnego adresu MAC.

Lokalny engine ID to unikalny ciąg znaków alfanumerycznych stosowany do identyfikacji silnika SNMP. Agent SNMP ma tylko jeden silnik SNMP, dlatego za pomocą lokalnego engine ID można jednoznacznie zidentyfikować agenta SNMP.

**Remote Engine ID** Ustaw ID zdalnego menadżera SNMP, używając od 10 do 64 znaków szesnastkowych. Jeżeli nie jest potrzebny żaden zdalny menedżer SNMP, możesz pozostawić to pole puste.

Zdalny engine ID to unikalny ciąg znaków alfanumerycznych stosowany do identyfikacji silnika SNMP urządzenia zdalnego, które otrzymuje od przełącznika komunikaty inform.

## 2) Kliknij **Apply**.









### Uwaga:

- Engine ID musi zawierać parzystą liczbę znaków.
- Zmiana wartości engine ID SNMP ma istotne konsekwencje. W wersji SNMPv3 hasło użytkownika jest konwertowane na kryptograficzną funkcję skrótu MD5 lub SHA w oparciu o hasło i ID silnika. Gdy wartość engine ID ulega zmianie, przełącznik automatycznie usuwa wszystkich lokalnych użytkowników SNMPv3, ponieważ ich algorytm kryptograficzny traci ważność. Tak samo wszyscy zdalni użytkownicy SNMPv3 są usuwani, gdy wartość zdalnego engine ID ulega zmianie.

## 2.1.2 Tworzenie widoku SNMP


Wybierz z menu **MAINTENANCE > SNMP > Global Config**, aby wyświetlić poniższą stronę.

Rys. 2-2 Konfiguracja widoku SNMP

| SNMP View Config         |       |             |           |                |                                                                                                                                                                             |
|--------------------------|-------|-------------|-----------|----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <input type="checkbox"/> | Index | View Name   | View Type | MIB Object ID  | Operation                                                                                                                                                                   |
| <input type="checkbox"/> | 1     | viewDefault | Include   | 1              |   |
| <input type="checkbox"/> | 2     | viewDefault | Exclude   | 1.3.6.1.6.3.15 |   |
| <input type="checkbox"/> | 3     | viewDefault | Exclude   | 1.3.6.1.6.3.16 |   |
| <input type="checkbox"/> | 4     | viewDefault | Exclude   | 1.3.6.1.6.3.18 |   |
| Total: 4                 |       |             |           |                |                                                                                                                                                                             |

NMS zarządza obiektami bazy MIB w oparciu o widok SNMP. Widok SNMP jest podzbiorem bazy MIB. System zapewnia domyślny widok o nazwie viewDefault, ale możesz także tworzyć inne widoki SNMP, stosownie do wymagań.

Wykonaj poniższe kroki, aby skonfigurować widok SNMP:

- 1) Kliknij  **Add**, aby wyświetlić poniższą stronę. Podaj nazwę widoku oraz wybierz typ widoku i obiekt bazy MIB, który będzie powiązany z widokiem.

Rys. 2-3 Tworzenie widoku SNMP

|                      |                                                                                                                                                                                                                                                                              |
|----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>View Name</b>     | Podaj nazwę widoku wpisując od 1 do 16 znaków. W pełni skonfigurowany widok składa się z obiektów bazy MIB o tej samej nazwie widoku.                                                                                                                                        |
| <b>View Type</b>     | Ustaw, które obiekty bazy MIB mają należeć do widoku. Domyślnie obiekt należy do widoku.<br><br><b>Include:</b> NMS może wyświetlać lub zarządzać funkcją wskazaną przez obiekt.<br><br><b>Exclude:</b> NMS nie może wyświetlać ani zarządzać funkcją wskazaną przez obiekt. |
| <b>MIB Object ID</b> | Wpisz identyfikator obiektu (OID) bazy MIB, aby określić funkcję urządzenia. Podanie OID bazy MIB określa wszystkie child OIDs. Szczegółowe reguły ID znajdują się w bazach MIB powiązanych z urządzeniami.                                                                  |

2) Kliknij **Create**.

### 2.1.3 Tworzenie społeczności SNMP (SNMP v1/v2c)

Wybierz z menu **MAINTENANCE > SNMP > SNMP v1/v2c** i kliknij  **Add**, aby wyświetlić poniższą stronę.

Rys. 2-4 Tworzenie SNMP Community

1) Podaj nazwę społeczności, określ uprawnienia dostępu i powiązany widok.

|                       |                                                                                                                                  |
|-----------------------|----------------------------------------------------------------------------------------------------------------------------------|
| <b>Community Name</b> | Skonfiguruj nazwę społeczności, która będzie pełnił rolę hasła dostępu dla NMS do obiektów bazy MIB w agencie SNMP przełącznika. |
|-----------------------|----------------------------------------------------------------------------------------------------------------------------------|

|                    |                                                                                                                                                                                                                                                                                   |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Access Mode</b> | Wybierz tryb dostępu do powiązanego widoku. Domyślnym ustawieniem jest read-only.<br><br><b>Read Only:</b> NMS może wyświetlać, ale nie może zmieniać parametrów określonego widoku.<br><br><b>Read &amp; Write:</b> NMS może wyświetlać i zmieniać parametry określonego widoku. |
| <b>MIB View</b>    | Wybierz widok SNMP, który zezwala na dostęp community. Domyślnym widokiem jest viewDefault.                                                                                                                                                                                       |

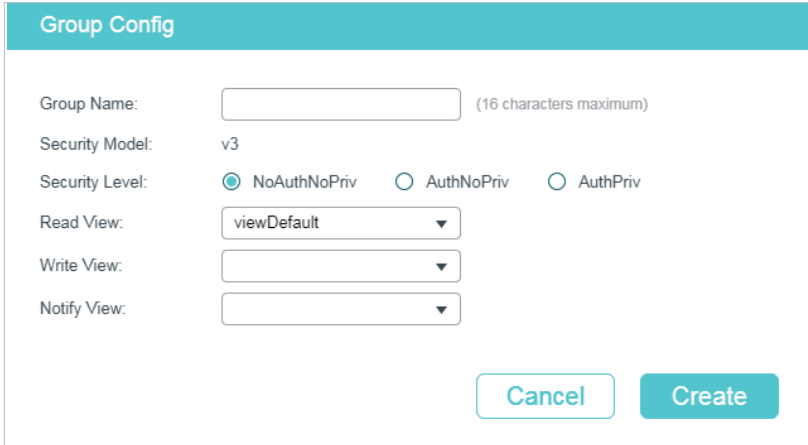
2) Kliknij **Create**.

## 2.1.4 Tworzenie grupy SNMP (SNMP v3)

Utwórz grupę SNMP i skonfiguruj odpowiednie parametry.

Wybierz z menu **MAINTENANCE > SNMP > SNMP v3 > SNMP Group** i kliknij  **Add**, aby wyświetlić poniższą stronę.

Rys. 2-5 Tworzenie grupy SNMP



Wykonaj poniższe kroki, aby utworzyć grupę SNMP:

1) Podaj nazwę grupy, a następnie ustaw poziom zabezpieczeń oraz widok odczytu, zapisu i powiadomień.

|                       |                                                                                                                                                                                                                     |
|-----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Group Name</b>     | Podaj nazwę grupy SNMP używając od 1 do 16 znaków.<br><br>Identyfikator grupy składa się z nazwy grupy, modelu zabezpieczeń i poziomu zabezpieczeń. Grupy o tym samym identyfikatorze uznawane są za te same grupy. |
| <b>Security Model</b> | Model zabezpieczeń. SNMPv3 korzysta z wersji 3, która zapewnia najwyższy poziom bezpieczeństwa.                                                                                                                     |

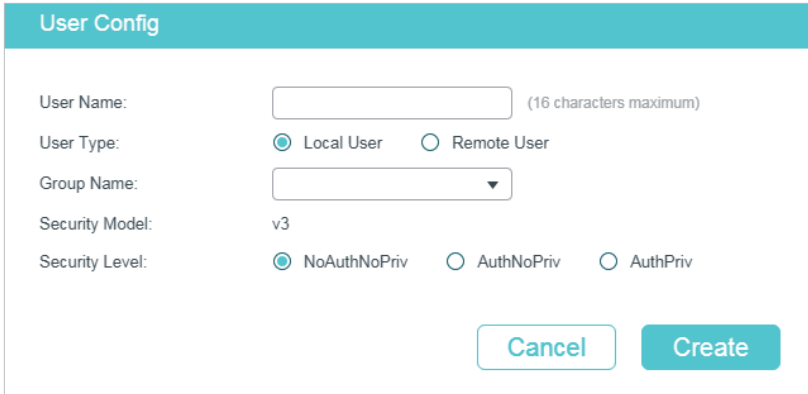
|                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Security Level | <p>Ustaw poziom zabezpieczeń dla grupy SNMPv3. Domyślnym ustawieniem jest NoAuthNoPriv.</p> <p><b>NoAuthNoPriv:</b> Pakiety nie są sprawdzane ani szyfrowane, ponieważ nie zastosowano trybu uwierzytelniania ani trybu ochrony prywatności.</p> <p><b>AuthNoPriv:</b> Pakiety są sprawdzane w trybie uwierzytelniania, ale nie są szyfrowane, ponieważ nie zastosowano trybu ochrony prywatności.</p> <p><b>AuthPriv:</b> Zastosowano tryb uwierzytelniania i tryb ochrony prywatności, dlatego pakiety są sprawdzane i szyfrowane.</p> |
| Read View      | Wybierz ten widok, aby zezwolić na wyświetlanie parametrów przez NMS. Modyfikowanie ich przez NMS nie będzie jednak możliwe. Wybór widoku jest konieczny dla każdej grupy. Widokiem domyślnym jest viewDefault. Zmiana parametrów widoku możliwa jest tylko w widoku zapisu.                                                                                                                                                                                                                                                             |
| Write View     | Wybierz ten widok, aby zezwolić na zmianę parametrów przez NMS. Wyświetlanie ich przez NMS nie będzie jednak możliwe. Widokiem domyślnym jest none. Widok zapisu wymaga włączenia widoku odczytu.                                                                                                                                                                                                                                                                                                                                        |
| Notify View    | Wybierz ten widok, aby zezwolić na wysyłanie powiadomień do NMS.                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |

2) Kliknij **Create**.

## 2.1.5 Tworzenie użytkowników SNMP (SNMP v3)

Wybierz z menu **MAINTENANCE > SNMP > SNMP v3 > SNMP User** i kliknij  Add , aby wyświetlić poniższą stronę.

Rys. 2-6 Tworzenie użytkownika SNMP



**User Config**

User Name:  (16 characters maximum)

User Type:  Local User  Remote User

Group Name:

Security Model: v3

Security Level:  NoAuthNoPriv  AuthNoPriv  AuthPriv

Wykonaj poniższe kroki, aby utworzyć użytkownika SNMP:

1) Podaj nazwę użytkownika, typ użytkownika i grupę, do której należy użytkownik. Następnie skonfiguruj poziom zabezpieczeń.

|           |                                                                                                     |
|-----------|-----------------------------------------------------------------------------------------------------|
| User Name | Podaj nazwę użytkownika SNMP używając od 1 do 16 znaków. Nazwy użytkowników nie mogą się powtarzać. |
|-----------|-----------------------------------------------------------------------------------------------------|

|                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| User Type      | <p>Wybierz typ użytkownika, aby określić jego lokalizację. Domyślnym ustawieniem jest Local User.</p> <p><b>Local User:</b> Użytkownik korzysta z lokalnego silnika, który jest agentem SNMP przełącznika.</p> <p><b>Remote User:</b> Użytkownik korzysta z NMS. Ze względu na to, że zdalny engine ID i hasło użytkownika są używane do obliczania skrótu uwierzytelniania i ochrony prywatności, przed skonfigurowaniem użytkownika zdalnego należy ustawić zdalny engine ID.</p>                                                                                                                                                                                                                  |
| Group Name     | Wybierz grupę, do której należy użytkownik. Użytkownicy o tej samej nazwie grupy, modelu zabezpieczeń i poziomie zabezpieczeń będą należeć do tej samej grupy.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Security Model | Model zabezpieczeń. SNMPv3 korzysta z wersji 3, która zapewnia najwyższy poziom bezpieczeństwa.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Security Level | <p>Ustaw poziom zabezpieczeń dla grupy SNMPv3. Poziomy zabezpieczeń od najwyższego do najniższego układają się następująco: NoAuthNoPriv, AuthNoPriv, AuthPriv. Ustawieniem domyślnym jest NoAuthNoPriv. Poziom zabezpieczeń użytkownika nie powinien być niższy niż grupy, do której należy.</p> <p><b>NoAuthNoPriv:</b> Do uwierzytelnienia dostępu wymagana jest nazwa użytkownika. Brak szyfrowania.</p> <p><b>AuthNoPriv:</b> Pakiety są sprawdzane w trybie uwierzytelniania, ale nie są szyfrowane, ponieważ nie zastosowano trybu ochrony prywatności.</p> <p><b>AuthPriv:</b> Zastosowano tryb uwierzytelniania i tryb ochrony prywatności, dlatego pakiety są sprawdzane i szyfrowane.</p> |

- 2) Jeżeli wybierzesz **AuthNoPriv** lub **AuthPriv**, musisz odpowiednio ustawić tryb uwierzytelniania lub tryb ochrony prywatności. W innym wypadku pomiń ten krok.

|                         |                                                                                                                                                                                                                                                                                                                                                               |
|-------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Authentication Mode     | <p>Jeżeli wybierzesz AuthNoPriv lub AuthPriv, skonfiguruj tryb uwierzytelniania i hasło. Do wyboru są dwa tryby uwierzytelniania:</p> <p><b>MD5:</b> Uwierzytelniaj za pomocą algorytmu HMAC-MD5.</p> <p><b>SHA:</b> Uwierzytelniaj za pomocą algorytmu SHA (Secure Hash Algorithm). Algorytm SHA zapewnia wyższy poziom bezpieczeństwa niż algorytm MD5.</p> |
| Authentication Password | Ustaw hasło uwierzytelniające.                                                                                                                                                                                                                                                                                                                                |
| Privacy Mode            | Jeżeli wybierzesz AuthPriv, skonfiguruj tryb ochrony prywatności i hasło szyfrowania. Przełącznik używa algorytmu DES (Data Encryption Standard) do szyfrowania.                                                                                                                                                                                              |
| Privacy Password        | Ustaw hasło szyfrowania.                                                                                                                                                                                                                                                                                                                                      |

- 3) Kliknij **Create**.

## 2.2 Przez CLI

### 2.2.1 Włączanie SNMP

---

|        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Krok 1 | <b>configure</b><br>Uruchom tryb konfiguracji globalnej.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Krok 2 | <b>snmp-server</b><br>Włączanie SNMP.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Krok 3 | <b>snmp-server engineID</b> {[ <i>local local-engineID</i> ] [ <i>remote remote-engineID</i> ]}<br>Skonfiguruj lokalny engine ID i zdalny engine ID.<br><br><i>local-engineID</i> : Ustaw engine ID lokalnego agenta SNMP (przełącznika) używając od 10 do 64 znaków szesnastkowych. Domyślnie przełącznik generuje engine ID korzystając z PEN firmy TP-LINK (80002e5703) i własnego adresu MAC.<br><br>Lokalny engine ID to unikalny ciąg znaków alfanumerycznych stosowany do identyfikacji silnika SNMP. Agent SNMP ma tylko jeden silnik SNMP, dlatego za pomocą lokalnego engine ID można jednoznacznie zidentyfikować agenta SNMP.<br><br><i>remote-engineID</i> : Ustaw ID zdalnego menadżera SNMP używając od 10 do 64 znaków szesnastkowych. Identyfikator musi zawierać parzystą liczbę znaków. Zdalny engine ID to unikalny ciąg znaków alfanumerycznych stosowany do identyfikacji silnika SNMP urządzenia zdalnego, które otrzymuje od przełącznika komunikaty inform.<br><br><i>Note:</i><br><br>Zmiana wartości engine ID SNMP ma istotne konsekwencje. W wersji SNMPv3 hasło użytkownika jest konwertowane na kryptograficzną funkcję skrótu MD5 lub SHA w oparciu o hasło i engine ID. Gdy wartość engine ID ulega zmianie, przełącznik automatycznie usuwa wszystkich lokalny użytkowników SNMPv3, ponieważ ich algorytm kryptograficzny traci ważność. Tak samo wszyscy zdalni użytkownicy SNMPv3 są usuwani, gdy wartość zdalnego engine ID ulega zmianie. |
| Krok 4 | <b>show snmp-server</b><br>Przejrzyj globalne ustawienia SNMP.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Krok 5 | <b>show snmp-server engineID</b><br>Sprawdź engine ID SNMP.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Krok 6 | <b>end</b><br>Powróć do trybu privileged EXEC.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Krok 7 | <b>copy running-config startup-config</b><br>Zapisz ustawienia w pliku konfiguracyjnym.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |

---

Poniższy schemat przedstawia przykładowy sposób włączania SNMP i ustawiania 123456789a jako zdalnego engine ID:

**Switch#configure**

```
Switch(config)#snmp-server
```

```
Switch(config)#snmp-server engineID remote 123456789a
```

```
Switch(config)#show snmp-server
```

```
SNMP agent is enabled.
```

```
0 SNMP packets input
```

```
0 Bad SNMP version errors
```

```
0 Unknown community name
```

```
0 Illegal operation for community name supplied
```

```
0 Encoding errors
```

```
0 Number of requested variables
```

```
0 Number of altered variables
```

```
0 Get-request PDUs
```

```
0 Get-next PDUs
```

```
0 Set-request PDUs
```

```
0 SNMP packets output
```

```
0 Too big errors (Maximum packet size 1500)
```

```
0 No such name errors
```

```
0 Bad value errors
```

```
0 General errors
```

```
0 Response PDUs
```

```
0 Trap PDUs
```

```
Switch(config)#show snmp-server engineID
```

```
Local engine ID: 80002e5703000aeb13a23d
```

```
Remote engine ID: 123456789a
```

```
Switch(config)#end
```

```
Switch#copy running-config startup-config
```

## 2.2.2 Tworzenie widoku SNMP

Podaj identyfikator obiektu (OID) widoku, aby określić zarządzane obiekty.

---

Krok 1

**configure**

Uruchom tryb konfiguracji globalnej.

---

|        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Krok 2 | <p><b>snmp-server view</b> <i>name mib-oid</i> {include   exclude}</p> <p>Skonfiguruj widok.</p> <p><i>name</i>: Podaj nazwę widoku wpisując 1 - 16 znaków. Możesz dodać wiele wpisów z powiązаныmi obiektami bazy MIB. W pełni skonfigurowany widok składa się z obiektów bazy MIB o tej samej nazwie widoku.</p> <p><i>mib-oid</i>: Podaj identyfikator obiektu bazy MIB używając od 1 do 61 znaków.</p> <p>include   exclude: Określ typ widoku. Include oznacza, że obiekty widoku mogą być zarządzane przez NMS, natomiast exclude wyklucza zarządzanie obiektów przez NMS.</p> |
| Krok 3 | <p><b>show snmp-server view</b></p> <p>Wyświetla tabelę widoków.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Krok 4 | <p><b>end</b></p> <p>Powróć do trybu privileged EXEC.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Krok 5 | <p><b>copy running-config startup-config</b></p> <p>Zapisz ustawienia w pliku konfiguracyjnym.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |

Poniższy schemat przedstawia przykładowy sposób konfiguracji zezwolenia na zarządzanie wszystkimi funkcjami przez NMS dla widoku. Nazwą widoku będzie View:

**Switch#configure**

**Switch(config)#snmp-server view** View 1 include

**Switch(config)#show snmp-server view**

| No. | View Name   | Type    | MOID           |
|-----|-------------|---------|----------------|
| --- | -----       | -----   | ----           |
| 1   | viewDefault | include | 1              |
| 2   | viewDefault | exclude | 1.3.6.1.6.3.15 |
| 3   | viewDefault | exclude | 1.3.6.1.6.3.16 |
| 4   | viewDefault | exclude | 1.3.6.1.6.3.18 |
| 5   | View        | include | 1              |

**Switch(config)#end**

**Switch#copy running-config startup-config**

### 2.2.3 Tworzenie społeczności SNMP (SNMP v1/v2c)

W przypadku SNMPv1 i SNMPv2c nazwa społeczności, pełniąc rolę hasła, będzie używana do uwierzytelniania dostępu.



|        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Krok 1 | <b>configure</b><br>Uruchom tryb konfiguracji globalnej.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Krok 2 | <b>snmp-server community name { read-only   read-write } [mib-view]</b><br>Skonfiguruj społeczność.<br><i>name</i> : Podaj nazwę grupy używając od 1 do 16 znaków.<br><i>read-only   read-write</i> : Wybierz uprawnienia dostępu dla społeczności. Read-only oznacza, że NMS może wyświetlać, ale nie może zmieniać parametrów widoku, natomiast read-write oznacza, że NMS może zarówno wyświetlać, jak i zmieniać parametry.<br><i>mib-view</i> : Wybierz widok, aby zezwolić społeczności na dostęp. Nazwa może zawierać od 1 do 61 znaków. Domyślnym widokiem jest viewDefault. |
| Krok 3 | <b>show snmp-server community</b><br>Wyświetla wpisy społeczności.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Krok 4 | <b>end</b><br>Powróć do trybu privileged EXEC.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Krok 5 | <b>copy running-config startup-config</b><br>Zapisz ustawienia w pliku konfiguracyjnym.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |

Poniższy schemat przedstawia przykładowy sposób ustawiania SNMP community. Nazwą społeczności będzie nms-monitor, a NMS będzie mieć zezwolenie na wyświetlanie i zmianę parametrów widoku View:

**Switch#configure**

**Switch(config)#snmp-server community nms-monitor read-write View**

**Switch(config)#show snmp-server community**

| Index | Name        | Type       | MIB-View |
|-------|-------------|------------|----------|
| ----- | -----       | -----      | -----    |
| 1     | nms-monitor | read-write | View     |

**Switch(config)#end**

**Switch#copy running-config startup-config**

## 2.2.4 Tworzenie grupy SNMP (SNMPv3)

Utwórz grupę SNMP i ustaw kontrolę dostępu użytkownika za pomocą widoków odczytu, zapisu i powiadomień. Ustaw także tryby uwierzytelniania i ochrony prywatności, aby zabezpieczyć komunikację między NMS a zarządzanymi urządzeniami.

|        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Krok 1 | <b>configure</b><br>Uruchom tryb konfiguracji globalnej.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Krok 2 | <b>snmp-server group name [ smode v3 ] [ slev {noAuthNoPriv   authNoPriv   authPriv} ] [ read read-view ] [ write write-view ] [ notify notify-view ]</b><br>Utwórz grupę SNMP.<br><br><i>name:</i> Podaj nazwę grupy SNMP używając od 1 do 16 znaków. Identyfikator grupy składa się z nazwy grupy, modelu zabezpieczeń i poziomu zabezpieczeń. Grupy o tym samym identyfikatorze uznawane są za te same grupy.<br><br><i>v3:</i> Skonfiguruj model zabezpieczeń dla grupy. SNMPv3 korzysta z wersji 3, która zapewnia najwyższy poziom bezpieczeństwa.<br><br><i>noAuthNoPriv   authNoPriv   authPriv:</i> Wybierz poziom zabezpieczeń spośród noAuthNoPriv (brak uwierzytelniania i szyfrowania), authNoPriv (uwierzytelnianie i brak szyfrowania), authPriv (uwierzytelnianie i szyfrowanie). Ustawieniem domyślnym jest noAuthNoPriv. Jeżeli wybranym modelem zabezpieczeń jest wersja 1 lub wersja 2, poziom zabezpieczeń nie może być skonfigurowany.<br><br><i>read-view:</i> Gdy ustawisz widok odczytu, NMS będzie mógł wyświetlać parametry określonego widoku.<br><br><i>write-view:</i> Gdy ustawisz widok zapisu, NMS będzie mógł zmieniać parametry określonego widoku. Pamiętaj, że widok zapisu wymaga włączenia widoku odczytu.<br><br><i>notify-view:</i> Gdy ustawisz widok powiadomień, NMS będzie mógł otrzymywać powiadomienia dotyczące określonego widoku od agenta. |
| Krok 3 | <b>show snmp-server group</b><br>Wyświetla wpisy grupy SNMP.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Krok 4 | <b>end</b><br>Powróć do trybu privileged EXEC.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Krok 5 | <b>copy running-config startup-config</b><br>Zapisz ustawienia w pliku konfiguracyjnym.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |

Poniższy schemat przedstawia przykładowy sposób tworzenia grupy SNMPv3 o nazwie nms1, ustawiania zabezpieczeń na poziomie authPriv, oraz widoku odczytu i powiadomień jako View1:

### Switch#configure

```
Switch(config)#snmp-server group nms1 smode v3 slev authPriv read View1 notify View1
```

### Switch(config)#show snmp-server group

| No. | Name  | Sec-Mode | Sec-Lev  | Read-View | Write-View | Notify-View |
|-----|-------|----------|----------|-----------|------------|-------------|
| --- | ----- | -----    | -----    | -----     | -----      | -----       |
| 1   | nms1  | v3       | authPriv | View1     |            | View1       |

```
Switch(config)#end
```

```
Switch#copy running-config startup-config
```

## 2.2.5 Tworzenie użytkowników SNMP (SNMPv3)

Skonfiguruj użytkowników grupy SNMP. Użytkownicy należący do grupy korzystają z tego samego poziomu zabezpieczeń i uprawnień dostępu co grupa.

|        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Krok 1 | <p><b>configure</b></p> <p>Uruchom tryb konfiguracji globalnej.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Krok 2 | <p><b>snmp-server user</b> <i>name</i> { local   remote } <i>group-name</i> [ <b>smode</b> v3 ] [ <b>slev</b> { noAuthNoPriv   authNoPriv   authPriv } ] [ <b>cmode</b> { none   MD5   SHA } ] [ <b>cpwd</b> <i>confirm-pwd</i> ] [ <b>emode</b> { none   DES } ] [ <b>epwd</b> <i>encrypt-pwd</i> ]</p> <p>Skonfiguruj użytkowników grupy SNMP.</p> <p><i>name</i>: Wprowadź nazwę użytkownika, wpisując od 1 do 16 znaków.</p> <p><i>local</i>   <i>remote</i>: Wybierz typ użytkownika. Typ Local oznacza, że użytkownik połączony jest z silnikiem lokalnym SNMP, natomiast remote oznacza, że użytkownika jest połączony z silnikiem zdalnym SNMP. Ze względu na to, że zdalny ID silnika i hasło użytkownika są używane do obliczania skrótu uwierzytelniania i ochrony prywatności, przed skonfigurowaniem użytkownika zdalnego należy ustawić zdalny ID silnika.</p> <p><i>group-name</i>: Podaj nazwę grupy, do której należy użytkownik. Grupę określa jej nazwa oraz tryb i poziom zabezpieczeń.</p> <p><i>v3</i>: Skonfiguruj tryb zabezpieczeń dla użytkownika. SNMPv3 korzysta z wersji 3, która zapewnia najwyższy poziom bezpieczeństwa..</p> <p><i>noAuthNoPriv</i>   <i>authNoPriv</i>   <i>authPriv</i>: Ustaw poziom zabezpieczeń dla grupy. Poziomy zabezpieczeń od najwyższego do najniższego układają się następująco: noAuthNoPriv (brak uwierzytelniania i brak szyfrowania), authNoPriv (uwierzytelnianie i brak szyfrowania) i authPriv (uwierzytelnianie i szyfrowanie). Ustawieniem domyślnym jest noAuthNoPriv. Poziom zabezpieczeń użytkownika nie powinien być niższy niż grupy, do której należy.</p> <p><i>none</i>   <i>MD5</i>   <i>SHA</i>: Wybierz algorytm uwierzytelniania. Algorytm SHA zapewnia wyższy poziom bezpieczeństwa niż algorytm. Domyślnym ustawieniem jest none.</p> <p><i>confirm-pwd</i>: Ustaw hasło uwierzytelniające, używając od 1 do 16 znaków, z wykluczeniem znaków zapytania i spacji. To hasło będzie wyświetlane w pliku konfiguracyjnym pod postacią szyfru symetrycznego.</p> <p><i>none</i>   <i>DES</i>: Wybierz tryb ochrony prywatności. None oznacza brak ustawień prywatności, natomiast DES wskazuje na użycie szyfrowania DES. Domyślnym ustawieniem jest none.</p> <p><i>encrypt-pwd</i>: Ustaw hasło ochrony prywatności, używając od 1 do 16 znaków, z wykluczeniem znaków zapytania i spacji. To hasło będzie wyświetlane w pliku konfiguracyjnym pod postacią szyfru symetrycznego.</p> |
| Krok 3 | <p><b>show snmp-server user</b></p> <p>Przejrzyj informacje o użytkownikach SNMP.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Krok 4 | <p><b>end</b></p> <p>Powróć do trybu privileged EXEC.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |

---

**Krok 5      copy running-config startup-config**

Zapisz ustawienia w pliku konfiguracyjnym.

---

Poniższy schemat przedstawia przykładowy sposób tworzenia użytkownika SNMP i dodawania go do grupy nms1. Nazwą użytkownika będzie admin, typem remote user, trybem zabezpieczeń SNMPv3, poziomem zabezpieczeń authPriv, algorytmem uwierzytelniania SHA, hasłem uwierzytelniającym 1234, algorytmem ochrony prywatności DES, a hasłem ochrony prywatności 1234:

**Switch#configure****Switch(config)#snmp-server user admin remote nms1 smode v3 slev authPriv cmode SHA cpwd 1234 emode DES epwd 1234****Switch(config)#show snmp-server user**

| No. | U-Name | U-Type | G-Name | S-Mode | S-Lev    | A-Mode | P-Mode |
|-----|--------|--------|--------|--------|----------|--------|--------|
| --- | -----  | -----  | -----  | -----  | -----    | -----  | -----  |
| 1   | admin  | remote | nms1   | v3     | authPriv | SHA    | DES    |

**Switch(config)#end****Switch#copy running-config startup-config**

# 3 Konfiguracja powiadomień

Po włączeniu powiadomień przełącznik będzie mógł wysyłać powiadomienia do NMS o ważnych zdarzeniach związanych z pracą urządzenia. Ułatwia to monitorowanie i zarządzanie NMS.

Wykonaj poniższe kroki, aby skonfigurować powiadomienia SNMP:

- 1) Skonfiguruj informacje o hostach NMS.
- 2) Włącz SNMP trap.

## Wskazówki dotyczące konfiguracji

Aby komunikację między przełącznikiem a NMS była możliwa, upewnij się, że przełącznik i NMS wykrywają się nawzajem.

## 3.1 Przez GUI

### 3.1.1 Konfiguracja informacji o hostach NMS

Wybierz z menu **MAINTENANCE > SNMP > Notification > Notification Config** i kliknij **+ Add**, aby wyświetlić poniższą stronę.

Rys. 3-1 Dodawanie hosta NMS

The screenshot shows the 'Notification Config' form with the following fields and options:

- IP Mode:** Radio buttons for IPv4 (selected) and IPv6.
- IP Address:** Text input field with a format hint '(Format:192.168.0.1)'. The field is currently empty.
- UDP Port:** Text input field with a range hint '(0-65535)'. The value '162' is entered.
- User:** Dropdown menu with 'admin' selected.
- Security Mode:** Radio buttons for v1, v2c, and v3 (selected).
- Security Level:** Radio buttons for NoAuthNoPriv, AuthNoPriv, and AuthPriv (selected).
- Type:** Radio buttons for Trap and Inform (selected).
- Retry Times:** Text input field with a range hint '(1-255)'. The field is currently empty.
- Timeout:** Text input field with a range hint '(1-3600)'. The field is currently empty.

At the bottom right of the form are two buttons: 'Cancel' and 'Create'.

Wykonaj poniższe kroki, aby dodać hosta NMS:

- 1) Wybierz tryb IP zgodny z otoczeniem sieciowym i podaj adres IP hosta NMS oraz port UDP, który odbiera powiadomienia.

|            |                                                                                                                                                                                                                                             |
|------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| IP Mode    | Wybierz tryb IP dla hosta NMS.                                                                                                                                                                                                              |
| IP Address | Jeżeli wybranym <b>IP Mode</b> jest IPv4, podaj adres IPv4 dla hosta NMS.<br><br>Jeżeli wybranym <b>IP Mode</b> jest IPv6, podaj adres IPv6 dla hosta NMS.                                                                                  |
| UDP Port   | Wybierz port UDP na hoście NMS do odbierania powiadomień. Portem domyślnym jest 162. W celu zapewnienia bezpieczeństwa komunikacji zalecamy zmianę numeru portu pod warunkiem, że komunikacja na innych portach UDP nie zostanie zakłócona. |

- 2) Podaj nazwę użytkownika lub nazwę społeczności, z której korzysta host NMS i skonfiguruj tryb i poziom zabezpieczeń, w zależności od ustawień użytkownika lub społeczności.

|                |                                                                                                                                                                                                                                                                                                 |
|----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| User Name      | Podaj nazwę użytkownika lub społeczności, z której korzysta host NMS.                                                                                                                                                                                                                           |
| Security Mode  | Jeżeli w polu User Name podałeś nazwę społeczności (stworzoną dla SNMPv1/v2c), trybem zabezpieczeń musi być v1 lub v2c. Jeżeli w polu User Name podałeś nazwę użytkownika (stworzoną dla SNMPv3), trybem zabezpieczeń będzie v3.<br><br>Host NMS powinien korzystać z odpowiedniej wersji SNMP. |
| Security Level | Jeżeli Security Level to v3, pole pokazuje poziom zabezpieczeń użytkownika.                                                                                                                                                                                                                     |

- 3) Wybierz typ powiadomień w oparciu o wersję SNMP. Jeżeli wybierzesz typ Inform, musisz także ustawić limit wysyłanych komunikatów oraz limit czasu oczekiwania.

|         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|---------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Type    | Wybierz typ powiadomień dla hosta NMS. Obsługiwanym typem dla SNMPv1, jest trap. Dla SNMPv2c i SNMPv3 dostępne są typy trap oraz inform.<br><br>Trap: Przełącznik wysyła komunikaty Trap do hosta NMS po wystąpieniu określonych zdarzeń. Gdy host NMS otrzymuje komunikat Trap, nie wysyła odpowiedzi do przełącznika. Zatem przełącznik nie może stwierdzić, czy komunikat został odebrany, czy nie i komunikaty, które nie zostały odebrane, nie zostaną wysłane ponownie.<br><br>Inform: Przełącznik wysyła komunikaty Inform do hosta NMS po wystąpieniu określonych zdarzeń. Gdy host NMS otrzymuje komunikat Inform, wysyła odpowiedź do przełącznika. Jeśli przełącznik nie otrzyma odpowiedzi w ustalonym limicie czasu oczekiwania, ponownie wysyła komunikat Inform. Zatem komunikaty Inform są bardziej przewidywalne niż komunikaty Trap. |
| Retry   | Ustaw limit wysyłanych komunikatów Inform. Jeżeli przełącznik nie otrzyma odpowiedzi od hosta NMS w ustalonym limicie czasu oczekiwania, ponownie wyśle komunikat Inform. Przełącznik zaprzestanie wysyłania komunikatów Inform po osiągnięciu ustalonego limitu.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Timeout | Ustaw czas oczekiwania przełącznika na odpowiedź od hosta NMS po przesłaniu komunikatu Inform.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |

- 4) Kliknij **Create**.

### 3.1.2 Włączanie SNMP Traps

Wybierz menu **MAINTENANCE > SNMP > Notification > Trap Config**, aby wyświetlić poniższą stronę.

Rys. 3-2 Włączanie komunikatów SNMP Trap

SNMP Traps

|                                                         |                                               |                                               |
|---------------------------------------------------------|-----------------------------------------------|-----------------------------------------------|
| <input checked="" type="checkbox"/> SNMP Authentication | <input checked="" type="checkbox"/> Coldstart | <input checked="" type="checkbox"/> Warmstart |
| <input checked="" type="checkbox"/> Link Status         | <input type="checkbox"/> CPU Utilization      | <input type="checkbox"/> Memory Utilization   |
| <input type="checkbox"/> Flash Operation                | <input type="checkbox"/> VLAN Create/Delete   | <input type="checkbox"/> IP Change            |
| <input type="checkbox"/> Storm Control                  | <input type="checkbox"/> Rate Limit           | <input type="checkbox"/> LLDP                 |
| <input type="checkbox"/> Loopback Detection             | <input type="checkbox"/> Spanning Tree        | <input type="checkbox"/> IP-MAC Binding       |
| <input type="checkbox"/> IP Duplicate                   | <input type="checkbox"/> DHCP Filter          | <input type="checkbox"/> ACL Counter          |

Apply

Na stronie znajduje się lista obsługiwanych komunikatów Trap. Wykonaj poniższe kroki, aby włączyć lub wyłączyć wybrane komunikaty Trap:

1) Wybierz komunikaty Trap, które chcesz włączyć, w zależności od swoich wymagań.

|                            |                                                                                                                                                                                                                                     |
|----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>SNMP Authentication</b> | Ma zastosowanie, gdy uwierzytelnianie otrzymanego żądania SNMP kończy się niepowodzeniem.                                                                                                                                           |
| <b>Coldstart</b>           | Wskazuje na inicjalizację SNMP spowodowaną ponowną inicjalizacją systemu przełącznika. Komunikat trap jest wysyłany po restarcie przełącznika.                                                                                      |
| <b>Warmstart</b>           | Wskazuje, że funkcja SNMP jest ponownie inicjalizowana na przełączniku z niezmienioną konfiguracją fizyczną. Komunikat trap jest wysyłany, gdy SNMP zostanie wyłączony i ponownie włączony po pełnej konfiguracji i włączeniu SNMP. |
| <b>Link Status</b>         | Ma zastosowanie, gdy przełącznik wykrywa zmianę stanu łącza.                                                                                                                                                                        |
| <b>CPU Utilization</b>     | Ma zastosowanie, gdy wykorzystanie procesora przekracza ustawiony limit. Domyślnym limitem dla przełącznika jest 80%.                                                                                                               |
| <b>Memory Utilization</b>  | Ma zastosowanie, gdy wykorzystanie pamięci przekracza 80%.                                                                                                                                                                          |
| <b>Flash Operation</b>     | Ma zastosowanie, gdy pamięć flash ulega zmianie poprzez takie działania, jak tworzenie kopii zapasowej, reset, aktualizacja firmware'u, import konfiguracji. .                                                                      |
| <b>VLAN Create/Delete</b>  | Ma zastosowanie, gdy określone VLAN-y zostaną pomyślnie utworzone lub usunięte.                                                                                                                                                     |
| <b>IP Change</b>           | Monitoruje zmiany adresu IP wszystkich interfejsów. Komunikat trap jest wysyłany, gdy adres IP interfejsu ulegnie zmianie.                                                                                                          |
| <b>Storm Control</b>       | Monitoruje, czy wskaźnik storm osiągnął ustawiony limit. Komunikat trap jest wysyłany, gdy funkcja jest włączona, a ramki broadcast/multicast/unknown-unicast są wysłane na port niezgodnie z ustawionym limitem.                   |

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Rate Limit         | Monitoruje przekroczenie limitu ustawionej przepustowości. Komunikat trap jest wysyłany, gdy opcja Rate Limit jest włączona, a pakiety są wysyłane na port niezgodnie z ustawionym limitem.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| LLDP               | Wskazuje na zmiany w topologii LLDP. Komunikat trap jest wysyłany, gdy nowe urządzenie zdalne, podłączone do portu lokalnego lub urządzenia zdalnego, traci połączenie lub zostaje podłączone do innego portu.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Loopback Detection | Ma zastosowanie, gdy przełącznik wykryje połączenie loopback lub, gdy połączenie loopback zostanie usunięte.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Spanning Tree      | Wskazuje na zmiany spanning tree. Komunikat trap jest wysyłany, gdy stan portu ulega zmianie z non-forwarding do forwarding lub na odwrót. Port odbiera pakiet z flagą TC lub pakiet TCN.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| PoE                | <p>Tylko dla urządzeń z obsługą funkcji PoE. Wszystkie komunikaty trap odnoszą się do PoE, tj.:</p> <p><b>Over-max-pwr-budget:</b> Ma zastosowanie, gdy całkowita moc wymagana przez podłączone urządzenia PD przekracza maksymalną moc, jaką może dostarczyć przełącznik PoE.</p> <p><b>Port-pwr-change:</b> Ma zastosowanie, gdy port zaczyna dostarczać energię lub wyłącza zasilanie urządzeń.</p> <p><b>Port-pwr-deny:</b> Ma zastosowanie, gdy przełącznik wyłącza zasilanie urządzeń PD na portach o niskim priorytecie. Gdy całkowita moc wymagana przez podłączone urządzenia PD przekroczy limit mocy systemowej, przełącznik wyłącza urządzenia PD na portach o niskim priorytecie, aby zapewnić stabilne działanie innych urządzeń PD.</p> <p><b>Port-pwr-over-30w:</b> Ma zastosowanie, gdy moc wymagana przez podłączone urządzenia PD przekracza 30W.</p> <p><b>Port-pwr-overload:</b> Ma zastosowanie, gdy moc wymagana przez podłączone urządzenia PD przekracza maksymalną moc, jaką może dostarczyć port.</p> <p><b>Port-short-circuit:</b> Ma zastosowanie, gdy na porcie zostanie wykryte zwarcie.</p> <p><b>Thermal-shutdown:</b> Ma zastosowanie, gdy układ PSE przegrzeje się. Przełącznik automatycznie wyłącza w tej sytuacji zasilanie.</p> |
| IP-MAC Binding     | Ma zastosowanie w następujących sytuacjach: funkcja inspekcji ARP jest włączona i przełącznik odbiera nielegalny pakiet ARP; funkcja IPv4 Source Guard jest włączona i przełącznik odbiera nielegalny pakiet IP.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| IP Duplicate       | Ma zastosowanie, gdy przełącznik wykrywa konflikt adresów IP.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| DHCP Filter        | Ma zastosowanie, gdy funkcja filtrowania DHCPv4 jest włączona i przełącznik odbiera pakiety DHCP z nielegalnego serwera DHCP.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| ACL Counter        | Monitoruje informacje o dopasowaniach ACL, w tym o ID dopasowań ACL, ID reguł oraz liczbie dopasowań pakietów. Włączenie tej opcji oraz funkcji <b>Logging</b> w ustawieniach reguł ACL sprawi, że przełącznik będzie sprawdzać informacje o dopasowaniach ACL co 5 minut i przysyłać komunikaty trap SNMP w przypadku zmian.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |



2) Kliknij **Apply**.

## 3.2 Przez CLI

### 3.2.1 Konfiguracja hostów NMS

Skonfiguruj parametry hostów NMS i mechanizm obsługi pakietów.

|        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Krok 1 | <p><b>configure</b></p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|        | <p>Uruchom tryb konfiguracji globalnej.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Krok 2 | <p><b>snmp-server host</b> <i>ip udp-port user-name</i> [<b>smode</b> { v1   v2c   v3 }] [<b>slev</b> {noAuthNoPriv   authNoPriv   authPriv }] [<b>type</b> { trap   inform}] [<b>retries</b> <i>retries</i>] [<b>timeout</b> <i>timeout</i>]</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|        | <p>Skonfiguruj parametry hosta NMS i mechanizm obsługi pakietów.</p> <p><i>ip</i>: Podaj adres IP hosta NMS w adresacji IPv4 lub IPv6. Upewnij się, że możliwa jest komunikacja dla podanych adresów IP hosta NMS i przełącznika.</p> <p><i>udp-port</i>: Wybierz port UDP na hoście NMS do odbierania powiadomień. Portem domyślnym jest 162. W celu zapewnienia bezpieczeństwa komunikacji zalecamy zmianę numeru portu pod warunkiem, że komunikacja na innych portach UDP nie zostanie zakłócona.</p> <p><i>user-name</i>: Podaj nazwę hosta NMS. Gdy host NMS korzysta z SNMPv1 lub SNMPv2c wprowadź Community Name; gdy host NMS korzysta z SNMPv3, wprowadź User Name grupy SNMP.</p> <p><b>v1   v2c   v3</b>: Wybierz tryb zabezpieczeń, z których korzysta użytkownik, spośród następujących opcji: SNMPv1, SNMPv2c, SNMPv3. Host NMS powinien korzystać z takiej samej wersji SNMP.</p> <p><b>noAuthNoPriv   authNoPriv   authPriv</b>: Wybierz poziom zabezpieczeń spośród noAuthNoPriv (brak uwierzytelniania i szyfrowania), authNoPriv (uwierzytelnianie i brak szyfrowania), authPriv (uwierzytelnianie i szyfrowanie). Ustawieniem domyślnym jest noAuthNoPriv. Jeżeli wybranym modelem zabezpieczeń jest wersja 1 lub wersja 2, poziom zabezpieczeń nie może być skonfigurowany.</p> <p><b>trap   inform</b>: Wybierz typ powiadomień dla hosta NMS. Obsługiwanym typem dla SNMPv1, jest trap. Dla SNMPv2c i SNMPv3 dostępne są typy trap oraz inform.</p> <p>Gdy host NMS otrzymuje komunikat Trap, nie wysyła odpowiedzi do przełącznika. Zatem przełącznik nie może stwierdzić, czy komunikat został odebrany, czy nie i komunikaty, które nie zostały odebrane, nie zostaną wysłane ponownie. Gdy host NMS otrzymuje komunikat Inform, wysyła odpowiedź do przełącznika. Jeżeli przełącznik nie otrzyma odpowiedzi w ustalonym limicie czasu oczekiwania, ponownie wysyła komunikat Inform. Zatem komunikaty Inform są bardziej przewidywalne niż komunikaty Trap.</p> <p><i>retries</i>: Ustaw limit wysyłanych komunikatów Inform, wybierając wartość z przedziału 1 - 255 (domyślnie 3). Jeżeli przełącznik nie otrzyma odpowiedzi od hosta NMS w ustalonym limicie czasu oczekiwania, ponownie wyśle komunikat Inform. Przełącznik zaprzestanie wysyłania komunikatów Inform po osiągnięciu ustalonego limitu.</p> <p><i>timeout</i>: Ustaw czas oczekiwania przełącznika na odpowiedź od hosta NMS po przesłaniu komunikatu Inform, wybierając wartość z przedziału 1 - 3600 sekund (domyślnie 100 sekund).</p> |

---

|        |                                                                                         |
|--------|-----------------------------------------------------------------------------------------|
| Krok 3 | <b>show snmp-server host</b><br>Przejrzyj informacje o hoście.                          |
| Krok 4 | <b>end</b><br>Powróć do trybu privileged EXEC.                                          |
| Krok 5 | <b>copy running-config startup-config</b><br>Zapisz ustawienia w pliku konfiguracyjnym. |

---

Poniższy schemat przedstawia przykładowy sposób ustawiania 192.30.1.222 jako adresu IP hosta NMS, portu 162 jako portu UDP, admin jako nazwy używanej przez hosta NMS, SNMPv3 jako trybu zabezpieczeń, authPriv jako poziomu zabezpieczeń, Inform jako typu powiadomień, 3 jako limitu wysyłanych komunikatów oraz 100 sekund jako czasu oczekiwania na odpowiedź:

### Switch#configure

```
Switch(config)#snmp-server host 192.30.1.222 162 admin smode v3 slev authPriv type
inform retries 3 timeout 100
```

### Switch(config)#show snmp-server host

| No. | Des-IP       | UDP  | Name  | SecMode | SecLev   | Type   | Retry | Timeout |
|-----|--------------|------|-------|---------|----------|--------|-------|---------|
| --- | -----        | ---- | ----  | -----   | -----    | ----   | ----- | -----   |
| 1   | 192.30.1.222 | 162  | admin | v3      | authPriv | inform | 3     | 100     |

### Switch(config)#end

### Switch#copy running-config startup-config

## 3.2.2 Włączanie SNMP Traps

Przełącznik obsługuje wiele komunikatów trap SNMP, w tym standardowe trap SNMP, trap ACL i trap VLAN. Wybierz komunikaty Trap, które chcesz włączyć, w zależności od swoich wymagań.

- Globalne włączanie standardowych komunikatów trap SNMP

---

|        |                                                          |
|--------|----------------------------------------------------------|
| Krok 1 | <b>configure</b><br>Uruchom tryb konfiguracji globalnej. |
|--------|----------------------------------------------------------|

---

---

|        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Krok 2 | <b>snmp-server traps snmp [ linkup   linkdown   warmstart   coldstart   auth-failure ]</b><br><p>Włącz wybrane komunikaty trap SNMP. Bez podania parametrów polecenie włącza wszystkie standardowe komunikaty trap SNMP. Domyślnie włączone są wszystkie standardowe komunikaty trap SNMP.</p> <p><b>linkup:</b> Wskazuje na zmianę stanu portu z linkdown do linkup i ma zastosowanie po podłączeniu urządzenia do portu.</p> <p><b>linkdown:</b> Wskazuje na zmianę stanu portu z linkup do linkdown i ma zastosowanie po odłączeniu urządzenia od portu.</p> <p><b>warmstart:</b> Wskazuje, że funkcja SNMP jest ponownie inicjalizowana na przełączniku z niezmienną konfiguracją fizyczną. Komunikat trap jest wysyłany, gdy SNMP zostanie wyłączony i ponownie włączony po pełnej konfiguracji i włączeniu SNMP.</p> <p><b>coldstart:</b> Wskazuje na inicjalizację SNMP spowodowaną ponowną inicjalizacją systemu przełącznika. Komunikat trap jest wysyłany po restarcie przełącznika.</p> <p><b>auth-failure:</b> Ma zastosowanie, gdy uwierzytelnianie otrzymanego żądania SNMP kończy się niepowodzeniem.</p> |
| Krok 3 | <b>end</b><br><p>Powróć do trybu privileged EXEC.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Krok 4 | <b>copy running-config startup-config</b><br><p>Zapisz ustawienia w pliku konfiguracyjnym.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

---

Poniższy schemat przedstawia przykładowy sposób konfiguracji na przełączniku przesyłania komunikatów trap linkup:

**Switch#configure**

**Switch(config)#snmp-server traps snmp linkup**

**Switch(config)#end**

**Switch#copy running-config startup-config**

- **Globalne włączanie rozszerzonych komunikatów trap SNMP**

---

|        |                                                                 |
|--------|-----------------------------------------------------------------|
| Krok 1 | <b>configure</b><br><p>Uruchom tryb konfiguracji globalnej.</p> |
|--------|-----------------------------------------------------------------|

---

|        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Krok 2 | <p><b>snmp-server traps</b> { rate-limit   cpu   flash   lldp remtableschange   lldp topologychange   loopback-detection   storm-control   spanning-tree   memory }</p> <p>Włącz wybrane komunikaty trap SNMP. Domyślnie włączone są wszystkie rozszerzone komunikaty trap SNMP.</p> <p><b>rate-limit:</b> Monitoruje przekroczenie limitu ustawionej przepustowości. Komunikat trap jest wysyłany, gdy opcja Rate Limit jest włączona, a pakiety są wysyłane na port niezgodnie z ustawionym limitem.</p> <p><b>cpu:</b> Monitoruje stan obciążenia procesora przełącznika. Ma zastosowanie, gdy wykorzystanie procesora przekracza ustawiony limit. Domyślnym limitem dla przełącznika jest 80%.</p> <p><b>flash:</b> Ma zastosowanie, gdy pamięć flash ulega zmianie poprzez takie działania, jak tworzenie kopii zapasowej, reset, aktualizacja firmware'u, import konfiguracji.</p> <p><b>lldp remtableschange:</b> Powiadomienie lldp RemTablesChange jest wysyłane, gdy wartość lldp StatsRemTableLastChangeTime ulega zmianie. Może być stosowany przez hosta NMS do wysyłania table maintenance polls systemów zdalnych LLDP.</p> <p><b>lldp topologychange:</b> Wskazuje na zmiany w topologii LLDP. Komunikat trap jest wysyłany, gdy nowe urządzenie zdalne, podłączone do portu lokalnego lub urządzenia zdalnego, traci połączenie lub zostaje podłączone do innego portu.</p> <p><b>loopback-detection:</b> Ma zastosowanie, gdy przełącznik wykryje połączenie loopback lub, gdy połączenie loopback zostanie usunięte.</p> <p><b>storm-control:</b> Funkcja monitoruje sieciowe burze rozgłoszeniowe. System wygeneruje komunikat trap, gdy liczba pakietów broadcast lub multicast osiągnie ustawiony limit.</p> <p><b>spanning-tree:</b> Wskazuje na zmiany spanning tree. Komunikat trap jest wysyłany, gdy stan portu ulega zmianie z non-forwarding do forwarding lub na odwrót. Port odbiera pakiet z flagą TC lub pakiet TCN.</p> <p><b>memory:</b> Monitoruje zużycie pamięci. Ma zastosowanie, gdy wykorzystanie pamięci przekracza 80%.</p> |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

|        |                                                           |
|--------|-----------------------------------------------------------|
| Krok 3 | <p><b>end</b></p> <p>Powróć do trybu privileged EXEC.</p> |
|--------|-----------------------------------------------------------|

|        |                                                                                                    |
|--------|----------------------------------------------------------------------------------------------------|
| Krok 4 | <p><b>copy running-config startup-config</b></p> <p>Zapisz ustawienia w pliku konfiguracyjnym.</p> |
|--------|----------------------------------------------------------------------------------------------------|

Poniższy schemat przedstawia przykładowy sposób włączania na przełączniku komunikatów trap bandwidth-control:

```
Switch#configure
```

```
Switch(config)#snmp-server traps bandwidth-control
```

```
Switch(config)#end
```

```
Switch#copy running-config startup-config
```

## ■ Globalne włączanie komunikatów trap VLAN

|        |                                                                                                                                                                                                                                                                                                                                                                            |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Krok 1 | <b>configure</b><br>Uruchom tryb konfiguracji globalnej.                                                                                                                                                                                                                                                                                                                   |
| Krok 2 | <b>snmp-server traps vlan [ create   delete ]</b><br>Włącz wybrane komunikaty trap VLAN. Bez podania parametrów polecenie włącza wszystkie komunikaty trap VLAN. Domyślnie komunikaty trap VLAN są wyłączone.<br><b>create:</b> Ma zastosowanie po pomyślnym utworzeniu określonych VLAN-ów.<br><b>delete:</b> Ma zastosowanie po pomyślnym usunięciu określonych VLAN-ów. |
| Krok 3 | <b>end</b><br>Powróć do trybu privileged EXEC.                                                                                                                                                                                                                                                                                                                             |
| Krok 4 | <b>copy running-config startup-config</b><br>Zapisz ustawienia w pliku konfiguracyjnym.                                                                                                                                                                                                                                                                                    |

Poniższy schemat przedstawia przykładowy sposób włączania wszystkich komunikatów trap VLAN SNMP na przełączniku:

**Switch#configure**

**Switch(config)#snmp-server traps vlan**

**Switch(config)#end**

**Switch#copy running-config startup-config**

## ■ Globalne włączanie komunikatów trap ochrony SNMP

|        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Krok 1 | <b>configure</b><br>Uruchom tryb konfiguracji globalnej.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Krok 2 | <b>snmp-server traps security { dhcp-filter   ip-mac-binding }</b><br>Włącz wybrane komunikaty trap ochrony. Domyślnie wszystkie komunikaty trap są wyłączone.<br><b>dhcp-filter:</b> Ma zastosowanie, gdy funkcja filtrowania DHCPv4 jest włączona i przełącznik odbiera pakiety DHCP z nielegalnego serwera DHCP.<br><b>ip-mac-binding:</b> Ma zastosowanie, gdy funkcja inspekcji ARP jest włączona i przełącznik odbiera nielegalny pakiet ARP lub funkcja IPv4 Source Guard jest włączona i przełącznik odbiera nielegalny pakiet IP. |
| Krok 3 | <b>end</b><br>Powróć do trybu privileged EXEC.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Krok 4 | <b>copy running-config startup-config</b><br>Zapisz ustawienia w pliku konfiguracyjnym.                                                                                                                                                                                                                                                                                                                                                                                                                                                    |

Poniższy schemat przedstawia przykładowy sposób włączania komunikatów trap dla filtrowania DHCP na przełączniku:

```
Switch#configure
```

```
Switch(config)#snmp-server traps security dhcp-filter
```

```
Switch(config)#end
```

```
Switch#copy running-config startup-config
```

#### ■ Globalne włączanie komunikatów trap ACL

|        |                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Krok 1 | <b>configure</b><br>Uruchom tryb konfiguracji globalnej.                                                                                                                                                                                                                                                                                                                                                                                  |
| Krok 2 | <b>snmp-server traps security acl</b><br>Włącz komunikaty trap ACL. Domyślnie opcja jest wyłączona.<br>Trap monitoruje informacje o dopasowaniach ACL, w tym o ID dopasowań ACL, ID reguł oraz liczbie dopasowań pakietów. Włączenie tej opcji oraz funkcji <b>Logging</b> w ustawieniach reguł ACL sprawi, że przełącznik będzie sprawdzać informacje o dopasowaniach ACL co 5 minut i przysyłać komunikaty trap SNMP w przypadku zmian. |
| Krok 3 | <b>end</b><br>Powróć do trybu privileged EXEC.                                                                                                                                                                                                                                                                                                                                                                                            |
| Krok 4 | <b>copy running-config startup-config</b><br>Zapisz ustawienia w pliku konfiguracyjnym.                                                                                                                                                                                                                                                                                                                                                   |

Poniższy schemat przedstawia przykładowy sposób włączania komunikatów trap ACL:

```
Switch#configure
```

```
Switch(config)#snmp-server traps acl
```

```
Switch(config)#end
```

```
Switch#copy running-config startup-config
```

#### ■ Globalne włączanie komunikatów trap IP

|        |                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Krok 1 | <b>configure</b><br>Uruchom tryb konfiguracji globalnej.                                                                                                                                                                                                                                                                                                                                                                                            |
| Krok 2 | <b>snmp-server traps ip { change   duplicate }</b><br>Włącz komunikaty trap IP. Domyślnie wszystkie komunikaty trap IP są wyłączone.<br><b>change:</b> Włącz komunikaty zmian IP SNMP. Trap monitoruje zmiany adresu IP wszystkich interfejsów. Komunikat trap jest wysyłany, gdy adres IP interfejsu ulegnie zmianie.<br><b>duplicate:</b> Włącz komunikaty duplikatów IP SNMP. Trap ma zastosowanie, gdy przełącznik wykrywa konflikt adresów IP. |

---

Krok 3      **end**  
Powróć do trybu privileged EXEC..

---

Krok 4      **copy running-config startup-config**  
Zapisz ustawienia w pliku konfiguracyjnym.

---

Poniższy schemat przedstawia przykładowy sposób włączania na przełączniku komunikatów trap dla zmian adresów IP:

**Switch#configure**

**Switch(config)#snmp-server traps ip change**

**Switch(config)#end**

**Switch#copy running-config startup-config**

- Włączanie komunikatów trap o stanie łącza dla portów

---

Krok 1      **configure**  
Uruchom tryb konfiguracji globalnej.

---

Krok 2      **interface {fastEthernet *port* | range fastEthernet *port-list* | gigabitEthernet *port* | range gigabitEthernet *port-list* | ten-gigabitEthernet *port* | range ten-gigabitEthernet *port-list* }**  
Skonfiguruj powiadomienia trap na określonych portach.  
*port/port-list*: Numer lub lista portów Ethernet dla powiadomień trap.

---

Krok 3      **snmp-server traps link-status**  
Włącz komunikaty trap o stanie łącza. Mają zastosowanie, gdy przełącznik wykrywa zmianę stanu łącza. Domyślnie opcja jest wyłączona.

---

Krok 4      **end**  
Powróć do trybu privileged EXEC..

---

Krok 5      **copy running-config startup-config**  
Zapisz ustawienia w pliku konfiguracyjnym.

---

Poniższy schemat przedstawia przykładowy sposób włączania na przełączniku komunikatów trap o zmianie stanu łącza:

**Switch#configure**

**Switch(config)#interface gigabitEthernet 1/0/1**

**Switch(config-if)#snmp-server traps link-status**

**Switch(config-if)#end**

**Switch#copy running-config startup-config**

# 4 RMON

- RMON (Remote Network Monitoring) to standard uzupełniający SNMP. Służy do badania ilości przesyłanych danych. RMON ogranicza ruch pomiędzy NMS a urządzeniami zarządzalnymi, co jest wygodnym rozwiązaniem w przypadku dużych środowisk sieciowych.
- RMON uwzględnia dwa aspekty: NMS oraz agentów działających na każdym urządzeniu sieciowym. NMS to zwykle host obsługujący oprogramowanie zarządzające agentami urządzeń sieciowych. Agentem jest zwykle przełącznik lub router, który zbiera statystyki ruchu (takie jak całkowita liczba pakietów segmentu sieci w określonym przedziale czasowym lub całkowita liczba prawidłowych pakietów wysyłanych do hosta). W oparciu o protokół SNMP, NMS zbiera dane sieciowe poprzez komunikację z agentami. Jednakże NMS nie może pozyskać wszystkich danych z bazy MIB RMON ze względu na ograniczone zasoby urządzenia. Zasadniczo NMS może uzyskać informacje tylko o czterech następujących grupach: Statistics (Statystyki), History (Historia), Event (Zdarzenie) i Alarm.
- **Statistics:** Zbiera statystyki portu Ethernet (takie jak całkowita wartość odebranych bajtów, całkowita liczba pakietów broadcast oraz całkowita liczba pakietów o określonym rozmiarze) w ramach interfejsu.
- **History:** Zapisuje Historię statystyk portów Ethernet w określonych interwałach sondowania.
- **Event:** Określa działanie, które zostanie podjęte, gdy Alarm wywoła Zdarzenie. Działanie może polegać na wygenerowaniu pozycji dziennika lub komunikatu trap SNMP.
- **Alarm:** Monitoruje określony obiekt bazy MIB przez ustalony czas, wyzwala zdarzenie o określonej wartości (próg wzrostu lub próg spadku)..



# 5 Konfiguracja RMON

Konfiguracja RMON umożliwia:

- konfigurację Statystyk;
- konfigurację Historii;
- konfigurację Zdarzeń;
- konfigurację Alarmu.

## Wskazówki dotyczące konfiguracji

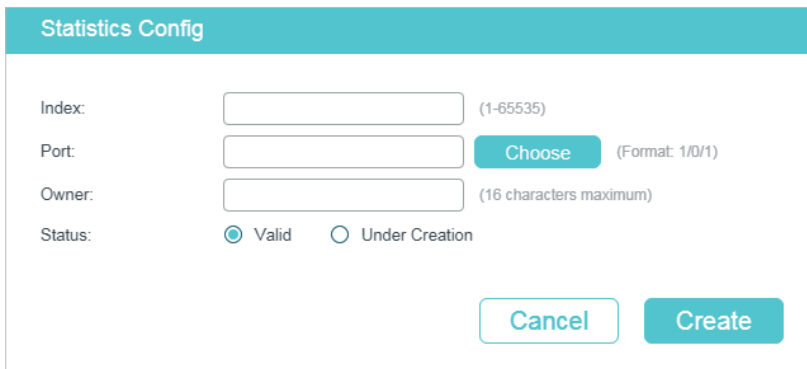
Aby mieć pewność, że NMS poprawnie odbiera powiadomienia, skonfiguruj najpierw SNMP i powiadomienia SNMP.

## 5.1 Przez GUI

### 5.1.1 Konfiguracja Statystyk

Wybierz z menu **MAINTENANCE > SNMP > RMON > Statistics** i kliknij  **Add**, aby wyświetlić poniższą stronę.

Rys. 5-1 Dodawanie pozycji do Statystyk



Wykonaj poniższe kroki, aby skonfigurować Statystyki:

- 1) Podaj numer identyfikacyjny pozycji, monitorowany port i nazwę właściciela wpisu. Ustaw dla pozycji stan Valid lub Under Creation.

|       |                                                                                                                     |
|-------|---------------------------------------------------------------------------------------------------------------------|
| Index | Podaj numer identyfikacyjny pozycji.                                                                                |
| Port  | Kliknij <b>Choose</b> , aby wybrać port Ethernet, który ma być monitorowany lub podaj numer portu w formacie 1/0/1. |
| Owner | Podaj nazwę właściciela pozycji, używając od 1 do 16 znaków.                                                        |

**Status** Ustaw stan wpisu, wybierając spośród opcji Valid i Under Creation. Domyślnym ustawieniem jest Valid, które powoduje, że przełącznik automatycznie zaczyna zbierać statystyki z portu Ethernet dla tej pozycji.

**Valid:** Pozycja została utworzona i jest aktywna.

**Under Creation:** Pozycja została utworzona, ale nie jest aktywna.

2) Kliknij **Create**.

## 5.1.2 Konfiguracja Historii

Wybierz z menu **MAINTENANCE > SNMP > RMON > History**, aby wyświetlić poniższą stronę.

Rys. 5-2 Konfiguracja wpisu historii

| History Control Config              |       |       |                    |                 |         |          |
|-------------------------------------|-------|-------|--------------------|-----------------|---------|----------|
| <input type="checkbox"/>            | Index | Port  | Interval (seconds) | Maximum Buckets | Owner   | Status   |
| <input checked="" type="checkbox"/> | 1     | 1/0/1 | 1800               | 50              | monitor | Disabled |
| <input type="checkbox"/>            | 2     | 1/0/1 | 1800               | 50              | monitor | Disabled |
| <input type="checkbox"/>            | 3     | 1/0/1 | 1800               | 50              | monitor | Disabled |
| <input type="checkbox"/>            | 4     | 1/0/1 | 1800               | 50              | monitor | Disabled |
| <input type="checkbox"/>            | 5     | 1/0/1 | 1800               | 50              | monitor | Disabled |
| <input type="checkbox"/>            | 6     | 1/0/1 | 1800               | 50              | monitor | Disabled |
| <input type="checkbox"/>            | 7     | 1/0/1 | 1800               | 50              | monitor | Disabled |
| <input type="checkbox"/>            | 8     | 1/0/1 | 1800               | 50              | monitor | Disabled |
| <input type="checkbox"/>            | 9     | 1/0/1 | 1800               | 50              | monitor | Disabled |
| <input type="checkbox"/>            | 10    | 1/0/1 | 1800               | 50              | monitor | Disabled |

Total: 12      1 entry selected.      Cancel Apply

Wykonaj poniższe kroki, aby skonfigurować grupę Historii:

1) Wybierz pozycję Historii i wybierz monitorowany port.

**Index** Numer identyfikacyjny wpisu Historii. Maksymalnie można dodać 12 pozycji.

**Port** Podaj numer portu, który ma być monitorowany, w formacie 1/0/1.

2) Ustaw częstotliwość próbkowania i maksymalną liczbę wyników dla wpisu Historii.

**Interval (seconds)** Ustal częstotliwość próbkowania. Prawidłowe wartości wahają się od 10 do 3600 sekund, a wartością domyślną jest 1800 sekund. Każdy wpis Historii ma swoje własne ustawienia czasu. W przypadku monitorowanego portu przełącznik pobiera informacje o pakietach i generuje wynik w ramach każdego interwału.

|                 |                                                                                                                                                                                                     |
|-----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Maximum Buckets | Ustaw maksymalną liczbę wpisów Historii. Gdy liczba wpisów przekroczy limit, najwcześniejsza pozycja zostanie nadpisana. Prawidłowe wartości wahają się od 10 do 130, a wartością domyślną jest 50. |
|-----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

3) Podaj nazwę właściciela i ustaw stan wpisu. Kliknij **Apply**.

|       |                                                                                         |
|-------|-----------------------------------------------------------------------------------------|
| Owner | Podaj nazwę właściciela wpisu, używając od 1 do 16 znaków. Domyślną nazwą jest monitor. |
|-------|-----------------------------------------------------------------------------------------|

|        |                                                             |
|--------|-------------------------------------------------------------|
| Status | Włącz lub wyłącz pozycję. Domyślnie pozycja jest wyłączona. |
|--------|-------------------------------------------------------------|

**Enable:** Pozycja jest włączona.

**Disable:** Pozycja jest wyłączona.

#### Uwaga:

Aby zmiana parametrów wpisu Historii była możliwa, pozycja musi być włączona. W przeciwnym razie zmiany nie zostaną wprowadzone.

## 5.1.3 Konfiguracja Zdarzeń

Wybierz z menu **MAINTENANCE > SNMP > RMON > Event**, aby wyświetlić poniższą stronę.

Rys. 5-3 Konfiguracja wpisu Zdarzeń

| <input type="checkbox"/>            | Index | User   | Description | Action Mode | Owner   | Status   |
|-------------------------------------|-------|--------|-------------|-------------|---------|----------|
| <input checked="" type="checkbox"/> | 1     | public |             | None        | monitor | Disabled |
| <input type="checkbox"/>            | 2     | public |             | None        | monitor | Disabled |
| <input type="checkbox"/>            | 3     | public |             | None        | monitor | Disabled |
| <input type="checkbox"/>            | 4     | public |             | None        | monitor | Disabled |
| <input type="checkbox"/>            | 5     | public |             | None        | monitor | Disabled |
| <input type="checkbox"/>            | 6     | public |             | None        | monitor | Disabled |
| <input type="checkbox"/>            | 7     | public |             | None        | monitor | Disabled |
| <input type="checkbox"/>            | 8     | public |             | None        | monitor | Disabled |
| <input type="checkbox"/>            | 9     | public |             | None        | monitor | Disabled |
| <input type="checkbox"/>            | 10    | public |             | None        | monitor | Disabled |

Total: 12      1 entry selected.     

Wykonaj poniższe kroki, aby skonfigurować grupę Zdarzeń:

1) Wybierz wpis Zdarzeń i ustaw dla pozycji użytkownika SNMP.

|       |                                                                            |
|-------|----------------------------------------------------------------------------|
| Index | Numer identyfikacyjny wpisu Zdarzenia. Maksymalnie można dodać 12 pozycji. |
|-------|----------------------------------------------------------------------------|

|      |                                                                                                                                  |
|------|----------------------------------------------------------------------------------------------------------------------------------|
| User | Wybierz nazwę użytkownika lub nazwę społeczności SNMP dla pozycji. Nazwa powinna się zgadzać z wcześniejszymi ustawieniami SNMP. |
|------|----------------------------------------------------------------------------------------------------------------------------------|

2) Uzupełnij opis zdarzenia i działanie, które należy podjąć po wywołaniu zdarzenia.

|             |                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Description | Wprowadź krótki opis tego zdarzenia, aby ułatwić jego identyfikację.                                                                                                                                                                                                                                                                                                                                                                                     |
| Action Mode | Określ działanie, które podejmie przełącznik po wywołaniu zdarzenia.<br><br><b>None:</b> Brak działania. Opcja jest domyślnie włączona.<br><br><b>Log:</b> Przełącznik rejestruje zdarzenie w dzienniku, a NMS, aby otrzymywać powiadomienia, powinien inicjować żądania.<br><br><b>Notify:</b> Przełącznik przesyła powiadomienia do NMS.<br><br><b>Log &amp; Notify:</b> Przełącznik rejestruje zdarzenie w dzienniku i przesyła powiadomienia do NMS. |

3) Uzupełnij nazwę właściciela i ustaw stan wpisu. Kliknij **Apply**.

|        |                                                                                                                                                         |
|--------|---------------------------------------------------------------------------------------------------------------------------------------------------------|
| Owner  | Podaj nazwę właściciela wpisu, używając od 1 do 16 znaków. Domyślną nazwą jest monitor.                                                                 |
| Status | Włącz lub wyłącz pozycję. Domyślnie pozycja jest wyłączona.<br><br><b>Enable:</b> Pozycja jest włączona.<br><br><b>Disable:</b> Pozycja jest wyłączona. |

## 5.1.4 Konfiguracja Alarmu

Przed rozpoczęciem konfiguracji dostosuj ustawienia Statystyk i Zdarzeń, ponieważ wpisy Alarmu muszą być zgodne z wcześniej skonfigurowanymi wpisami Statystyk i Zdarzeń.

Wybierz z menu **MAINTENANCE > SNMP > RMON > Alarm**, aby wyświetlić poniższą stronę.

Rys. 5-4 Konfiguracja wpisu Alarmu

| <input type="checkbox"/>            | Index | Variable | Statistics | Sample Type | Rising Threshold | Rising Event | Falling Threshold | Falling Event |
|-------------------------------------|-------|----------|------------|-------------|------------------|--------------|-------------------|---------------|
| <input checked="" type="checkbox"/> | 1     | RecBytes | 0          | Absolute    | 100              | 0            | 100               | 0             |
| <input type="checkbox"/>            | 2     | RecBytes | 0          | Absolute    | 100              | 0            | 100               | 0             |
| <input type="checkbox"/>            | 3     | RecBytes | 0          | Absolute    | 100              | 0            | 100               | 0             |
| <input type="checkbox"/>            | 4     | RecBytes | 0          | Absolute    | 100              | 0            | 100               | 0             |
| <input type="checkbox"/>            | 5     | RecBytes | 0          | Absolute    | 100              | 0            | 100               | 0             |
| <input type="checkbox"/>            | 6     | RecBytes | 0          | Absolute    | 100              | 0            | 100               | 0             |
| <input type="checkbox"/>            | 7     | RecBytes | 0          | Absolute    | 100              | 0            | 100               | 0             |
| <input type="checkbox"/>            | 8     | RecBytes | 0          | Absolute    | 100              | 0            | 100               | 0             |
| <input type="checkbox"/>            | 9     | RecBytes | 0          | Absolute    | 100              | 0            | 100               | 0             |
| <input type="checkbox"/>            | 10    | RecBytes | 0          | Absolute    | 100              | 0            | 100               | 0             |

Total: 12      1 entry selected.     

Wykonaj poniższe kroki, aby skonfigurować grupę Alarmu:

- Wybierz wpisy Alarmu i zmienne, które będą monitorowane, a następnie powiąż wpisy z pozycjami Statystyk.

|                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Index</b>    | Numer identyfikacyjny wpisu Alarmu. Maksymalnie można dodać 12 pozycji.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Variable</b> | <p>Wybierz zmienne, które będą kontrolowane. Przełącznik będzie monitorować wybrane zmienne cyklicznie i reagować w ustalony sposób na uruchomienia alarmu. Domyślnie wybraną zmienną jest RecBytes.</p> <p><b>RecBytes:</b> Łącznie odebrane bajty.</p> <p><b>RecPackets:</b> Łącznie odebrane pakiety.</p> <p><b>BPackets:</b> Całkowita liczba pakietów broadcast.</p> <p><b>MPackets:</b> Całkowita liczba pakietów multicast.</p> <p><b>CRC&amp;Align ERR:</b> Pakiety o wielkości od 64 do 1518 bajtów, zawierające błąd FCS lub błąd wyrównania.</p> <p><b>Undersize:</b> Pakiety mniejsze niż 64 bajty.</p> <p><b>Oversize:</b> Pakiety większe niż 1518 bajtów.</p> <p><b>Jabbers:</b> Pakiety wysyłane po wystąpieniu kolizji portów.</p> <p><b>Collisions:</b> Czasy kolizji w segmencie sieci.</p> <p><b>64, 65-127, 128-255, 256-511, 512-1023, 1024-10240:</b> Łączna liczba pakietów o określonym rozmiarze.</p> |

|            |                                                                                                          |
|------------|----------------------------------------------------------------------------------------------------------|
| Statistics | Powiąz wpis Alarmu z wpisem Statystyk. Przełącznik będzie monitorować określoną zmienną wpisu Statystyk. |
|------------|----------------------------------------------------------------------------------------------------------|

- 2) Wybierz typ próbkowania, próg wzrostu i spadku, odpowiedni tryb działania dla zdarzenia oraz typ alarmu dla wpisu.

|                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|-------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Sample Type       | Wybierz metodę próbkowania dla określonej zmiennej Domyślnym ustawieniem jest absolute.<br><br><b>Absolute:</b> Porównuje wartość próbkowania z ustawionym progiem.<br><br><b>Delta:</b> Przełącznik oblicza różnicę pomiędzy wartościami próbkowania bieżącego i poprzedniego cyklu, a następnie porównuje tą różnicę z ustawionym progiem.                                                                                                                     |
| Rising Threshold  | Ustaw próg wzrostu dla zmiennej. Gdy wartość próbkowania przekroczy ustawiony próg, system uruchomi odpowiednie zdarzenie ( <b>Rising Event</b> ). Poprawne wartości wynoszą od 1 do 2147483647, a wartość domyślna to 100.                                                                                                                                                                                                                                      |
| Rising Event      | Podaj numer identyfikacyjny wpisu Zdarzenia, które będzie uruchamiane, gdy wartość próbkowania przekroczy ustawiony próg. Podany tutaj wpis Zdarzenia musi być włączony.                                                                                                                                                                                                                                                                                         |
| Falling Threshold | Ustaw próg spadku dla zmiennej. Gdy wartość próbkowania będzie niższa niż ustawiony próg, system uruchomi odpowiednie zdarzenie ( <b>Falling Event</b> ). Poprawne wartości wynoszą od 1 do 2147483647, a wartość domyślna to 100.                                                                                                                                                                                                                               |
| Falling Event     | Podaj numer identyfikacyjny wpisu Zdarzenia, które będzie uruchamiane, gdy wartość próbkowania będzie niższa niż ustawiony próg. Podany tutaj wpis Zdarzenia musi być włączony.                                                                                                                                                                                                                                                                                  |
| Alarm Type        | Określ typ alarmu dla wpisu. Domyślnym typem alarmu jest all.<br><br><b>Rising:</b> Alarm uruchamiany jest tylko wtedy, gdy wartość próbkowania przekracza ustawiony próg wzrostu.<br><br><b>Falling:</b> Alarm uruchamiany jest tylko wtedy, gdy wartość próbkowania jest niższa od ustawionego progu spadku.<br><br><b>All:</b> Alarm uruchamiany jest, gdy wartość próbkowania przekracza ustawiony próg wzrostu lub jest niższa od ustawionego progu spadku. |

- 3) Podaj nazwę właściciela i ustaw stan wpisu. Kliknij **Apply**.

|                    |                                                                                                                |
|--------------------|----------------------------------------------------------------------------------------------------------------|
| Interval (seconds) | Ustaw interwał próbkowania. Poprawne wartości wynoszą od 10 do 3600 sekund, a wartość domyślna to 1800 sekund. |
| Owner              | Podaj nazwę właściciela wpisu, używając od 1 do 16 znaków. Domyślną nazwą jest monitor.                        |

---

|        |                                                          |
|--------|----------------------------------------------------------|
| Status | Włącz lub wyłącz wpis. Domyślnie pozycja jest wyłączona. |
|        | <b>Enable:</b> Wpis jest włączony.                       |
|        | <b>Disable:</b> Wpis jest wyłączony.                     |

---

## 5.2 Przez CLI

### 5.2.1 Konfiguracja Statystyk

---

|        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Krok 1 | <b>configure</b><br>Uruchom tryb konfiguracji globalnej.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Krok 2 | <b>rmon statistics index interface interface { fastEthernet port   gigabitEthernet port   ten-gigabitEthernet port } [ owner owner-name ] [ status { underCreation   valid } ]</b><br>Skonfiguruj wpisy Statystyk RMON.<br><br><i>index:</i> Uzpełnij ID wpisu Statystyk wartością z przedziału 1 - 65535 w formacie 1-3 lub 5.<br><br><i>port:</i> Wprowadź numer portu w formacie 1/0/1, aby przypisać go do wpisu.<br><br><i>owner-name:</i> Podaj nazwę właściciela wpisu, używając od 1 do 16 znaków. Domyślną nazwą jest monitor.<br><br><i>underCreation   valid:</i> Ustaw stan wpisu. UnderCreation oznacza, że wpis został utworzony, ale nie jest aktywny, natomiast Valid oznacza, że wpis został utworzony i jest aktywny. Domyślnym ustawieniem jest valid.<br><br>Stan Valid oznacza, że przełącznik automatycznie zaczyna zbierać statystyki z portu Ethernet dla tej pozycji Statystyk. |
| Krok 3 | <b>show rmon statistics [ index ]</b><br>Wyświetla wpisy Statystyk i ich ustawienia.<br><br><i>index:</i> Wpisz numery identyfikacyjne wpisów Statystyk, które chcesz wyświetlić. Poprawne wartości wynoszą od 1 do 65535.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Krok 4 | <b>end</b><br>Powróć do trybu privileged EXEC.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Krok 5 | <b>copy running-config startup-config</b><br>Zapisz ustawienia w pliku konfiguracyjnym.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |

---

Poniższy schemat przedstawia przykładowy sposób tworzenia wpisów Statystyk na przełączniku do monitorowania odpowiednio portu 1/0/1 oraz portu 1/0/2. Właścicielem obu wpisów będzie monitor, a wartością stanu Valid:

**Switch#configure**

```
Switch(config)#rmon statistics 1 interface gigabitEthernet 1/0/1 owner monitor status
valid
```

```
Switch(config)#rmon statistics 2 interface gigabitEthernet 1/0/2 owner monitor status
valid
```

```
Switch(config)#show rmon statistics
```

```
Index Port Owner State

1 Gi1/0/1 monitor valid
2 Gi1/0/2 monitor valid
```

```
Switch(config)#end
```

```
Switch#copy running-config startup-config
```

## 5.2.2 Konfiguracja Historii

|        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Krok 1 | <p><b>configure</b></p> <p>Uruchom tryb konfiguracji globalnej.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Step 2 | <p><b>rmon history</b> <i>index</i> <b>interface</b> { <b>fastEthernet</b> <i>port</i>   <b>gigabitEthernet</b> <i>port</i>   <b>ten-gigabitEthernet</b> <i>port</i> } [<b>interval</b> <i>seconds</i>] [<b>owner</b> <i>owner-name</i>] [<b>buckets</b> <i>number</i>]</p> <p>Konfiguracja wpisów Historii RMON.</p> <p><i>index</i>: Uzupełnij numer identyfikacyjny wpisu Historii wartością z przedziału 1 - 12 w formacie 1-3 lub 5.</p> <p><i>port</i>: Wprowadź numer portu w formacie 1/0/1, aby przypisać go do wpisu.</p> <p><i>seconds</i>: Ustaw częstotliwość próbkowania. Wartości wahają się od 10 do 3600 sekund, a wartością domyślną jest 1800 sekund.</p> <p><i>owner-name</i>: Podaj nazwę właściciela wpisu, używając od 1 do 16 znaków. Domyślną nazwą jest monitor.</p> <p><i>number</i>: Ustaw maksymalną liczbę wpisów Historii. Gdy liczba wpisów przekroczy limit, najwcześniejsza pozycja zostanie nadpisana. Prawidłowe wartości wahają się od 10 do 130, a wartością domyślną jest 50.</p> |
| Krok 3 | <p><b>show rmon history</b> [<i>index</i>]</p> <p>Wyświetla skonfigurowany wpis Historii i jego ustawienia.</p> <p><i>index</i>: Wpisz numery identyfikacyjne wpisów Historii, które chcesz wyświetlić. Poprawne wartości wynoszą od 1 do 12, a stosowanym formatem jest 1-3 lub 5.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Krok 4 | <p><b>end</b></p> <p>Powróć do trybu privileged EXEC.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |



---

Krok 5      **copy running-config startup-config**  
Zapisz ustawienia w pliku konfiguracyjnym.

---

Poniższy schemat przedstawia przykładową sposób tworzenia wpisu Historii na przełączniku do monitorowania portu 1/0/1. Wartością częstotliwości próbkowania będzie 100 sekund, maksymalną liczbą wpisów 50, a właścicielem monitor:

**Switch#configure**

**Switch(config)#rmon history 1 interface gigabitEthernet 1/0/1 interval 100 owner monitor buckets 50**

**Switch(config)#show rmon history**

| Index | Port    | Interval | Buckets | Owner   | State  |
|-------|---------|----------|---------|---------|--------|
| 1     | Gi1/0/1 | 100      | 50      | monitor | Enable |

**Switch(config)#end**

**Switch#copy running-config startup-config**

### 5.2.3 Konfiguracja Zdarzeń

---

Krok 1      **configure**  
Uruchom tryb konfiguracji globalnej.

---

Krok 2      **rmon event index [ user user-name ] [ description description ] [ type { none | log | notify | log-notify } ] [ owner owner-name ]**  
Konfiguracja wpisów Zdarzeń RMON.

*index*: Uzupełnij numer identyfikacyjny wpisu Zdarzeń wartością z przedziału 1 - 12 w formacie 1-3 lub 5.

*user-name*: Wybierz nazwę użytkownika lub nazwę społeczności SNMP dla pozycji. Nazwa powinna się zgadzać z wcześniejszymi ustawieniami SNMP. Domyślna nazwa to public.

*description*: Wprowadź krótki opis dla wpisu, używając od 1 do 16 znaków. Domyślnie opis jest pusty.

*none | log | notify | log-notify*: Określ działanie, które podejmie przełącznik po wywołaniu zdarzenia. Domyślnie ustawionym typem jest none. None oznacza brak działania, log oznacza, że przełącznik rejestruje zdarzenie, notify oznacza, że przełącznik wysyła powiadomienia do NMS, a log-notify oznacza, że przełącznik rejestruje zdarzenie i wysyła powiadomienia do NMS.

*owner-name*: Podaj nazwę właściciela wpisu, używając od 1 do 16 znaków. Domyślną nazwą jest monitor.

---

---

Krok 3      **show rmon event [ index ]**

Wyświetla skonfigurowany wpis Zdarzeń i jego ustawienia.

*index:* Wpisz numery identyfikacyjne wpisów Zdarzeń, które chcesz wyświetlić. Poprawne wartości wynoszą od 1 do 12, a stosowanym formatem jest 1-3 lub 5.

---

Krok 4      **end**

Powróć do trybu privileged EXEC.

---

Krok 5      **copy running-config startup-config**

Zapisz ustawienia w pliku konfiguracyjnym.

---

Poniższy schemat przedstawia przykładowy sposób tworzenia wpisu Zdarzeń na przełączniku. Nazwą użytkownika będzie admin, typem zdarzenia Notify (przełącznik przesyła powiadomienia do NMS), a właścicielem monitor:

**Switch#configure**

**Switch(config)#rmon event 1 user admin description rising-notify type notify owner monitor**

**Switch(config)#show rmon event**

| Index | User  | Description   | Type   | Owner   | State  |
|-------|-------|---------------|--------|---------|--------|
| ----- | ----  | -----         | ----   | -----   | -----  |
| 1     | admin | rising-notify | Notify | monitor | Enable |

**Switch(config)#end**

**Switch#copy running-config startup-config**

## 5.2.4 Konfiguracja Alarmu

---

Krok 1      **configure**

Uruchom tryb konfiguracji globalnej.

---

## Krok 2

**rmon alarm index stats-index *sindex* [ alarm-variable { revbyte | revpkt | bpkt | mpkt | crc-align | undersize | oversize | jabber | collision | 64 | 65-127 | 128-255 | 256-511 | 512-1023 | 1024-10240} ] [ s-type { absolute | delta} ] [ rising-threshold *r-hold* ] [ rising-event-index *r-event* ] [ falling-threshold *f-hold* ] [ falling-event-index *f-event* ] [ a-type { rise | fall | all} ] [ owner *owner-name* ] [ interval *interval* ]**

Skonfiguruj wpisy Alarmu RMON.

*index*: Uzupełnij numer identyfikacyjny wpisu Alarmu wartością z przedziału 1 - 12 w formacie 1-3 lub 5.

*sindex*: Ustaw numery identyfikacyjne powiązanych wpisów Statystyk (od 1 do 65535).

*revbyte | revpkt | bpkt | mpkt | crc-align | undersize | oversize | jabber | collision | 64 | 65- 127 | 128-255 | 256-511 | 512-1023 | 1024-10240*: Wybierz zmienne, które będą kontrolowane. Przełącznik będzie monitorować wybrane zmienne cyklicznie i reagować w ustalony sposób na uruchomienia alarmu. Domyślnie wybraną zmienną jest *revbyte*.

*revbyte* oznacza łącznie odebrane bajty; *revpkt* oznacza łącznie odebrane pakiety; *bpkt* oznacza całkowitą liczbę pakietów broadcast. *mpkt* oznacza całkowitą liczbę pakietów multicast; *crc-align* oznacza pakiety o wielkości od 64 do 1518 bajtów, zawierające błąd FCS lub błąd wyrównania; *undersize* oznacza pakiety mniejsze niż 64 bajty; *oversize* oznacza pakiety większe niż 1518 bajty; *jabber* oznacza pakiety wysyłane po wystąpieniu kolizji portów; *collision* oznacza Czasy kolizji w segmencie sieci; *64 | 65-127 | 128-255 | 256-511 | 512-1023 | 1024-10240* oznacza łączną liczbę pakietów o określonym rozmiarze.

*absolute | delta*: Wybierz metodę próbkowania dla określonej zmiennej Domyślnym ustawieniem jest *absolute*. W trybie *absolute* przełącznik porównuje wartość próbkowania z ustawionym progiem; w trybie *delta* przełącznik oblicza różnicę pomiędzy wartościami próbkowania bieżącego i poprzedniego cyklu, a następnie porównuje tą różnicę z ustawionym progiem.

*r-hold*: Ustaw próg wzrost dla zmiennej. Poprawne wartości wynoszą od 1 do 2147483647, a wartość domyślna to 100.

*r-event*: Podaj numer identyfikacyjny wpisu Zdarzenia (od 1 do 12), które będzie uruchamiane, gdy wartość próbkowania przekroczy ustawiony próg. Podany tutaj wpis Zdarzenia musi być włączony.

*f-hold*: Ustaw próg spadku dla zmiennej. Poprawne wartości wynoszą od 1 do 2147483647, a wartość domyślna to 100.

*f-event*: Podaj numer identyfikacyjny wpisu Zdarzenia, które będzie uruchamiane, gdy wartość próbkowania będzie niższa niż ustawiony próg. Podany tutaj wpis Zdarzenia musi być włączony.

*rise | fall | all*: Określ typ alarmu. Domyślnym ustawieniem jest *all*. *Rise* oznacza, że Alarm uruchamiany jest tylko wtedy, gdy wartość próbkowania przekracza ustawiony próg wzrostu. *Fall* oznacza, że alarm uruchamiany jest tylko wtedy, gdy wartość próbkowania jest niższa od ustawionego progu spadku. *All* oznacza, że alarm uruchamiany jest, gdy wartość próbkowania przekracza ustawiony próg wzrostu lub jest niższa od ustawionego progu spadku.

*owner-name*: Podaj nazwę właściciela wpisu, używając od 1 do 16 znaków. Domyślną nazwą jest *monitor*.

*interval*: Ustaw częstotliwość próbkowania. Wartości wahają się od 10 do 3600 sekund, a wartością domyślną jest 1800 sekund.

---

|        |                                                                                                                                                                 |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Krok 3 | <b>show rmon alarm</b> [ <i>index</i> ]                                                                                                                         |
|        | Wyświetla skonfigurowany wpis Alarmu i jego ustawienia.                                                                                                         |
|        | <i>index</i> : Wpisz numery identyfikacyjne wpisów Alarmu, które chcesz wyświetlić. Poprawne wartości wynoszą od 1 do 12, a stosowanym formatem jest 1-3 lub 5. |
| Krok 4 | <b>end</b>                                                                                                                                                      |
|        | Powróć do trybu privileged EXEC.                                                                                                                                |
| Krok 5 | <b>copy running-config startup-config</b>                                                                                                                       |
|        | Zapisz ustawienia w pliku konfiguracyjnym.                                                                                                                      |

---

Poniższy schemat przedstawia przykładowy sposób tworzenia wpisu Alarmu do monitorowania BPkets na przełączniku. ID powiązanego wpisu Statystyk będzie 1, typem próbkowania Absolute, progiem wzrostu 3000, numerem identyfikacyjnym powiązanego wpisu zdarzenia dla wzrostu 1, progiem spadku 2000, numerem identyfikacyjnym powiązanego zdarzenia dla spadku 2, typem alarmu all, interwałem powiadomień 10 sekund, a właścicielem wpisu monitor:

### Switch#configure

```
Switch(config)#rmon alarm 1 stats-index 1 alarm-variable bpkt s-type absolute rising-
threshold 3000 rising-event-index 1 falling-threshold 2000 falling-event-index 2 a-type
all interval 10 owner monitor
```

### Switch(config)#show rmon alarm

```
Index-State: 1-Enabled
Statistics index: 1
Alarm variable: BPkt
Sample Type: Absolute
RHold-REvent: 3000-1
FHold-FEvent: 2000-2
Alarm startup: All
Interval: 10
Owner: monitor
```

### Switch(config)#end

### Switch#copy running-config startup-config

# 6 Przykład konfiguracji

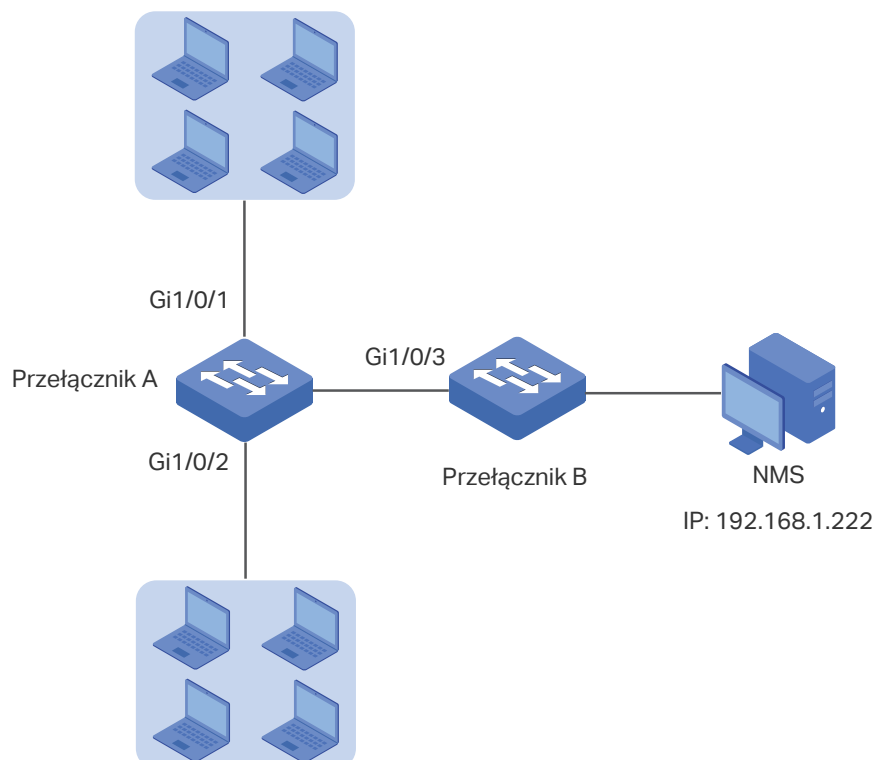
## 6.1 Wymagania sieciowe

Poniższy schemat przedstawia topologię sieci firmy. Wymagania są następujące:

- 1) Monitorowanie ruchu na portach 1/0/1 i 1/0/2 przełącznika A i wysyłanie powiadomień do NMS, gdy rzeczywista częstotliwość przesyłania i odbierania pakietów przekroczy ustawiony próg.
- 2) Monitorowanie stanu wysyłania na portach 1/0/1 i 1/0/2 przełącznika A oraz zbieranie i zapisywanie na bieżąco danych do dalszej kontroli. W szczególności w okresie próbkowania przełącznik A powinien powiadamiać NMS, gdy liczba pakietów przesyłanych i odbieranych na porcie przekracza ustawiony próg; przełącznik A powinien rejestrować, ale nie powinien powiadamiać NMS, gdy liczba pakietów przesyłanych i odbieranych utrzymuje się na poziomie niższym od progu.

Host NMS o adresie IP 192.168.1.222 jest podłączony do przełącznika głównego - przełącznika B. Przełącznik A jest podłączony do przełącznika B poprzez port 1/0/3. Natomiast port 1/0/3 i NMS są zdolne do wykrywania się nawzajem.

Rys. 6-1 Topologia sieci



## 6.2 Schemat konfiguracji

- 1) Ustaw limit szybkości określonych portów, a następnie włącz SNMP na przełączniku A. Skonfiguruj SNMP i powiadomienia oraz włącz komunikaty Trap na portach. Przełącznik A będzie mógł w ten sposób wysyłać powiadomienia do NMS, gdy szybkość przesyłania przekroczy ustawiony próg.
- 2) Po skonfigurowaniu SNMP i powiadomień utwórz wpisy Statystyk na portach w celu monitorowania w czasie rzeczywistym przesyłanych i odbieranych pakietów oraz wpisy Historii w celu zbierania i zapisywania na bieżąco powiązanych danych. Utwórz dwa wpisy Zdarzeń: jeden wpis typu notyfy w celu wysyłania powiadomień do NMS, a drugi typu log w celu rejestrowania powiązanych zdarzeń. Ponadto utwórz także wpis Alarmu, aby monitorować pakiety broadcast (BPkets), ustawić progi wzrostu i spadku oraz powiązać zdarzenie rising z wpisem zdarzenia notyfy oraz zdarzenie falling z wpisem zdarzenia log.

W poniższych podrozdziałach opisano dwa sposoby przeprowadzenia procedury konfiguracji: przez GUI oraz przez CLI.

## 6.3 Przez GUI

### ■ Konfiguracja limitów szybkości na portach

Skonfiguruj limit szybkości na wymaganych portach. Szczegółowe informacje dotyczące konfiguracji znajdują się w części *Konfiguracja QoS*.

## ■ Konfiguracja SNMP

- 1) Wybierz **MAINTENANCE > SNMP > Global Config**, aby wyświetlić poniższą stronę. W sekcji **Global Config** włącz SNMP i ustaw Remote Engine ID jako 123456789a. Kliknij **Apply**.

Rys. 6-2 Włączanie SNMP

Global Config

SNMP:  Enable

Local Engine ID:  Default ID (10-64 Hex)

Remote Engine ID:  (Null or 10-64 Hex)

- 2) W sekcji **SNMP View Config** kliknij **+ Add**, aby wyświetlić poniższą stronę. Ustaw nazwę widoku SNMP jako View, typ widoku jako Include, a MIB Object ID jako 1 (co oznacza wszystkie funkcje). Kliknij **Create**.

Rys. 6-3 Tworzenie widoku SNMP

SNMP View Config

View Name:  (16 characters maximum)

View Type:  Include  Exclude

MIB Object ID:  (61 characters maximum)

- 3) Wybierz **MAINTENANCE > SNMP > SNMP v3 > SNMP Group** i kliknij **+ Add**, aby wyświetlić poniższą stronę. Utwórz grupę o nazwie nms-monitor, włącz uwierzytelnianie i szyfrowanie i dodaj View do Read View i Notify View. Kliknij **Create**.

Rys. 6-4 Konfiguracja grupy SNMP

Group Config

Group Name:  (16 characters maximum)

Security Model: v3

Security Level:  NoAuthNoPriv  AuthNoPriv  AuthPriv

Read View:

Write View:

Notify View:

- 4) Wybierz **MAINTENANCE > SNMP > SNMP v3 > SNMP User** i kliknij **+ Add**, aby wyświetlić poniższą stronę. Utwórz użytkownika o nazwie admin dla NMS, typ

użytkownika jako Remote User i podaj nazwę grupy. Ustaw poziom zabezpieczeń (Security Level) zgodnie z ustawieniami grupy nms-monitor. Wybierz algorytm uwierzytelniania SHA oraz algorytm szyfrowania DES. Ustaw także odpowiednie hasła. Kliknij **Create**.

Rys. 6-5 Tworzenie użytkownika SNMP

**User Config**

User Name:  (16 characters maximum)

User Type:  Local User  Remote User

Group Name:

Security Model: v3

Security Level:  NoAuthNoPriv  AuthNoPriv  AuthPriv

Authentication Mode:  MD5  SHA

Authentication Password:  (16 characters maximum)

Privacy Mode:  DES

Privacy Password:  (16 characters maximum)

- 5) Wybierz **MAINTENANCE > SNMP > Notification > Notification Config** i kliknij Add aby wyświetlić poniższą stronę. Ustaw tryb IP jako IPv4 oraz podaj adres IP hosta NMS i port hosta do przesyłania powiadomień. W polu User wybierz admin, a w polu Type Inform. Ustaw wartość powtórzeń (retry times) jako 3, a limit czasu (timeout period) jako 100 sekund. Kliknij **Create**.

Rys. 6-16 Tworzenie wpisu powiadomienia SNMP

**Notification Config**

IP Mode:  IPv4  IPv6

IP Address:  (Format:192.168.0.1)

UDP Port:  (0-65535)

User:

Security Mode:  v1  v2c  v3

Security Level:  NoAuthNoPriv  AuthNoPriv  AuthPriv

Type:  Trap  Inform

Retry Times:  (1-255)

Timeout:  (1-3600)

- 6) Wybierz **MAINTENANCE > SNMP > Notification > Trap Config**, aby wyświetlić poniższą stronę. Włącz komunikat trap limitu szybkości i kliknij **Apply**.



Rys. 6-17 Włączenie komunikatu trap limitu prędkości

Notification Config   Trap Config


SNMP Traps

|                                                         |                                                |                                               |
|---------------------------------------------------------|------------------------------------------------|-----------------------------------------------|
| <input checked="" type="checkbox"/> SNMP Authentication | <input checked="" type="checkbox"/> Coldstart  | <input checked="" type="checkbox"/> Warmstart |
| <input checked="" type="checkbox"/> Link Status         | <input type="checkbox"/> CPU Utilization       | <input type="checkbox"/> Memory Utilization   |
| <input type="checkbox"/> Flash Operation                | <input type="checkbox"/> VLAN Create/Delete    | <input type="checkbox"/> IP Change            |
| <input type="checkbox"/> Storm Control                  | <input checked="" type="checkbox"/> Rate Limit | <input type="checkbox"/> LLDP                 |
| <input type="checkbox"/> Loopback Detection             | <input type="checkbox"/> Spanning Tree         | <input type="checkbox"/> IP-MAC Binding       |
| <input type="checkbox"/> IP Duplicate                   | <input type="checkbox"/> DHCP Filter           | <input type="checkbox"/> ACL Counter          |

**Apply**

7) Kliknij , aby zapisać ustawienia.

### ■ Konfiguracja RMON

- Wybierz **MAINTENANCE > SNMP > RMON > Statistics** i kliknij  Add , aby wyświetlić poniższą stronę. Utwórz dwa wpisy i powiąż je odpowiednio z portami 1/0/1 i 1/0/2. Ustaw właściciela wpisów (owner) jako monitor, a stan jako valid.

Rys. 6-18 Konfiguracja wpisu 1 Statystyk

Statistics Config

Index:  (1-65535)

Port:  **Choose** (Format: 1/0/1)

Owner:  (16 characters maximum)

Status:  Valid  Under Creation

**Cancel**   **Create**

Rys. 6-19 Konfiguracja wpisu 2 Statystyk

Statistics Config

Index:  (1-65535)

Port:  **Choose** (Format: 1/0/1)

Owner:  (16 characters maximum)

Status:  Valid  Under Creation

**Cancel**   **Create**

- Wybierz z menu **MAINTENANCE > SNMP > RMON > History**, aby wyświetlić poniższą stronę. Skonfiguruj wpisy 1 i 2. Powiąż wpisy 1 i 2 odpowiednio z portami 1/0/1 i 1/0/2, ustaw interwał jako 100 sekund, Maximum Buckets jako 50, właściciela wpisów (owner) jako monitor, a stan jako Enable.

Rys. 6-20 Konfiguracja wpisów Historii

| History Control Config   |       |       |                    |                 |         |          |
|--------------------------|-------|-------|--------------------|-----------------|---------|----------|
| <input type="checkbox"/> | Index | Port  | Interval (seconds) | Maximum Buckets | Owner   | Status   |
| <input type="checkbox"/> | 1     | 1/0/1 | 100                | 50              | monitor | Enabled  |
| <input type="checkbox"/> | 2     | 1/0/2 | 100                | 50              | monitor | Enabled  |
| <input type="checkbox"/> | 3     | 1/0/1 | 1800               | 50              | monitor | Disabled |
| <input type="checkbox"/> | 4     | 1/0/1 | 1800               | 50              | monitor | Disabled |
| <input type="checkbox"/> | 5     | 1/0/1 | 1800               | 50              | monitor | Disabled |
| <input type="checkbox"/> | 6     | 1/0/1 | 1800               | 50              | monitor | Disabled |
| <input type="checkbox"/> | 7     | 1/0/1 | 1800               | 50              | monitor | Disabled |
| <input type="checkbox"/> | 8     | 1/0/1 | 1800               | 50              | monitor | Disabled |
| <input type="checkbox"/> | 9     | 1/0/1 | 1800               | 50              | monitor | Disabled |
| <input type="checkbox"/> | 10    | 1/0/1 | 1800               | 50              | monitor | Disabled |
| Total: 12                |       |       |                    |                 |         |          |

- 3) Wybierz z menu **MAINTENANCE > SNMP > RMON > Event**, aby wyświetlić poniższą stronę. Skonfiguruj wpisy 1 i 2. Dla wpisu 1 ustaw nazwę użytkownika SNMP (user name) jako admin, typ jako Notify, opis (description) jako "rising\_notify", właściciela (owner) jako monitor, a stan jako enable. Dla wpisu 2 ustaw nazwę użytkownika SNMP (user name) jako admin, typ jako Log, opis (description) jako "falling\_log", właściciela (owner) jako monitor, a stan jako enable.

Rys. 6-21 Konfiguracja wpisów Zdarzeń

| Event Config             |       |        |               |             |         |          |
|--------------------------|-------|--------|---------------|-------------|---------|----------|
| <input type="checkbox"/> | Index | User   | Description   | Action Mode | Owner   | Status   |
| <input type="checkbox"/> | 1     | admin  | rising_notify | Notify      | monitor | Enabled  |
| <input type="checkbox"/> | 2     | admin  | falling_log   | Log         | monitor | Enabled  |
| <input type="checkbox"/> | 3     | public |               | None        | monitor | Disabled |
| <input type="checkbox"/> | 4     | public |               | None        | monitor | Disabled |
| <input type="checkbox"/> | 5     | public |               | None        | monitor | Disabled |
| <input type="checkbox"/> | 6     | public |               | None        | monitor | Disabled |
| <input type="checkbox"/> | 7     | public |               | None        | monitor | Disabled |
| <input type="checkbox"/> | 8     | public |               | None        | monitor | Disabled |
| <input type="checkbox"/> | 9     | public |               | None        | monitor | Disabled |
| <input type="checkbox"/> | 10    | public |               | None        | monitor | Disabled |
| Total: 12                |       |        |               |             |         |          |

- 4) Wybierz **MAINTENANCE > SNMP > RMON > Alarm**, aby wyświetlić poniższą stronę. Skonfiguruj wpisy 1 i 2. Dla wpisu 1 ustaw zmienną alarmu (alarm variable) jako BPkets, ID wpisów powiązanych statystyk (statistics entry ID) jako 1 (powiązanie z portem 1/0/1), typ próbkowania (sample type) jako Absolute, próg wzrostu (rising threshold) jako 3000, ID wpisu powiązanego zdarzenia (rising event entry ID) jako 1 (oznacza typ notify), próg spadku (falling threshold) jako 2000, ID wpisu powiązanego zdarzenia (falling event entry ID) jako 2 (oznacza typ log), typ alarmu jako All, interwał jako 10 sekund, a nazwę właściciela (owner name) jako monitor. Dla wpisu 2 ustaw ID wpisów powiązanych

statystyk (statistics entry ID) jako 2 (powiązanie z portem 1/0/2). Pozostałe ustawienia są takie same jak dla wpisu 1.

Rys. 6-22 Konfiguracja wpisów Alarmu

| <input type="checkbox"/> | Index | Variable | Statistics | Sample Type | Rising Threshold | Rising Event | Falling Threshold | Falling Event | Alarm Type | Interval (seconds) | Owner   | Status   |
|--------------------------|-------|----------|------------|-------------|------------------|--------------|-------------------|---------------|------------|--------------------|---------|----------|
| <input type="checkbox"/> | 1     | BPackets | 1          | Absolute    | 3000             | 1            | 2000              | 2             | All        | 10                 | monitor | Enabled  |
| <input type="checkbox"/> | 2     | BPackets | 2          | Absolute    | 3000             | 1            | 2000              | 2             | All        | 10                 | monitor | Enabled  |
| <input type="checkbox"/> | 3     | RecBytes | 0          | Absolute    | 100              | 0            | 100               | 0             | All        | 1800               | monitor | Disabled |
| <input type="checkbox"/> | 4     | RecBytes | 0          | Absolute    | 100              | 0            | 100               | 0             | All        | 1800               | monitor | Disabled |
| <input type="checkbox"/> | 5     | RecBytes | 0          | Absolute    | 100              | 0            | 100               | 0             | All        | 1800               | monitor | Disabled |
| <input type="checkbox"/> | 6     | RecBytes | 0          | Absolute    | 100              | 0            | 100               | 0             | All        | 1800               | monitor | Disabled |
| <input type="checkbox"/> | 7     | RecBytes | 0          | Absolute    | 100              | 0            | 100               | 0             | All        | 1800               | monitor | Disabled |
| <input type="checkbox"/> | 8     | RecBytes | 0          | Absolute    | 100              | 0            | 100               | 0             | All        | 1800               | monitor | Disabled |
| <input type="checkbox"/> | 9     | RecBytes | 0          | Absolute    | 100              | 0            | 100               | 0             | All        | 1800               | monitor | Disabled |
| <input type="checkbox"/> | 10    | RecBytes | 0          | Absolute    | 100              | 0            | 100               | 0             | All        | 1800               | monitor | Disabled |

Total: 12

5) Kliknij , aby zapisać ustawienia.

## 6.4 Przez CLI

### ■ Konfiguracja limitu szybkości na portach

Skonfiguruj limit szybkości na wymaganych portach przełącznika A. Szczegółowe informacje dotyczące konfiguracji znajdują się w części [Konfiguracja QoS](#).

### ■ Konfiguracja SNMP

1) Włącz SNMP i ustaw zdalny engine ID.

```
Switch_A#configure
```

```
Switch_A(config)#snmp-server
```

```
Switch_A(config)#snmp-server engineID remote 123456789a
```

2) Ustaw widok o nazwie View; ustaw MIB Object ID jako 1 (co oznacza wszystkie funkcje), a typ widoku jako Include.

```
Switch_A(config)#snmp-server view View 1 include
```

3) Utwórz grupę SNMPv3 o nazwie nms-monitor. Włącz tryb Auth i Privacy oraz ustaw widok jako read view i notify view.

```
Switch_A(config)#snmp-server group nms-monitor smode v3 slev authPriv read View notify View
```

4) Utwórz użytkownika SNMP o nazwie admin. Ustaw typ jako remote user i skonfiguruj parametry Security Model i Security Level zgodnie z ustawieniami grupy. Ustaw tryb Auth jako algorytm SHA, hasło jako 1234, tryb Privacy jako DES, a hasło jako 1234.

```
Switch_A(config)#snmp-server user admin remote nms-monitor smode v3 slev authPriv cmode SHA cpwd 1234 emode DES epwd 1234
```

- 5) Aby skonfigurować Notification, ustaw adres IP hosta NMS i portu UDP. Ustaw parametry User, Security Model i Security Level zgodnie z ustawieniami użytkownika SNMP. Wybierz typ jako Inform, i ustaw retry times jako 3, a timeout period jako 100 sekund.

```
Switch_A(config)#snmp-server host 192.168.1.222 162 admin smode v3 slev authPriv
type inform retries 3 timeout 100
```

- Włączanie komunikatów trap kontroli przepustowości (Bandwidth-control Trap)

```
Switch_A(config)#snmp-server traps bandwidth-control
```

- Konfiguracja RMON

- 1) Utwórz dwa wpisy Statystyk, aby monitorować odpowiednio porty 1/0/1 i 1/0/2. Właściciel wpisów (owner) ustawiony jest jako monitor, a stan jako valid.

```
Switch_A(config)#rmon statistics 1 interface gigabitEthernet 1/0/1 owner monitor
status valid
```

```
Switch_A(config)#rmon statistics 2 interface gigabitEthernet 1/0/2 owner monitor
status valid
```

- 2) Utwórz dwa wpisy Historii i powiąż je odpowiednio z portami 1/0/1 i 1/0/2. Ustaw sample interval jako 100, max buckets jako 50, a właściciela (owner) jako monitor.

```
Switch_A(config)#rmon history 1 interface gigabitEthernet 1/0/1 interval 100 owner
monitor buckets 50
```

```
Switch_A(config)#rmon history 2 interface gigabitEthernet 1/0/2 interval 100 owner
monitor buckets 50
```

- 3) Utwórz dwa wpisy Zdarzeń o nazwie admin, czyli nazwie użytkownika SNMP. Ustaw typ wpisu 1 jako Notify, a jego opis jako "rising\_notify". Ustaw typ wpisu 2 jako Log, a jego opis jako "falling\_log". Ustaw ich właściciela (owner) jako monitor.

```
Switch_A(config)#rmon event 1 user admin description rising_notify type notify owner
monitor
```

```
Switch_A(config)#rmon event 2 user admin description falling_log type log owner
monitor
```

- 4) Utwórz dwa wpisy Alarmu. Dla wpisu 1 ustaw zmienną alarmu (alarm variable) jako Bpackets, ID wpisów powiązanych statystyk (statistics entry ID) jako 1 (powiązanie z portem 1/0/1), typ próbkowania (sample type) jako Absolute, próg wzrostu (rising threshold) jako 3000, ID wpisu powiązanego zdarzenia (rising event entry ID) jako 1 (oznacza typ notify), próg spadku (falling threshold) jako 2000, ID wpisu powiązanego zdarzenia (falling event entry ID) jako 2 (oznacza typ log), typ alarmu jako All, interwał jako 10 sekund, a nazwę właściciela (owner name) jako monitor. Dla wpisu 2 ustaw ID wpisu powiązanych statystyk (statistics entry ID) jako 2 (powiązanie z portem 1/0/2). Pozostałe ustawienia są takie same jak dla wpisu 1.

```
Switch_A(config)#rmon alarm 1 stats-index 1 alarm-variable bpkt s-type absolute
rising-threshold 3000 rising-event-index 1 falling-threshold 2000 falling-event-index 2
a-type all interval 10 owner monitor
```

```
Switch_A(config)#rmon alarm 2 stats-index 2 alarm-variable bpkt s-type absolute
rising-threshold 3000 rising-event-index 1 falling-threshold 2000 falling-event-index 2
a-type all interval 10 owner monitor
```

## Sprawdzanie konfiguracji

Sprawdzanie globalnej konfiguracji SNMP:

```
Switch_A(config)#show snmp-server
```

SNMP agent is enabled.

- 0 SNMP packets input
  - 0 Bad SNMP version errors
  - 0 Unknown community name
  - 0 Illegal operation for community name supplied
  - 0 Encoding errors
  - 0 Number of requested variables
  - 0 Number of altered variables
  - 0 Get-request PDUs
  - 0 Get-next PDUs
  - 0 Set-request PDUs
- 0 SNMP packets output
  - 0 Too big errors(Maximum packet size 1500)
  - 0 No such name errors
  - 0 Bad value errors
  - 0 General errors
  - 0 Response PDUs
  - 0 Trap PDUs

Sprawdzanie engine ID SNMP:

```
Switch_A(config)#show snmp-server engineID
```

Local engine ID: 80002e5703000aeb13a23d

Remote engine ID: 123456789a

Sprawdzanie konfiguracji widoku SNMP:

Switch\_A(config)#show snmp-server view

| No. | View Name   | Type    | MOID           |
|-----|-------------|---------|----------------|
| 1   | viewDefault | include | 1              |
| 2   | viewDefault | exclude | 1.3.6.1.6.3.15 |
| 3   | viewDefault | exclude | 1.3.6.1.6.3.16 |
| 4   | viewDefault | exclude | 1.3.6.1.6.3.18 |
| 5   | View        | include | 1              |

Sprawdzanie konfiguracji grupy SNMP:

Switch\_A(config)#show snmp-server group

| No. | Name        | Sec-Mode | Sec-Lev  | Read-View | Write-View | Notify-View |
|-----|-------------|----------|----------|-----------|------------|-------------|
| 1   | nms-monitor | v3       | authPriv | View      |            | View        |

Sprawdzanie konfiguracji użytkownika SNMP:

Switch\_A(config)#show snmp-server user

| No. | U-Name | U-Type | G-Name      | S-Mode | S-Lev    | A-Mode | P-Mode |
|-----|--------|--------|-------------|--------|----------|--------|--------|
| 1   | admin  | remote | nms-monitor | v3     | authPriv | SHA    | DES    |

Sprawdzanie konfiguracji hosta SNMP:

Switch\_A(config)#show snmp-server host

| No. | Des-IP        | UDP | Name  | SecMode | SecLev   | Type   | Retry | Timeout |
|-----|---------------|-----|-------|---------|----------|--------|-------|---------|
| 1   | 172.168.1.222 | 162 | admin | v3      | authPriv | inform | 3     | 100     |

Sprawdzanie konfiguracji statystyk RMON:

Switch\_A(config)#show rmon statistics

| Index | Port    | Owner   | State |
|-------|---------|---------|-------|
| 1     | Gi1/0/1 | monitor | valid |
| 2     | Gi1/0/2 | monitor | valid |

Sprawdzanie konfiguracji historii RMON:

Switch\_A(config)#show rmon history

| Index | Port    | Interval | Buckets | Owner   | State  |
|-------|---------|----------|---------|---------|--------|
| 1     | Gi1/0/1 | 100      | 50      | monitor | Enable |
| 2     | Gi1/0/2 | 100      | 50      | monitor | Enable |

Sprawdzanie konfiguracji zdarzeń RMON:

Switch\_A(config)#show rmon event

| Index | User  | Description   | Type   | Owner   | State  |
|-------|-------|---------------|--------|---------|--------|
| 1     | admin | rising-notify | Notify | monitor | Enable |
| 2     | admin | falling-log   | Log    | monitor | Enable |

Sprawdzanie konfiguracji alarmu RMON:

Switch\_A(config)#show rmon alarm

Index-State: 1-Enabled

Statistics index: 1

Alarm variable: BPkt

Sample Type: Absolute

RHold-REvent: 3000-1

FHold-FEvent: 2000-2

Alarm startup: All

Interval: 10

Owner: monitor

---

Index-State: 2-Enabled  
Statistics index: 2  
Alarm variable: BPkt  
Sample Type: Absolute  
RHold-REvent: 3000-1  
FHold-FEvent: 2000-2  
Alarm startup: All  
Interval: 10  
Owner: monitor



# Część 33

## Konfiguracja dzienników systemowych

### ROZDZIAŁY

1. Informacje ogólne
2. Konfiguracja dzienników systemowych
3. Przykład konfiguracji

# 1 Informacje ogólne

Przełącznik generuje komunikaty w odpowiedzi na wydarzenia, awarie lub błędy, a także na zmiany w konfiguracji lub inne zdarzenia. Komunikaty systemowe są pomocne w procesie debugowania i zarządzania siecią.

Dzienniki systemowe mogą być zapisywane w różnych lokalizacjach, takich jak bufor dzienników (log buffer), plik dzienników (log file), czy też zdalne serwery dzienników, w zależności od konfiguracji. Dzienniki zapisane w buforze lub pliku dzienników nazywane są dziennikami lokalnymi (local logs), a dzienniki zapisane na serwerze zdalnym nazywane są dziennikami zdalnymi (remote logs). Dzienniki zdalne umożliwiają zdalne monitorowanie stanu działania sieci.

Parametr istotności komunikatu zdarzenia (severity level) pozwala na kontrolowanie typu komunikatów dziennika zapisywanych w różnych lokalizacjach.

## 2 Konfiguracja dzienników systemowych

Na konfigurację dzienników systemowych składają się:

- konfiguracja dzienników lokalnych.
- konfiguracja dzienników zdalnych.
- tworzenie kopii zapasowych dzienników.
- wyświetlanie tablicy dzienników.

### Wskazówki dotyczące konfiguracji

Zdarzenia systemowe klasyfikuje się przez przypisywanie ich do jednego z ośmiu poziomów. Komunikaty poziomów 0-4 świadczą o pogorszeniu działania przełącznika. W przypadku komunikatu o zdarzeniu należy podjąć sugerowane działanie.

Tabela 2-1 Poziomy zdarzeń

| Komunikaty    | Poziom | Opis                                                                                                                             | Przykład                                                     |
|---------------|--------|----------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------|
| Emergencies   | 0      | System nie działa i konieczny jest restart przełącznika.                                                                         | Usterki oprogramowania wpływające na działanie przełącznika. |
| Alerts        | 1      | Należy natychmiastowo podjąć odpowiednie działania.                                                                              | Wykorzystanie pamięci osiągnęło wyznaczony limit.            |
| Critical      | 2      | Należy natychmiastowo podjąć odpowiednie działania lub przeprowadzić analizę przyczyn.                                           | Wykorzystanie pamięci osiągnęło próg ostrzegawczy.           |
| Errors        | 3      | Błędne działania lub niestandardowe przetwarzanie, które nie wpłyną na kolejne działania. Powinny jednak zostać przeanalizowane. | Wprowadzono błędne polecenie lub hasło.                      |
| Warnings      | 4      | Warunki, które mogą spowodować błąd przetwarzania i które powinny być odnotowane.                                                | Wykryto błędne pakiety protokołu.                            |
| Notifications | 5      | Standardowe, ale istotne warunki.                                                                                                | Zastosowano polecenie zamknięcia portu.                      |
| Informational | 6      | Standardowe komunikaty informacyjne.                                                                                             | Zastosowano polecenie wyświetlania.                          |
| Debugging     | 7      | Komunikaty z poziomu śledzenia, które możesz zignorować.                                                                         | Standardowe informacje operacyjne.                           |

## 2.1 Przez GUI

### 2.1.1 Konfiguracja dzienników lokalnych

Wybierz z menu **MAINTENANCE > Logs > Local Logs**, aby wyświetlić poniższą stronę.

Rys. 2-1 Konfiguracja dzienników lokalnych

| <input type="checkbox"/>            | Channel    | Severity | Status  | Sync-Period |
|-------------------------------------|------------|----------|---------|-------------|
| <input checked="" type="checkbox"/> | Log Buffer | level_6  | Enable  | Immediately |
| <input type="checkbox"/>            | Log File   | level_3  | Disable | 24hour(s)   |

Total: 2      1 entry selected.      Cancel Apply

Wykonaj poniższe kroki, aby skonfigurować dzienniki lokalne:

- 1) Wybierz kanał i skonfiguruj odpowiedni poziom istotności zdarzenia oraz stan kanału.

|               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|---------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Channel       | <p>Dzienniki lokalne zawierają 2 kanały: Log buffer (bufor dziennika) i Log file (plik dziennika).</p> <p>Bufor dziennika wskazuje RAM do zapisywania dzienników systemowych. Kanał jest domyślnie włączony. Informacje z buforu dziennika wyświetlane są na stronie <b>MAINTENANCE &gt; Logs &gt; Logs Table</b>. Po restarcie przełącznika dane zostaną utracone.</p> <p>Plik dziennika wskazuje na sektor pamięci flash do zapisywania dzienników systemowych. Informacje zapisane w pliku dziennika nie zostaną utracone po restarcie przełącznika i mogą być wyeksportowane na stronie <b>MAINTENANCE &gt; Logs &gt; Back Up Logs</b>.</p> |
| Severity      | <p>Ustaw poziom istotności komunikatu zdarzenia zapisanego na wybranym kanale. Zapisywane będą tylko komunikaty o tym samym co wyznaczony tu poziom lub o niższym poziomie istotności. Istnieje osiem poziomów istotności, oznaczonych od 0 do 7. Im niższy poziom, tym istotniejsza jest wiadomość.</p>                                                                                                                                                                                                                                                                                                                                        |
| Status        | <p>Włącz lub wyłącz kanał.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Sync-Periodic | <p>Domyślnie dane dziennika są natychmiastowo zapisywane w buforze dziennika i synchronizowane w pliku dziennika raz na 24 godziny. W razie konieczności możesz zmodyfikować częstotliwość synchronizacji dziennika, używając CLI.</p>                                                                                                                                                                                                                                                                                                                                                                                                          |

- 2) Kliknij **Apply**.

### 2.1.2 Konfiguracja dzienników zdalnych

Możesz skonfigurować otrzymywanie dzienników systemowych przełącznika na maks. czterech hostach. Hosty te nazywane są Log Servers (Serwery dzienników). Po wygenerowaniu komunikatu dziennika przełącznik będzie przekazywał komunikat do

serwerów. Aby wyświetlić dzienniki, serwery powinny obsługiwać oprogramowanie dziennika serwera zgodne ze standardem dzienników systemowych.

Wybierz z menu **MAINTENANCE > Logs > Remote Logs**, aby wyświetlić poniższą stronę.

Rys. 2-2 Konfiguracja dzienników zdalnych

| Log Server Config        |       |           |          |          |         |  |
|--------------------------|-------|-----------|----------|----------|---------|--|
| <input type="checkbox"/> | Index | Server IP | UDP Port | Severity | Status  |  |
| <input type="checkbox"/> | 1     | 0.0.0.0   | 514      | level_6  | Disable |  |
| <input type="checkbox"/> | 2     | 0.0.0.0   | 514      | level_6  | Disable |  |
| <input type="checkbox"/> | 3     | 0.0.0.0   | 514      | level_6  | Disable |  |
| <input type="checkbox"/> | 4     | 0.0.0.0   | 514      | level_6  | Disable |  |
| Total: 4                 |       |           |          |          |         |  |

Wykonaj poniższe kroki, aby skonfigurować informacje o serwerach dziennika zdalnego:

- 1) Wybierz wpis do włączenia serwera, następnie ustaw adres IP serwera i poziom istotności zdarzenia.

|           |                                                                                                                                                                              |
|-----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Server IP | Wyznacz adres IP serwera dziennika.                                                                                                                                          |
| UDP Port  | Informacja o porcie UDP, wykorzystywanym przez serwer do odbierania komunikatów dziennika. Do wysyłania komunikatów dziennika przełącznik wykorzystuje standardowy port 514. |
| Severity  | Określ poziom istotności komunikatów dziennika wysyłanych na wybrany serwer dziennika. Zapisywane będą tylko komunikaty o tym samym lub o niższym poziomie istotności.       |
| Status    | Włącz lub wyłącz serwer dziennika.                                                                                                                                           |

- 2) Kliknij **Apply**.

### 2.1.3 Tworzenie kopii zapasowych dzienników

Wybierz z menu **MAINTENANCE > Logs > Back Up Logs**, aby wyświetlić poniższą stronę.

Rys. 2-3 Tworzenie kopii zapasowej pliku dziennika

Back Up Logs

---

Click this button to back up the log file.

[Back Up Logs](#)

Kliknij **Back Up Logs**, aby zapisać dzienniki systemowe jako plik na twoim komputerze. W przypadku awarii systemu przełącznika, możesz sprawdzić plik do rozwiązywania problemów.

## 2.1.4 Wyświetlanie tablicy dzienników

Wybierz z menu **MAINTENANCE > Logs > Log Table**, aby wyświetlić poniższą stronę.

Rys. 2-4 Wyświetlanie tablicy dzienników

| Log Info   |                     |               |              |                                                 |
|------------|---------------------|---------------|--------------|-------------------------------------------------|
| Index      | Time                | Module        | Severity     | Content                                         |
|            |                     | All Modules ▼ | All Levels ▼ |                                                 |
| 1          | 2006-01-13 08:53:42 | User          | level_5      | Login the web by admin on web (192.168.0.200).  |
| 2          | 2006-01-13 08:26:39 | User          | level_5      | Login the web by admin on web (192.168.0.200).  |
| 3          | 2006-01-13 08:02:52 | User          | level_5      | Login the web by admin on web (192.168.0.200).  |
| 4          | 2006-01-13 07:43:30 | User          | level_5      | Login the web by admin on web (192.168.0.200).  |
| 5          | 2006-01-13 07:13:29 | User          | level_5      | Login the web by admin on web (192.168.0.200).  |
| 6          | 2006-01-13 06:57:09 | User          | level_5      | Login the web by admin on web (192.168.0.200).  |
| 7          | 2006-01-13 06:48:10 | User          | level_5      | Login the web by admin on web (192.168.0.200).  |
| 8          | 2006-01-13 06:27:44 | User          | level_5      | Login the web by admin on web (192.168.0.200).  |
| 9          | 2006-01-11 15:27:43 | User          | level_5      | Logout the CLI.                                 |
| 10         | 2006-01-11 15:27:08 | User          | level_5      | Login the CLI by admin on vty0 (192.168.0.200). |
| Total: 184 |                     |               |              |                                                 |

Wybierz blok i poziom istotności, aby wyświetlić odpowiednie dane dziennika.

|          |                                                                                                                                                                                                             |
|----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Time     | Informacja o czasie, w którym wystąpiło zdarzenie dziennika. Aby poznać dokładny czas zdarzenia, należy skonfigurować czas systemu na stronie zarządzania <b>SYSTEM &gt; System Info &gt; System Time</b> . |
| Module   | Z rozwijanej listy wybierz blok, aby wyświetlić odpowiednie dane dziennika.                                                                                                                                 |
| Severity | Wybierz poziom istotności. Wyświetlane będą tylko komunikaty o tym samym lub o niższym poziomie istotności.                                                                                                 |
| Content  | Szczegółowe dane zdarzenia dziennika.                                                                                                                                                                       |

## 2.2 Przez CLI

### 2.2.1 Konfiguracja dzienników lokalnych

Wykonaj poniższe kroki, aby skonfigurować dzienniki lokalne:

|        |                                                          |
|--------|----------------------------------------------------------|
| Krok 1 | <b>configure</b><br>Uruchom tryb konfiguracji globalnej. |
|--------|----------------------------------------------------------|

---

|        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Krok 2 | <b>logging buffer</b><br>Skonfiguruj przełącznik tak, aby zapisywał komunikaty systemowe w buforze dziennika. Bufor dziennika wskazuje RAM do zapisywania dzienników systemowych. Po restarcie przełącznika dane w buforze dziennika zostaną utracone. Możesz wyświetlić dzienniki za pomocą polecenia <code>show logging buffer</code> .                                                                                                                                                                                                            |
| Krok 3 | <b>logging buffer level <i>level</i></b><br>Określ, na jakim poziomie istotności dane dziennika powinny być zapisywane w buforze.<br><i>level</i> : Wpisz poziom istotności, między 0 a 7. Im niższy poziom, tym większa waga komunikatu. Zapisywane będą tylko zdarzenia o wyznaczonym tu lub niższym poziomie istotności. Poziom domyślny to 6. Oznacza to, że w buforze dziennika zapisywane będą komunikaty zdarzeń o poziomie istotności między 0 a 6.                                                                                          |
| Krok 4 | <b>logging file flash</b><br>Skonfiguruj przełącznik tak, by komunikaty systemowe zapisywane były w pliku dziennika. Plik dziennika wskazuje na sektor pamięci flash do zapisywania dzienników systemowych. Informacje zapisane w pliku dziennika nie zostaną utracone po restarcie przełącznika. Możesz wyświetlić dzienniki za pomocą polecenia <b>show logging flash</b> .                                                                                                                                                                        |
| Krok 5 | <b>logging file flash frequency { <i>periodic</i> <i>periodic</i>   <i>immediate</i> }</b><br>Ustaw częstotliwość, z jaką synchronizowane będą dzienniki systemowe z bufora dziennika w sektorze pamięci flash.<br><i>periodic</i> : Wyznacz częstotliwość, między 1 a 48 godzin. Domyślnie synchronizacja przeprowadzana jest raz na 24 godziny.<br><b>immediate</b> : Plik dziennika systemowego w buforze będzie natychmiastowo synchronizowany w sektorze pamięci flash. Opcja ta oznacza, że częste działania w obszarze flash nie są zalecane. |
| Krok 6 | <b>logging file flash level <i>level</i></b><br>Określ, na jakim poziomie istotności dane dziennika powinny być zapisywane w sektorze flash.<br><i>level</i> : Wpisz poziom istotności, między 0 a 7. Im niższy poziom, tym większa waga komunikatu. W sektorze flash zapisywane będą tylko komunikaty zdarzeń o wyznaczonym tu lub niższym poziomie istotności. Poziom domyślny to 3. Oznacza to, że w sektorze flash zapisywane będą komunikaty zdarzeń o poziomie istotności między 0 a 3.                                                        |
| Krok 7 | <b>show logging local-config</b><br>Sprawdź dane konfiguracyjne dzienników lokalnych.                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Krok 8 | <b>end</b><br>Wróć do trybu privileged EXEC.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Krok 9 | <b>copy running-config startup-config</b><br>Zapisz ustawienia w pliku konfiguracyjnym.                                                                                                                                                                                                                                                                                                                                                                                                                                                              |

---

Poniższy przykład prezentuje konfigurację na przełączniku dzienników lokalnych. W buforze dziennika zapisywane będą komunikaty z poziomów 0-5, komunikaty z poziomów 0-2 będą synchronizowane w sektorze flash raz na 10 godzin:

### Switch#configure

```
Switch(config)#logging buffer
```

```
Switch(config)#logging buffer level 5
```

```
Switch(config)#logging file flash
```

```
Switch(config)#logging file flash frequency periodic 10
```

```
Switch(config)#logging file flash level 2
```

```
Switch(config)#show logging local-config
```

| Channel | Level | Status | Sync-Periodic |
|---------|-------|--------|---------------|
| -----   | ----- | -----  | -----         |
| Buffer  | 5     | enable | Immediately   |
| Flash   | 2     | enable | 10 hour(s)    |
| Console | 5     | enable | Immediately   |
| Monitor | 5     | enable | Immediately   |

```
Switch(config)#end
```

```
Switch#copy running-config startup-config
```

## 2.2.2 Konfiguracja dzienników zdalnych

Możesz skonfigurować otrzymywanie dzienników systemowych przełącznika na maks. czterech hostach. Hosty te nazywane są Log Servers (Serwery dzienników). Po wygenerowaniu komunikatu dziennika przełącznik będzie przekazywał komunikat do serwerów. Aby wyświetlić dzienniki, serwery powinny obsługiwać oprogramowanie dziennika serwera zgodne ze standardem dzienników systemowych.

Wykonaj poniższe kroki, aby skonfigurować dziennik zdalny:

### Krok 1 **configure**

Uruchom tryb konfiguracji globalnej.

### Krok 2 **logging host index *idx* host-ip level**

Skonfiguruj host zdalny, który będzie odbierał dzienniki systemowe przełącznika. Taki host nazywany jest Log Server (Serwer dziennika). Za pomocą serwera dziennika możesz zdalnie monitorować ustawienia i status działania przełącznika.

*idx*: Wpisz indeks serwera dziennika. Przełącznik może obsługiwać maks. 4 serwery dziennika.

*host-ip*: Wpisz adres IP serwera dziennika.

*level*: Określ, na jakim poziomie istotności dane dziennika powinny być zapisywane na serwerze dziennika. Wpisz poziom istotności, między 0 a 7. Im niższy poziom, tym większa waga komunikatu. Zapisywane będą tylko komunikaty zdarzeń o wyznaczonym tu lub niższym poziomie istotności. Poziom domyślny to 6. Oznacza to, że zapisywane będą komunikaty zdarzeń o poziomie istotności między 0 a 6.



Krok 3 **show logging loghost [ *index* ]**

Sprawdź dane konfiguracyjne serwera dziennika.

*index*: Wpisz indeks serwera dziennika, aby wyświetlić odpowiednie dane konfiguracyjne. Jeżeli nie zostanie wyznaczona żadna wartość, wyświetlone zostaną dane wszystkich hostów dziennika.

Krok 4 **end**

Wróć do trybu privileged EXEC.

Krok 5 **copy running-config startup-config**

Zapisz ustawienia w pliku konfiguracyjnym.

Poniższy przykład prezentuje ustawianie na przełączniku dziennika zdalnego, włączanie dziennika serwera 2, ustawianie jego adresu IP na 192.168.0.148 i włączenie wysyłania na serwer komunikatów zdarzeń z poziomów 0-5:

**Switch#configure**

**Switch(config)# logging host index 2 192.168.0.148 5**

**Switch(config)# show logging loghost**

| Index | Host-IP       | Severity | Status  |
|-------|---------------|----------|---------|
| ----  | -----         | -----    | -----   |
| 1     | 0.0.0.0       | 6        | disable |
| 2     | 192.168.0.148 | 5        | enable  |
| 3     | 0.0.0.0       | 6        | disable |
| 4     | 0.0.0.0       | 6        | disable |

**Switch(config)#end**

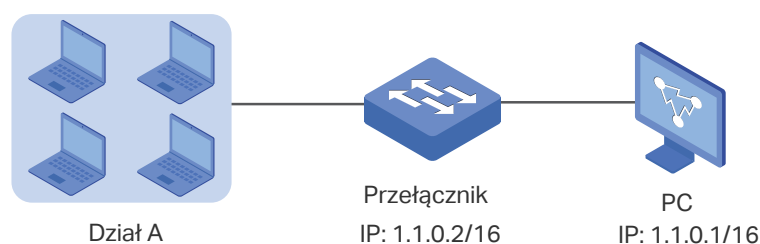
**Switch#copy running-config startup-config**

# 3 Przykład konfiguracji

## 3.1 Wymagania sieciowe

Administrator sieci firmowej musi monitorować sieć działu A, aby wykrywać i rozwiązywać występujące problemy.

Rys. 3-1 Topologia sieci



## 3.2 Schemat konfiguracji

Administrator sieci może skonfigurować komputer tak, aby pełnił funkcję serwera dzienników, na którym zapisywane będą dzienniki systemowe przełącznika. Należy upewnić się, że przełącznik i komputer wykrywają się nawzajem, a następnie skonfigurować serwer dzienników, który jest zgodny ze standardem syslog na komputerze oraz ustawić komputer jako serwer dzienników.

W poniższych podrozdziałach opisano dwa sposoby przeprowadzenia procedury konfiguracji: przez GUI oraz przez CLI.

## 3.3 Przez GUI

- 1) Wybierz z menu **MAINTENANCE > Logs > Remote Logs**, aby wyświetlić poniższą stronę. Włącz hosta 1, ustaw adres IP 1.1.0.1 komputera jako adres IP serwera, a severity jako level\_5; kliknij **Apply**.

Rys. 3-2 Konfiguracja serwera dzienników

Log Server Config

| <input type="checkbox"/>            | Index | Server IP         | UDP Port | Severity | Status  |
|-------------------------------------|-------|-------------------|----------|----------|---------|
| <input type="checkbox"/>            |       | 1.1.0.1           |          | level_6  | Enable  |
| <input checked="" type="checkbox"/> | 1     | 1.1.0.1           | 514      | level_6  | Enable  |
| <input type="checkbox"/>            | 2     | 0.0.0.0           | 514      | level_6  | Disable |
| <input type="checkbox"/>            | 3     | 0.0.0.0           | 514      | level_6  | Disable |
| <input type="checkbox"/>            | 4     | 0.0.0.0           | 514      | level_6  | Disable |
| Total: 4                            |       | 1 entry selected. |          | Cancel   | Apply   |

2) Kliknij , aby zapisać ustawienia.

### 3.4 Przez CLI

Skonfiguruj hosta dziennika zdalnego.

```
Switch#configure
```

```
Switch(config)# logging host index 1 1.1.0.1 5
```

```
Switch(config)#end
```

```
Switch#copy running-config startup-config
```

#### Sprawdzanie konfiguracji

```
Switch# show logging loghost
```

| Index | Host-IP | Severity | Status  |
|-------|---------|----------|---------|
| ----- | -----   | -----    | -----   |
| 1     | 1.1.0.1 | 5        | enable  |
| 2     | 0.0.0.0 | 6        | disable |
| 3     | 0.0.0.0 | 6        | disable |
| 4     | 0.0.0.0 | 6        | disable |

# Część 34

## Diagnostyka urządzenia i sieci

### ROZDZIAŁY

1. Diagnostyka urządzenia
2. Diagnostyka sieci

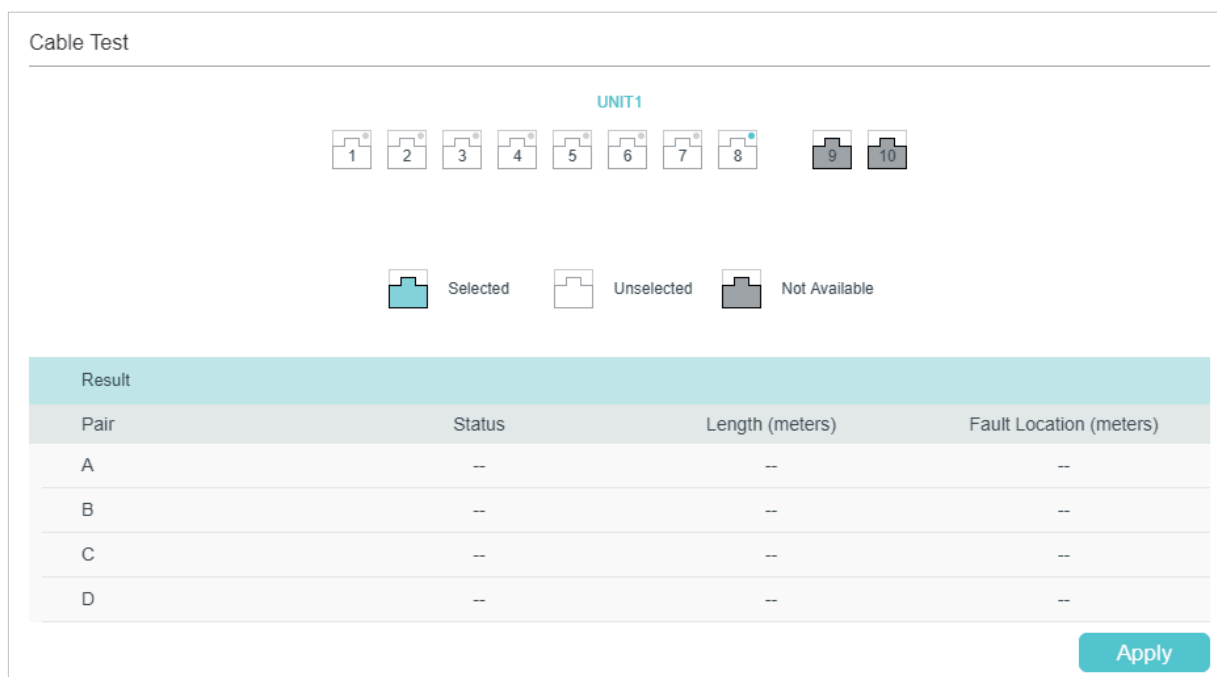
# 1 Diagnostyka urządzenia

Diagnostyka urządzenia polega na testowaniu kabli. Funkcja umożliwia rozwiązywanie problemów związanych ze stanem połączenia, długością kabla czy lokalizacją usterki.

## 1.1 Przez GUI

Wybierz z menu **MAINTENANCE > Device Diagnostics**, aby wyświetlić poniższą stronę.

Rys. 1-1 Diagnostyka kabla



Wykonaj poniższe kroki, aby sprawdzić stan kabla:

- 1) Wybierz port do przeprowadzenia testu i kliknij **Apply**.
- 2) Sprawdź wyniki testu w sekcji **Result**.

|        |                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Pair   | Informacja o numerze pary.                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Status | <p>Informacja o stanie kabla. Dostępne opcje to: normal, closed, open i crosstalk.</p> <p><b>Normal:</b> Kabel jest podłączony normalnie (standardowo).</p> <p><b>Closed:</b> Nieprawidłowy kontakt przewodów w kablu spowodował zwarcie w obwodzie.</p> <p><b>Open:</b> Do drugiego końca nie jest podłączone żadne urządzenie, co spowodowało błąd połączenia.</p> <p><b>Crosstalk:</b> Niedopasowanie rezystencji spowodowane słabą jakością kabla.</p> |

|                |                                                                                                                                              |
|----------------|----------------------------------------------------------------------------------------------------------------------------------------------|
| Length         | Jeżeli stan kabla to Normal, w tym miejscu wyświetlana jest informacja o zakresie długości kabla.                                            |
| Fault Location | Jeżeli stan kabla to Short, Close lub Crosstalk, w tym miejscu wyświetlana jest informacja o odległości między portem a lokalizacją usterki. |

## 1.2 Przez CLI

W trybie privileged EXEC, tak jak w każdym innym trybie konfiguracji, za pomocą poniższego polecenia sprawdzić można stan połączenia kabla podłączonego do przełącznika.

```
show cable-diagnostics interface { fastEthernet port | gigabitEthernet port | ten-gigabitEthernet port }
```

Wyświetl wyniki diagnostyki kabla podłączonego portu Ethernet.

*port*: Wpisz numer portu w formacie 1/0/1, aby sprawdzić wyniki testu kabla.

```
show cable-diagnostics careful interface { fastEthernet port | gigabitEthernet port | ten-gigabitEthernet port }
```

Wyświetl wyniki diagnostyki kabla podłączonego portu Ethernet. Po przeprowadzeniu szczegółowego testu kabli, przełącznik będzie testował jedynie kabel dla portu ze statusem tzw. łączy w dół.

*port*: Wpisz numer portu w formacie 1/0/1, aby sprawdzić wyniki testu kabla.

Poniższy przykład prezentuje sprawdzanie wyników diagnostyki kabla portu 1/0/2:

```
Switch#show cable-diagnostics interface gigabitEthernet 1/0/2
```

| Port    | Pair   | Status | Length      | Error |
|---------|--------|--------|-------------|-------|
| Gi1/0/2 | Pair-A | Normal | 2 (+/- 10m) | ---   |
|         | Pair-B | Normal | 2 (+/- 10m) | ---   |
|         | Pair-C | Normal | 0 (+/- 10m) | ---   |
|         | Pair-D | Normal | 2 (+/- 10m) | ---   |

# 2 Diagnostyka sieci

Funkcja diagnostyki sieci polega na testowaniu Ping i testowaniu Tracert. Możesz przeprowadzić test połączenia z hostami zdalnymi lub z bramami, od przełącznika do punktu docelowego.

Funkcja diagnostyki sieci (Network Diagnostics) umożliwia:

- rozwiązywanie problemów poprzez testy Ping;
- rozwiązywanie problemów poprzez testy Tracert.

## 2.1 Przez GUI

### 2.1.1 Rozwiązywanie problemów poprzez testy Ping

Narzędzie Ping służy do testowania połączenia ze zdalnymi hostami.

Wybierz z menu **MAINTENANCE > Network Diagnostics > Ping**, aby wyświetlić poniższą stronę.

Rys. 2-1 Rozwiązywanie problemów przez testy Ping

The screenshot displays the 'Ping Config' interface. It includes input fields for 'Destination IP' (192.168.0.26), 'Ping Times' (4), 'Data Size' (64), and 'Interval' (1000). A 'Ping' button is visible on the right. Below the configuration is a 'Ping Result' section showing the command 'Pinging 192.168.0.26 with 64 bytes of data:' followed by four successful replies with response times of 19ms and 3ms. A 'Ping statistics' section shows 4 packets sent and received with 0% loss. Finally, an 'Approximate round trip times' section shows a maximum of 19ms, a minimum of 3ms, and an average of 7ms.

| Section                      | Value                                                                                                                                                                                                                                                                |
|------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Destination IP               | 192.168.0.26                                                                                                                                                                                                                                                         |
| Ping Times                   | 4                                                                                                                                                                                                                                                                    |
| Data Size                    | 64                                                                                                                                                                                                                                                                   |
| Interval                     | 1000                                                                                                                                                                                                                                                                 |
| Ping Result                  | Pinging 192.168.0.26 with 64 bytes of data:<br>Reply from 192.168.0.26 : bytes=64 time=19ms TTL=64<br>Reply from 192.168.0.26 : bytes=64 time=3ms TTL=64<br>Reply from 192.168.0.26 : bytes=64 time=3ms TTL=64<br>Reply from 192.168.0.26 : bytes=64 time=3ms TTL=64 |
| Ping statistics              | Packets: Sent=4, Received=4, Loss=0 (0%Loss)                                                                                                                                                                                                                         |
| Approximate round trip times | Maximum=19ms, Minimum=3ms, Average=7ms                                                                                                                                                                                                                               |

Wykonaj poniższe kroki, aby sprawdzić stan połączenia między przełącznikiem a innym urządzeniem w sieci:

- 1) W sekcji **Ping Config** wpisz adres IP urządzenia docelowego w teście Ping, ustaw dowolnie wartość Ping times, rozmiar danych oraz interwał i kliknij **Ping**, aby rozpocząć test.

|                |                                                                                                                                          |
|----------------|------------------------------------------------------------------------------------------------------------------------------------------|
| Destination IP | Wpisz adres IP węzła docelowego w teście Ping. Obsługiwane są adresy IPv4 i IPv6.                                                        |
| Ping Times     | Wpisz, ile razy dane testowe będą przesłane do testowania Ping. Zaleca się zachowanie wartości domyślnej, wynoszącej 4.                  |
| Data Size      | Wpisz rozmiar danych wysłanych do testowania Ping. Zaleca się zachowanie wartości domyślnej, wynoszącej 64 bajty.                        |
| Interval       | Wyznacz odstęp czasu, w którym wysyłane będą pakiety żądania ICMP. Zaleca się zachowanie wartości domyślnej, wynoszącej 1000 milisekund. |

- 2) W sekcji **Ping Result** sprawdź wyniki testu.

## 2.1.2 Rozwiązywanie problemów poprzez testy Tracert

Narzędzie Tracert służy to lokalizacji ścieżki między przełącznikiem a punktem docelowym i testowania połączenia między przełącznikiem a routerami wzdłuż tej ścieżki.

Wybierz z menu **MAINTENANCE > Network Diagnostics > Tracert**, aby wyświetlić poniższą stronę.

Rys. 2-2 Rozwiązywanie problemów przez testy Tracert

The screenshot shows the 'Tracert Config' interface. It has two input fields: 'Destination IP' with the value '192.168.0.26' and a format note '(Format: 192.168.0.1 or 2001::1)'; and 'Maximum Hops' with the value '4' and a range note 'hops (1-30)'. A blue 'Tracert' button is on the right. Below is the 'Tracert Result' section, which displays the text 'Tracing route to [192.168.0.26] over a maximum of 4 hops' followed by a table of results:

|   |     |     |     |              |
|---|-----|-----|-----|--------------|
| 1 | 3ms | 3ms | 3ms | 192.168.0.26 |
|---|-----|-----|-----|--------------|

Wykonaj poniższe kroki, aby sprawdzić połączenie między przełącznikiem i routerami wzdłuż ścieżki od źródła do punktu docelowego:

- 1) W sekcji **Tracert Config** wpisz adres IP punktu docelowego, ustaw maks. liczbę przeskoków i kliknij **Tracert**, aby rozpocząć test.

|                |                                                                                  |
|----------------|----------------------------------------------------------------------------------|
| Destination IP | Wpisz adres IP urządzenia docelowego. Obsługiwane są IPv4 i IPv6.                |
| Maximum Hops   | Wpisz maks. liczbę przeskoków na ścieżce, przez które mogą przejść dane testowe. |



2) W sekcji **Tracert Result** sprawdź wyniki testu.

## 2.2 Przez CLI

### 2.2.1 Konfiguracja testu Ping

W trybie privileged EXEC za pomocą poniższego polecenia sprawdzić można stan połączenia między przełącznikiem a węzłem sieci.

---

```
ping [ip | ipv6] {ip_addr} [-n count] [-l size] [-i interval]
```

Przetestuj połączenie między przełącznikiem a urządzeniem docelowym.

*ip*: Wymagany typ adresu IP do testu Ping to IPv4.

*ipv6*: Wymagany typ adresu IP do testu Ping to IPv6.

*ip\_addr*: Adres IP węzła docelowego w teście Ping. Jeżeli nie ustawiono parametru ip/ipv6, obsługiwane będą zarówno adresy IPv4, jak i IPv6d (np. 192.168.0.100 lub fe80::1234).

*count*: Wyznacz, ile razy wysyłane będą dane do testu Ping. Wartość powinna wynosić od 1 do 10 razy; wartość domyślna to 4.

*size*: Wpisz rozmiar danych wysyłanych do testowania Ping. Wartość powinna wynosić między 1 a 1500 bajtów; wartość domyślna to 64 bajty

*interval*: Wyznacz odstęp czasu, w którym wysyłane będą pakiety żądania ICMP. Wartość powinna wynosić między 100 a 1000 milisekund; wartość domyślna to 1000 milisekund

---

Poniższy przykład prezentuje testowanie połączenia między przełącznikiem a urządzeniem docelowym o adresie IP 192.168.0.10, wyznaczanie wartości Ping Times na 3, rozmiaru danych na 1000 bajtów i interwału na 500 milisekund:

```
Switch#ping ip 192.168.0.10 -n 3 -l 1000 -i 500
```

Pinging 192.168.0.10 with 1000 bytes of data :

Reply from 192.168.0.10 : bytes=1000 time<16ms TTL=64

Reply from 192.168.0.10 : bytes=1000 time<16ms TTL=64

Reply from 192.168.0.10 : bytes=1000 time<16ms TTL=64

Statystyki Ping dla adresu 192.168.0.10:

Packets: Sent = 3 , Received = 3 , Lost = 0 (0% loss)

Approximate round trip times in milli-seconds:

Minimum = 0ms , Maximum = 0ms , Average = 0ms

## 2.2.2 Konfiguracja testu Tracert

W trybie privileged EXEC, za pomocą poniższego polecenia, można sprawdzić stan połączenia między przełącznikiem a routerami wzdłuż ścieżki od źródła do punktu docelowego:

---

```
tracert [ip | ipv6] ip_addr [maxHops]
```

Sprawdź połączenie bram wzdłuż ścieżki od źródła do punktu docelowego.

*ip*: Wymagany typ adresu IP do testu Tracert to IPv4.

*ipv6*: Wymagany typ adresu IP do testu Tracert to IPv6.

*ip\_addr*: Wpisz adres IP urządzenia docelowego. Jeżeli nie ustawiono parametru ip/ipv6, obsługiwane będą zarówno adresy IPv4, jak i IPv6d (np. 192.168.0.100 lub fe80::1234).

*maxHops*: Określ maks. liczbę przeskoków na ścieżce, przez które mogą przejść dane testowe, między 1 a 30; wartość domyślna to 4 przeskoki.

---

Poniższy przykład prezentuje testowanie połączenia między przełącznikiem a urządzeniem sieciowym o adresie IP 192.168.0.100. Maks. liczba przeskoków to 2:

```
Switch#tracert 192.168.0.100 2
```

```
Tracing route to 192.168.0.100 over a maximum of 2 hops
```

```
 1 8 ms 1 ms 2 ms 192.168.1.1
 2 2 ms 2 ms 2 ms 192.168.0.100
```

```
Trace complete.
```

## Uwaga do oznaczenia CE



Urządzenie jest produktem klasy A. W środowisku domowym produkt może generować zakłócenia radiowe, wymagając od użytkownika podjęcia kroków zapobiegawczych.

## Deklaracja zgodności UE

TP-Link deklaruje, że niniejsze urządzenie spełnia wszystkie kluczowe wymagania oraz jest zgodne z postanowieniami dyrektyw 2014/30/UE, 2014/35/UE, 2009/125/WE i 2011/65/UE.

Pełna deklaracja zgodności UE znajduje się na stronie <https://www.tp-link.com/pl/support/ce/>.



## Środki ostrożności

- Trzymaj urządzenie z dala od wody, ognia, wilgoci oraz wysokich temperatur.
- Nie demontuj, nie naprawiaj i nie modyfikuj urządzenia na własną rękę.
- Nie korzystaj z uszkodzonych ładowarek i kabli USB do ładowania urządzenia.

Zapoznaj się z powyższymi zasadami bezpieczeństwa i przestrzegaj ich podczas korzystania z urządzenia. Nie możemy wykluczyć ryzyka wypadku lub szkody w przypadku, gdy urządzenie użytkowane jest w sposób nieprawidłowy. Korzystaj z niniejszego produktu z ostrożnością.

## Objaśnienia symboli z etykiety produktu

| Symbol | Objaśnienie                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|        | Napięcie prądu przemiennego (AC)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|        | Urządzenie przeznaczone wyłącznie do użytku domowego                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|        | <p><b>PRAWIDŁOWE USUWANIE PRODUKTU</b></p> <p>Niniejszy produkt opatrzone symbolem klasyfikacji zużytych urządzeń elektrycznych i elektronicznych (WEEE). Oznacza to, że z urządzeniem należy obchodzić się zgodnie z dyrektywą Unii Europejskiej 2012/19/UE, czyli poddawać recyklingowi lub demontować, aby zminimalizować jego szkodliwy wpływ na środowisko.</p> <p>Użytkownik może oddać swój produkt do punktu utylizacji urządzeń elektrycznych i elektronicznych lub do punktu sprzedaży, przy okazji zakupu nowego sprzętu elektrycznego lub elektronicznego.</p> |

## PRAWA AUTORSKIE I ZNAKI TOWAROWE

Specyfikacje mogą ulec zmianie bez uprzedzenia ze strony producenta.  tp-link jest zastrzeżonym znakiem handlowym TP-Link Technologies Co., Ltd. Inne wymienione marki oraz nazwy produktów są znakami towarowymi lub zastrzeżonymi znakami handlowymi ich właścicieli.

Żadna część niniejszego podręcznika nie może być w żaden sposób reprodukowana lub powielana np. w formie tłumaczenia, przekształcenia lub adaptacji bez wyraźnej zgody TP-Link Technologies Co., Ltd. Copyright © 2018 TP-Link Technologies Co., Ltd. Wszelkie prawa zastrzeżone.

<https://www.tp-link.com/pl/>