

TP-LINK®

Instrukcja użytkownika

TD-W8960N

Bezprzewodowy router/modem ADSL2+, standard N, 300Mb/s



REV2.0.0

1910011377

PRAWA AUTORSKIE I ZNAKI HANDLOWE

Charakterystyki produktu mogą ulec zmianie bez wcześniejszego powiadomienia. **TP-LINK®** jest zarejestrowanym znakiem handlowym firmy TP-LINK TECHNOLOGIES CO., LTD. Inne wymienione marki i nazwy produktów są znakami handlowymi lub zarejestrowanymi znakami handlowymi ich odpowiednich właścicieli.

Żadna część niniejszej specyfikacji nie powinna być w jakikolwiek sposób powielana, przetwarzana, adaptowana bądź używana do uzyskiwania tekstów pochodnych, takich jak tłumaczenia bez pisemnej zgody firmy TP-LINK TECHNOLOGIES CO., LTD. Copyright © 2015 TP-LINK TECHNOLOGIES CO., LTD. Wszelkie prawa zastrzeżone.

<http://www.tp-link.com>

STANOWISKO FCC



Niniejsze urządzenie zostało przetestowane i spełnia wymogi stawiane urządzeniom cyfrowym klasy B, zgodnie z punktem 15 Reguł FCC. Obostrzenia te zostały ustanowione, by zapewnić racjonalną ochronę przeciw występowaniu szkodliwych zakłóceń w instalacji domowej. Urządzenie generuje, wykorzystuje oraz może emitować fale radiowe, co w przypadku nieprzestrzegania zaleceń niniejszej instrukcji, związanych z instalacją i użytkowaniem, może powodować zakłócenia komunikacji radiowej. Nie ma jednak całkowitej gwarancji że nie wystąpią one również w przypadku prawidłowej instalacji i obsługi. Jeżeli urządzenie jest przyczyną zakłóceń w odbiorze sygnału radiowego lub telewizyjnego, co można stwierdzić poprzez wyłączenie i ponowne włączenie, użytkownik może spróbować zminimalizować zakłócenia na następujące sposoby:

- Zmianę położenia anteny odbiorczej.
- Zwiększenie odległości pomiędzy urządzeniem a odbiornikiem.
- Podłączenie urządzenia do innego obwodu elektrycznego niż odbiornik w którym występują zakłócenia.
- Zasięgnięcie porady u sprzedawcy lub doświadczonego technika RTV.

Niniejsze urządzenie spełnia wymogi zawarte w 15. punkcie Reguł FCC. Działanie urządzenia spełnia następujące dwa warunki:

- 1) Urządzenie nie jest źródłem szkodliwych zakłóceń.
- 2) Urządzenie musi przyjmować wszystkie zakłócenia, włącznie z zakłóceniami mogącymi powodować nieprawidłowe działanie.

Wszystkie zmiany lub modyfikacje bez wyraźnego zezwolenia strony odpowiedzialnej za zgodność urządzenia mogą unieważnić pozwolenie na używanie produktu.

Uwaga: Producent urządzenia nie ponosi odpowiedzialności za jakiegokolwiek zakłócenia odbioru sygnału radiowego lub telewizyjnego spowodowane nieautoryzowanymi zmianami w urządzeniu. Tego typu zmiany mogą unieważnić pozwolenie na używanie produktu.

Stanowisko FCC dotyczące promieniowania radiowego

Niniejsze urządzenie jest zgodne z ograniczeniami i limitami dotyczącymi emisji fal radiowych w środowisku niekontrolowanym ustalonymi przez FCC. Urządzenie i jego antena nie powinny być umieszczane w bezpośrednim sąsiedztwie jakiegokolwiek innej anteny lub nadajnika.

„Aby zapewnić zgodność z wymaganiami FCC dotyczącymi promieniowania radiowego anteny używane z tym nadajnikiem muszą być umieszczone w odległości co najmniej 20 cm od najbliższej osoby i nie mogą być umieszczone w pobliżu jakiegokolwiek innej anteny lub nadajnika.”

Ostrzeżenie związane ze znakiem CE

CE 1588

Urządzenie jest produktem klasy B. W środowisku domowym może generować zakłócenia radiowe. W takim wypadku użytkownik powinien podjąć odpowiednie kroki zapobiegawcze.

Informacje dotyczące bezpieczeństwa

- Jeżeli produkt posiada wyłącznik prawidłowym sposobem wyłączenia zasilania jest użycie wyłącznika. Jeżeli produkt wyłącznika nie posiada, jedynym sposobem na jego wyłączenie jest odłączenie produktu lub jego zasilacza od prądu.
- Nie należy samodzielnie rozmontowywać produktu lub dokonywać w nim napraw. Niesie to ze sobą ryzyko porażenia elektrycznego lub utraty gwarancji. Jeżeli pomoc techniczna jest niezbędna należy kontaktować się ze wsparciem technicznym firmy TP-LINK.
- Urządzenie powinno być umieszczane w suchym miejscu, z dala od wody.

Produkt dopuszczony do użytku w następujących krajach:

AT	BG	BY	CA	CZ	DE	DK	EE
ES	FI	FR	GB	GR	HU	IE	IT
LT	LV	MT	NL	NO	PL	PT	RO
RU	SE	SK	TR	UA	US		

DEKLARACJA ZGODNOŚCI

Dla następującego urządzenia:

Opis produktu: **Bezprzewodowy router/modem ADSL2+ Standard N, 300Mb/s**

Model: **TD-W8960N**

Znak handlowy: **TP-LINK**

Deklarujemy na własną odpowiedzialność, że powyższe produkty spełniają wszystkie wymagania techniczne właściwe dla produktów będących w zakresach Dyrektyw Rady:

Dyrektywa 1999/5/EC, Dyrektywa 2004/108/EC, Dyrektywa 2006/95/EC, Dyrektywa 1999/519/EC, Dyrektywa 2011/65/EU

Powyższy produkt jest zgodny z następującymi standardami i dokumentami normatywnymi

EN 300 328 V1.8.1

EN 301 489-1 V1.9.2 & EN 301 489-17 V2.2.1

EN 55022: 2010 + AC: 2011

EN 55024: 2010

EN 60950-1: 2006 + A11: 2009 + A1: 2010 + A12: 2011 +A2: 2013

EN 50385: 2002

Produkt nosi oznaczenie CE:

CE 1588

Osoba odpowiedzialna za sporządzenie tej deklaracji:



Yang Hongliang

Product Manager of International Business

Data wystawienia: 2015-08-10

TP-LINK TECHNOLOGIES CO., LTD

Building 24 (floors 1, 3, 4, 5), and 28 (floors 1-4) Central Science and Technology Park,
Shennan Rd, Nanshan, Shenzhen, China

SPIS TREŚCI

Zawartość opakowania.....	1
Rozdział 1. Wstęp.....	2
1.1 Informacje ogólne	2
1.2 Główne cechy	3
1.3 Wygląd urządzenia	3
1.3.1 Panel przedni	3
1.3.2 Panel tylny	4
Rozdział 2. Podłączanie routera.....	6
2.1 Wymagania systemowe.....	6
2.2 Środowisko instalacji	6
2.3 Podłączanie routera.....	7
Rozdział 3. Instrukcja szybkiej instalacji.....	8
3.1 Konfiguracja TCP/IP	8
3.2 Instrukcja szybkiej instalacji.....	9
Rozdział 4. Konfigurowanie routera	13
4.1 Logowanie.....	13
4.2 Informacje.....	13
4.3 Szybka konfiguracja	14
4.4 Ustawienia zaawansowane	14
4.4.1 Interfejs warstwy 2	15
4.4.2 Usługi WAN.....	18
4.4.3 Klonowanie MAC	27
4.4.4 LAN	28
4.4.5 NAT	31
4.4.6 Bezpieczeństwo	36
4.4.7 Kontrola rodzicielska.....	39
4.4.8 Quality of Service.....	41
4.4.9 Kontrola przepustowości.....	44
4.4.10 Routing.....	46
4.4.11 DNS	48
4.4.12 DSL	51

4.4.13 UPnP.....	51
4.4.14 Grupowanie interfejsów	52
4.4.15 Tunel IP.....	53
4.4.16 IPSec	55
4.4.17 Multicast.....	58
4.5 Sieć bezprzewodowa.....	58
4.5.1 Podstawowe.....	59
4.5.2 Zabezpieczenia.....	60
4.5.3 Harmonogram.....	71
4.5.4 Filtrowanie MAC.....	72
4.5.5 Połączenie Bridge.....	73
4.5.6 Zaawansowane.....	74
4.5.7 Podłączone urządzenia	75
4.6 Sieć dla gości	76
4.6.1 Podstawowe.....	76
4.6.2 Podłączone urządzenia	77
4.7 Diagnostyka.....	78
4.8 Zarządzanie.....	78
4.8.1 Ustawienia	78
4.8.2 Dziennik systemowy	81
4.8.3 Agent SNMP	82
4.8.4 Klient TR-069	84
4.8.5 Pobieranie czasu	85
4.8.6 Kontrola dostępu.....	85
4.8.7 Aktualizacja oprogramowania.....	87
4.8.8 Restart	87
4.9 Wyloguj	88
Dodatek A: Specyfikacja	89
Dodatek B: Konfiguracja komputerów.....	90
Dodatek C: Rozwiązywanie problemów.....	94
Dodatek D: Wsparcie techniczne	96

Zawartość opakowania

W opakowaniu powinny znajdować się następujące przedmioty:

- Jeden bezprzewodowy router/modem ADSL2+ Standard N, 300Mb/s
- Jeden zasilacz bezprzewodowego routera/modemu ADSL2+ Standard N, 300Mb/s
- Instrukcja szybkiej instalacji
- Jeden kabel RJ45
- Dwa kable RJ11 (Telefoniczne/ADSL)
- Jeden splitter ADSL
- Jedna płyta CD, zawierająca:
 - Niniejszą instrukcję
 - Inne użyteczne informacje

Uwaga:

Upewnij się, że opakowanie zawiera wszystkie przedmioty wymienione powyżej. W przypadku jakichkolwiek braków lub uszkodzeń, skontaktuj się z dystrybutorem.

Rozdział 1. Wstęp

Dziękujemy za wybranie bezprzewodowego routera/modemu ADSL2+ 300Mb/s TD-W8960N.

1.1 Informacje ogólne

Bezprzewodowy router/modem ADSL2+ Standard N, 300Mb/s TD-W8960N łączy w sobie funkcje 4-portowego przełącznika, zapory Firewall, routera NAT oraz bezprzewodowego punktu dostępowego. Dzięki technologii MIMO 2x2, MIMO router umożliwia korzystanie z sieci bezprzewodowej o dużej prędkości i zasięgu, odpowiedniej dla najbardziej wymagających zastosowań w domu lub małym biurze.

Router TD-W8960N wyposażony jest we wbudowany modem ADSL2+ i wydajny procesor. Urządzenie obsługuje pełen zakres połączeń ADSL2+, zgodnie ze standardami ITU oraz ANSI.

Poza podstawowymi funkcjami warstwy fizycznej DMT, ADSL2+ PHY wspiera dwie prędkości przesyłania ramek (szybką i z przepłotem) oraz standard warstwy fizycznej ATM I.432.

Router zapewnia połączenia z urządzeniami bezprzewodowymi w standardzie 802.11n z prędkością do 300Mb/s. Wysoka prędkość połączeń umożliwia wielostrumieniowy transfer danych, gwarantując stabilność i płynne działanie sieci. Router jest również kompatybilny z urządzeniami działającymi w standardach IEEE 802.11g oraz IEEE 802.11b.

Router wyposażony jest w wiele funkcji zabezpieczających, takich jak możliwość wyłączenia rozgłaszania nazwy sieci bezprzewodowej, szyfrowanie WEP(64/128-bit) i Wi-Fi protected Access (WPA2-PSK, WPA-PSK) oraz zaawansowana ochrona Firewall. Zapewnia to użytkownikowi sieci wysoki poziom bezpieczeństwa danych.

Router wyposażony jest w funkcję kontroli dostępu, pozwalającą rodzicom lub administratorom na ograniczenie dzieciom lub pracownikom dostępu do zasobów sieci. Obsługuje również takie funkcje jak Serwery Wirtualne, Host DMZ oraz Port Triggering, umożliwiające zdalne łączenie się z urządzeniami w sieci lokalnej, a także funkcję zdalnego zarządzania, umożliwiającą monitorowanie oraz zmiany konfiguracji routera od strony WAN.

Router jest kompatybilny ze wszystkimi głównymi systemami operacyjnymi i łatwy w zarządzaniu. Zawarta na stronie konfiguracyjnej routera i dokładnie opisana w tej instrukcji funkcja Szybkiej Konfiguracji, umożliwia łatwe skonfigurowanie podstawowych funkcji routera. Przed instalacją tego routera zaleca się zapoznanie z jego funkcjami, opisanymi w niniejszej instrukcji.

1.2 Wygląd urządzenia

1.2.1 Panel przedni

Diody sygnalizujące status routera, umieszczone są na jego przednim panelu.



Rysunek 1-1

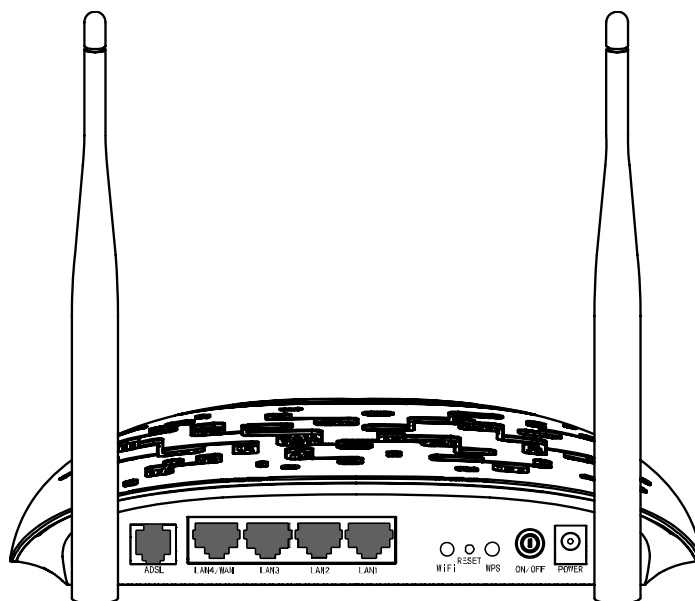
Opis diod:

Nazwa	Status	Wskazanie
⏻(Zasilanie)	Świeci	Router jest włączony.
	Nie świeci	Router jest wyłączony. Upewnij się, że zasilacz urządzenia jest prawidłowo podłączony.
⚡(ADSL)	Świeci	Linia ADSL jest zsynchronizowana i gotowa do użycia.
	Miga	Trwa synchronizacja ADSL.
	Nie świeci	Nieudana synchronizacja. Aby rozwiązać problem, patrz punkt Uwaga 1 .
🌐(Internet)	Świeci	Urządzenie ma połączenie z Internetem.
	Miga	Urządzenie przesyła lub odbiera dane z Internetu.
	Nie świeci	Brak połączenia z Internetem lub router pracuje w trybie Bridge. Aby rozwiązać problem, patrz punkt Uwaga 2 .
📶(WLAN)	Miga	Sieć bezprzewodowa jest włączona.
	Nie świeci	Sieć bezprzewodowa jest wyłączona.
🔒(WPS)	Świeci	Urządzenie połączyło się z siecią dzięki funkcji WDS.
	Miga powoli	Nawiązywanie połączenia WPS jest w toku i może potrwać do 2 minut. Zanim dioda przestanie migać naciśnij przycisk WPS na urządzeniu, które ma być podłączone do sieci.
	Miga szybko	Nie udało się połączyć urządzenia WPS w ciągu 2 minut. Więcej informacji w punkcie 4.5.2.1 Ustawienia WPS
📡(LAN1-4)	Świeci	Do danego portu LAN podłączone jest urządzenie.
	Miga	Router wysyła lub odbiera dane przez dany port LAN.
	Nie świeci	Żadne urządzenie nie jest podłączone do danego portu LAN.

☞ Uwaga:

1. Jeżeli dioda ADSL się nie świeci, sprawdź połączenie routera z gniazdem ADSL. Sposób prawidłowego podłączania routera opisany jest w punkcie [2.3 Podłączanie routera](#). Jeżeli router podłączony jest prawidłowo, skontaktuj się z dostawcą Internetu aby upewnić się czy usługa jest aktualnie dostępna.
2. Jeżeli dioda Internet się nie świeci sprawdź diodę ADSL. Jeżeli dioda ADSL również się nie świeci wróć do punktu **Uwaga 1**. Jeżeli dioda ADSL świeci ciągłym światłem, sprawdź konfigurację połączenia z Internetem. Aby potwierdzić prawidłowe parametry połączenia, skontaktuj się z dostawcą Internetu. Następnie upewnij się, że parametry zostały wprowadzone prawidłowo. Więcej informacji znajduje się w punkcie [4.2 Informacje](#).

1.2.2 Panel tylny



Rysunek 1-2

- **ADSL** : Port służący do podłączania routera do linii telefonicznej lub splitera.
- **LAN4/WAN, LAN3, LAN2, LAN1**: Porty służące do podłączania komputerów oraz innych urządzeń Ethernet. Po włączeniu funkcji EWAN można podłączyć port LAN4/WAN do modemu Kablowego/FTTH/VDSL/ADSL.
- **WiFi**: Przycisk służący do włączania/wyłączania sieci bezprzewodowej.
- **RESET**: Przycisk służący do przywracania ustawień fabrycznych. Istnieją dwa sposoby:
 - 1) Użycie przycisku **Przywróć ustawienia fabryczne** w menu **Zarządzanie** -> **Ustawienia** -> **Przywróć domyślne** na stronie zarządzania routerem.
 - 2) Użycie przycisku **RESET**: Podłącz router do zasilania. Za pomocą wąskiego przedmiotu, naciśnij znajdujący się w otworze **RESET** przycisk i przytrzymaj go przez co najmniej 10 sekund. Router zostanie zrestartowany, a ustawienia powrócą do ustawień fabrycznych.
- **WPS**: Przycisk WPS. Szczegółowy opis znajduje się w punkcie [4.5.2.1 Ustawienia WPS](#).
- **WYŁĄCZNIK (ON/OFF)**: Wyłącznik zasilania.
- **ZASILANIE (POWER)**: Gniazdo zasilania – podłącza się do niego zasilacz urządzenia.
- **Anteny**: Używane do transmisji bezprzewodowej.

1.3 Główne cechy

- Zgodność ze standardem IEEE 802.11n, prędkość połączeń bezprzewodowych do 300Mb/s
- Jeden port RJ11, cztery porty RJ45 10/100Mb/s (autonegocjacja, auto MDI/MDIX)
- Szybko reagujący, skuteczny obwód zabezpieczenia przeciwprzepięciowego
- Przetwornik analogowy obsługujący połączenia Annex A oraz Annex L
- Zewnętrzny splitter sygnału
- Udostępnianie szybkiego połączenia internetowego wielu użytkownikom
- Możliwość nawiązywania połączenia na żądanie i automatycznego rozłączania dla połączeń PPPoE
- Obsługa zabezpieczeń WPA/WPA2, WPA-PSK/WPA2-PSK z szyfrowaniem TKIP/AES
- Obsługa zabezpieczeń WEP 64/128-bit WEP oraz list kontroli dostępu ACL
- Obsługa zaawansowanej technologii modulacji i demodulacji DMT
- Funkcja kontroli dostępu, pozwalająca rodzicom lub administratorom na ograniczenie dzieciom lub pracownikom dostępu do zasobów sieci.
- Obsługa funkcji Serwery Wirtualne, Port Triggering oraz Host DMZ
- Obsługa funkcji UPnP, Dynamiczny DNS, Routing Statyczny
- Praca w trybie routera NAT, możliwość nawiązania połączenia typu Bridge
- Zarządzanie przez przeglądarkę internetową
- Możliwość aktualizacji firmware
- Statystyki przepływu danych
- Wbudowany firewall, obsługujący filtrowanie adresów IP, MAC oraz funkcję kontroli rodzicielskiej
- Wbudowany serwer DHCP
- Obsługa IPv6
- Sieć bezprzewodowa dla gości
- Obsługa połączeń WPS

Rozdział 2. Podłączanie routera

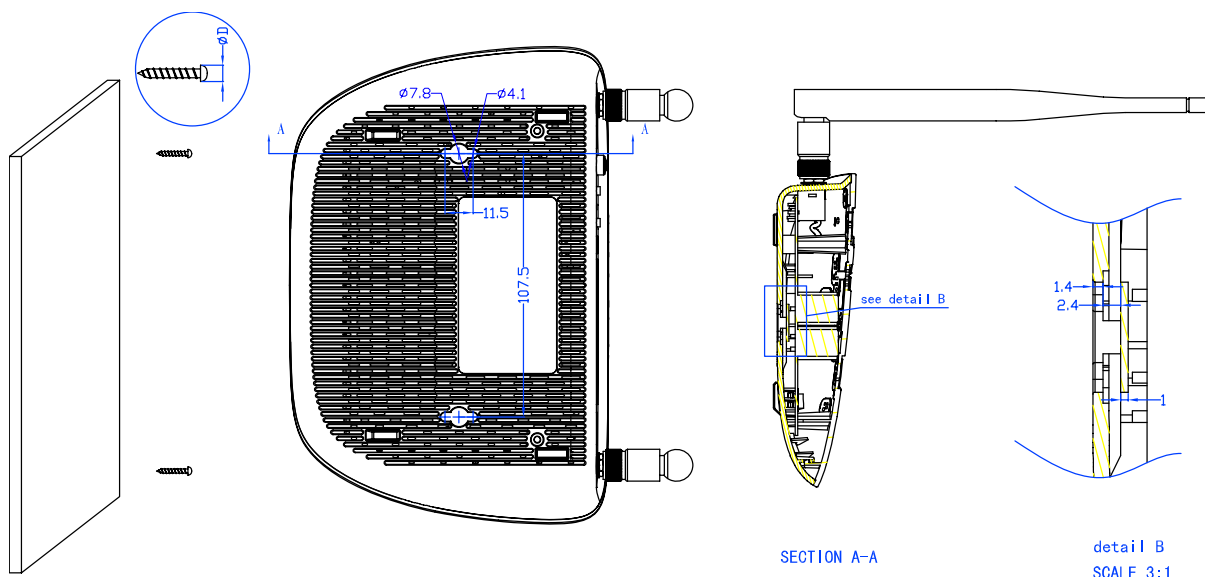
2.1 Wymagania systemowe

- Szerokopasmowe połączenie z Internetem (ADSL/Kablowe/Ethernet).
- Komputer z działającą kartą Ethernet oraz kabel Ethernet z wtyczką RJ45.
- Włączona obsługa protokołu TCP/IP na każdym podłączonym urządzeniu.
- Przeglądarka internetowa, np. Microsoft Internet Explorer, Mozilla Firefox lub Apple Safari.

2.2 Środowisko instalacji

- Produkt nie powinien być narażony na dużą wilgotność i wysokie temperatury.
- Router należy umieścić w miejscu umożliwiającym podłączenie go do innych urządzeń oraz do źródła zasilania.
- Kable oraz zasilacz należy umieścić tak, by wyeliminować niebezpieczeństwo potknięcia.
- Router może być umieszczony na półce lub na biurku.
- Urządzenie należy umieszczać z dala od źródeł promieniowania elektromagnetycznego oraz urządzeń wrażliwych na tego typu promieniowanie.

Urządzenie TD-W8960N umieszczane jest najczęściej na płaskich, poziomych powierzchniach. Może jednak być również zamontowane na ścianie, tak jak pokazano to na Rysunku 2-1.



Rysunek 2-1 Instalacja na ścianie

Uwaga:

Należy używać wkrętów o promieniu $4,1\text{mm} < D < 7,8\text{mm}$, odległość pomiędzy wkrętami: 107,5mm. Odległość łebka od ściany powinna wynosić ok. 4mm, a długość wkrętów co najmniej 20mm.

2.3 Podłączanie routera

Przed instalacją urządzenia upewnij się, że połączenie z siecią jest dostępne. W przypadku jakichkolwiek problemów, skontaktuj się z dostawcą Internetu. Kable należy podłączać suchymi rękami, przy odłączonym zasilaniu. Instalując router postępuj według poniższych kroków:

1) Podłącz kabel ADSL.

a) **Sposób pierwszy:** Podłącz jeden z końców kabla ADSL do portu ADSL na tylnym panelu routera TD-W8960N, a drugi koniec do gniazdka w ścianie.

b) **Sposób drugi:** Możesz zastosować Splitter rozdzielający transmisję danych od transmisji głosu. Dzięki temu można jednocześnie prowadzić rozmowy telefoniczne i korzystać z Internetu. Splitter posiada 3 porty:

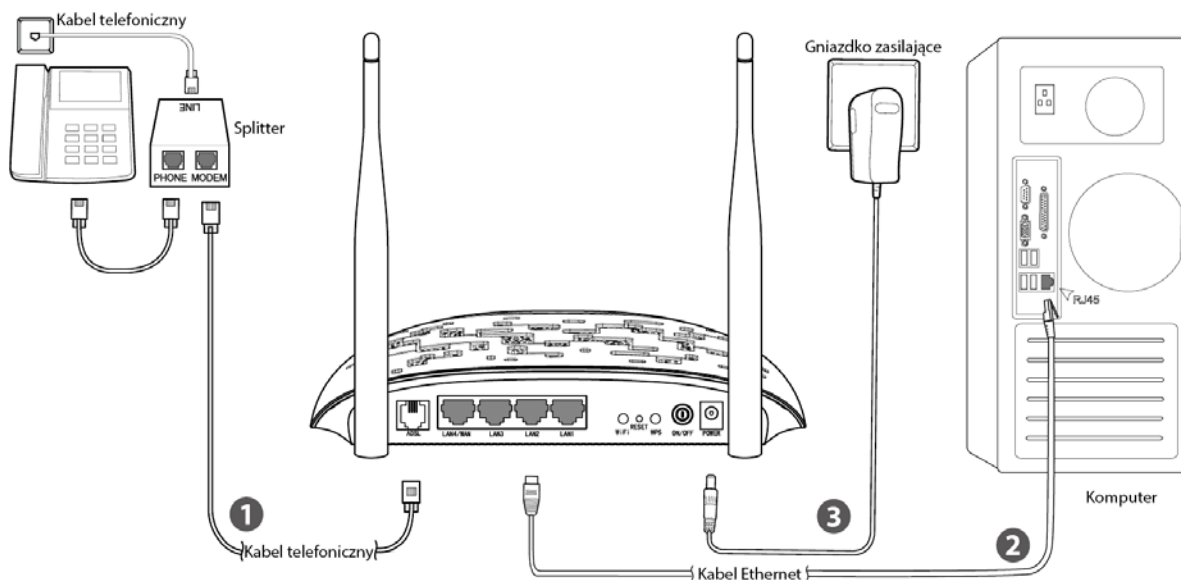
- LINIA (LINE): Podłączany do gniazda telefonicznego w ścianie
- TELEFON (PHONE): Podłączany do telefonu
- MODEM: Podłączany do portu ADSL routera

Podłącz jeden koniec kabla ADSL do portu ADSL na tylnym panelu TD-W8960N. Drugi koniec kabla podłącz do portu MODEM na splitterze.

2) Podłącz jeden koniec kabla Ethernet do portu Ethernet w komputerze, a drugi koniec kabla do jednego z portów LAN routera. Podłącz pozostałe urządzenia jeśli to konieczne.

3) Włącz komputery i inne urządzenia sieciowe.

4) Podłącz zasilacz routera do gniazda zasilania na tylnym panelu routera, a następnie do gniazda zasilającego. Gniazdo elektryczne powinno znajdować się w pobliżu routera i być łatwo dostępne.



Rysunek 2-2

Rozdział 3. Instrukcja szybkiej instalacji

Rozdział ten zawiera opis szybkiej konfiguracji routera TD-W8960N za pomocą narzędzia **Szybka konfiguracja**.

3.1 Konfiguracja TCP/IP

Domyślny adres IP routera TD-W8960N to 192.168.1.1, a domyślna maska podsieci to 255.255.255.0. Wartości te mogą być dowolnie zmieniane. W niniejszej instrukcji stosowane są wartości domyślne.

Podłącz komputer do portu LAN routera. Twój komputer powinien automatycznie uzyskać adres IP z serwera DHCP routera. Jeżeli komputer nie uzyska adresu IP:

- 1) Skonfiguruj protokół TCP/IP wybierając opcję „**Uzyskaj adres IP automatycznie**”. Dokładna instrukcja postępowania znajduje się w sekcji [Dodatek B: „Konfiguracja komputera PC”](#).
- 2) Po udanej konfiguracji komputer otrzyma adres IP od serwera DHCP routera.

Teraz możesz użyć komendy Ping, aby sprawdzić połączenie sieciowe. Naciśnij przycisk **Start**, wybierz opcję **uruchom**, w pustym polu wpisz **cmd** i naciśnij **Enter**. W kolejnym oknie wpisz **ping 192.168.1.1** i naciśnij **Enter**.

Jeżeli wynik komendy jest podobny do pokazanego na poniższym rysunku, połączenie między routerem a twoim komputerem zostało nawiązane.

```
C:\Users\tplink>ping 192.168.1.1

Badanie 192.168.1.1 z 32 bajtami danych:
Odpowiedź z 192.168.1.1: bajtów=32 czas=4ms TTL=254
Odpowiedź z 192.168.1.1: bajtów=32 czas=1ms TTL=254
Odpowiedź z 192.168.1.1: bajtów=32 czas=1ms TTL=254
Odpowiedź z 192.168.1.1: bajtów=32 czas=1ms TTL=254

Statystyka badania ping dla 192.168.1.1:
    Pakiety: Wysłane = 4, Odebrane = 4, Utracone = 0
             (0% straty),
Szacunkowy czas błędzenia pakietów w milisekundach:
    Minimum = 1 ms, Maksimum = 4 ms, Czas średni = 1 ms
```

Rysunek 3-1

Jeżeli wynik komendy jest podobny do pokazanego na poniższym rysunku, oznacza to, że między twoim komputerem a routerem nie zostało nawiązane połączenie.

```
C:\Users\tplink>ping 192.168.1.1

Badanie 192.168.1.1 z 32 bajtami danych:
Upłynął limit czasu żądania.
Upłynął limit czasu żądania.
Upłynął limit czasu żądania.
Upłynął limit czasu żądania.

Statystyka badania ping dla 192.168.1.1:
    Pakiety: Wysłane = 4, Odebrane = 0, Utracone = 4
             (100% straty),
```

Rysunek 3-2

Przyczynę problemu możesz sprawdzić według poniższych kroków:

1) Czy połączenie między komputerem a routerem jest prawidłowe?

Dioda portu LAN na routerze i dioda portu Ethernet komputera powinny się świecić.

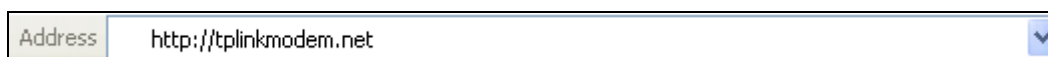
2) Czy konfiguracja TCP/IP komputera jest prawidłowa?

Jeżeli adres IP routera to 192.168.1.1, adres IP twojego komputera powinien być adresem z zakresu 192.168.1.2~192.168.1.254.

3.2 Instrukcja szybkiej instalacji

Dzięki narzędziu szybkiej konfiguracji można łatwo przeprowadzić wstępną konfigurację routera TD-W8960N. Z narzędzia można skorzystać używając dowolnego komputera z systemem Windows, MacOS lub UNIX wyposażonego w przeglądarkę internetową, taką jak np. Microsoft Internet Explorer, Mozilla Firefox lub Apple Safari.

1. Aby uzyskać dostęp do strony konfiguracyjnej routera otwórz przeglądarkę internetową, wprowadź <http://tplinkmodem.net/> w pasek adresu i naciśnij Enter.



Rysunek 3-3

Po kilku sekundach pojawi się okno logowania, pokazane na Rysunku 3-4. Wprowadź domyślną nazwę użytkownika – **admin**, oraz domyślne hasło - **admin**. Następnie naciśnij przycisk **Zaloguj** lub klawisz **Enter**.



Rysunek 3-4

Uwaga:

- 1) Nazwa użytkownika i hasło logowania do strony konfiguracyjnej routera są inne niż nazwa użytkownika i hasło konta ADSL używanego do konfiguracji połączenia z Internetem.
- 2) Jeżeli powyższe okno nie zostanie wyświetlone, może to oznaczać, że komputer skonfigurowany jest do korzystania z serwera proxy. Jeżeli korzystasz z przeglądarki Internet Explorer, otwórz menu **Narzędzia** i wybierz **Opcje internetowe** → **Połączenia** → **Ustawienia sieci LAN**, odznacz opcję Używaj serwera proxy i naciśnij przycisk **OK**.

2. Po udanym zalogowaniu pojawi się okno pokazane na Rysunku 3-5. Wybierz opcję **Szybka konfiguracja**, aby uruchomić narzędzie szybkiej konfiguracji routera.

Informacje o urządzeniu

Wersje

Wersja Firmware:	1.1.1 Build 150623 Rel.57081
Wersja sprzętowa:	TD-W8960N V6 0x00000001
Czas działania systemu:	0 Dni 00:36:36

Informacje o sieci LAN

IPv4	Adres LAN IP:	192.168.1.1
	Adres MAC LAN:	02:10:18:01:00:01
IPv6	Adres/długość prefiksu IPV6:	NULL
	Autokonfiguracja:	RADVD&DHCPv6

Informacje o sieci ADSL

Stan linii:	Brak połączenia
Prędkość linii – Wysyłanie (Kb/s):	0
Prędkość linii – Pobieranie (Kb/s):	0

Informacje o połączeniu z Internetem

Uwaga:	Aktualnie żaden interfejs nie jest skonfigurowany.
Skrót:	Kliknij tutaj aby przejść przez proces Szybkiej konfiguracji. Kliknij tutaj aby wyświetlić status interfejsów WAN i informacje o rozwiązywaniu problemów.

Rysunek 3-5

3. Wybierz **Typ połączenia z Internetem** i naciśnij przycisk „Dalej”.

Szybka konfiguracja - konfiguracja WAN

Wybierz typ połączenia z Internetem.

Wybierz typ połączenia WAN:

ADSL WAN Połączenie ADSL (linia telefoniczna RJ11)

Ethernet WAN Połączenie kablem Ethernet (RJ45)

Włącz IPv6 dla tego połączenia

Rysunek 3-6

 **Uwaga:**

- Po naciśnięciu przycisku „Dalej” przejdziesz do konfiguracji parametrów połączenia WAN.
- Jeżeli nie chcesz teraz konfigurować połączenia WAN, wybierz opcję **Pomiń WAN**. Połączenie WAN można skonfigurować później według punktu [4.4.1 Interfejs warstwy 2](#).

4. Po wybraniu połączenia ADSL WAN należy wybrać **Kraj** oraz **Dostawcę Internetu**. Upewnij się, że **Typ połączenia WAN** oraz pozostałe parametry są zgodne z zaleceniami dostawcy Internetu i naciśnij przycisk „Dalej”. Na przykładzie pokazane jest połączenie PPPoE.

Szybka konfiguracja - ustawienia WAN

Kraj: POLSKA ▾
Dostawca Internetu: Dialog (PPPoE) ▾
VPI/VCI: 0 / 35 ([0-255] / [32-65535])
Tryb enkapsulacji: LLC/SNAP-BRIDGING ▾ (opcjonalnie)

Typ łącza WAN: PPPoE ▾
Nazwa użytkownika PPP:
Hasło PPP:
Nazwa usługi PPPoE: (opcjonalnie)
MTU (bajtów): 1480 (opcjonalnie)

Rysunek 3-7

 **Uwaga:**

Jeżeli twój dostawca Internetu nie jest wymieniony na liście, wybierz opcję Inne. Następnie ręcznie wprowadź parametry połączenia, takie jak VPI/VCI, tryb enkapsulacji oraz **Typ łącza WAN**, zgodnie z zaleceniami dostawcy Internetu.

Po wybraniu połączenia Ethernet WAN należy wybrać **Typ łącza WAN** oraz wprowadzić odpowiednie parametry, zgodnie z zaleceniami dostawcy Internetu, a następnie nacisnąć przycisk „Dalej”. Na przykładzie pokazane jest połączenie PPPoE.

Szybka konfiguracja - ustawienia WAN

Port Ethernet WAN: LAN4/WAN

Typ łącza WAN: PPPoE ▾
Nazwa użytkownika PPP:
Hasło PPP:
Nazwa usługi PPPoE: (opcjonalnie)
MTU (bajtów): 1480 (opcjonalnie)

Rysunek 3-8

5. Kolejny ekran umożliwi konfigurację sieci bezprzewodowej. Domyślnie sieć bezprzewodowa jest włączona. Możesz nadać sieci nową nazwę, wybrać typ zabezpieczeń i utworzyć własne hasło. Domyślna nazwa sieci bezprzewodowej to TP-LINK_XXXXXX, a domyślne hasło, takie samo jak kod PIN, znajduje się na naklejce u spodu routera. Aby kontynuować, naciśnij przycisk „Dalej”.

Szybka konfiguracja -- Sieć bezprzewodowa

Włącz sieć bezprzewodową:

Możesz skonfigurować nazwę sieci oraz typ uwierzytelniania.

Nazwa sieci bezprzewodowej: (Nazywana też SSID)

Aby zabezpieczyć sieć przed niepożądanymi użytkownikami zalecane jest wybranie jednego z następujących typów zabezpieczeń.

Typ uwierzytelniania:

Hasło WPA: (Nazywane też kluczem sieciowym)
(Możesz wprowadzić od 8 do 63 znaków ASCII lub 64 znaków szesnastkowych.)

Rysunek 3-9

6. Wyświetlony zostanie ekran **Podsumowanie**. Naciśnij przycisk „Potwierdź”, aby zatwierdzić wprowadzone ustawienia.

Szybka konfiguracja - Podsumowanie

Konfiguracja WAN

Typ połączenia WAN:	ADSL WAN
Informacje o Warstwie 2:	0/35 LLC/SNAP-BRIDGING
Typ połączenia WAN:	PPPoE
Nazwa użytkownika PPP:	1234567890
Hasło PPP:	1234567890
MTU PPP:	1480

Uwaga1: Niektóre połączenia WAN lub interfejsy Warstwy 2 mogą zostać zastąpione!

Uwaga2: Ustawienia Serwerów wirtualnych dla niektórych interfejsów WAN mogą zostać usunięte!

Konfiguracja Wi-Fi

Nazwa sieci bezprzewodowej:	TP-LINK_0001
Uwierzytelnianie:	WPA2-Personal
Hasło sieci bezprzewodowej:	76229909

Rysunek 3-10

Rozdział 4. Konfigurowanie routera

W rozdziale tym omówione są poszczególne strony menu konfiguracji routera.

4.1 Logowanie

Po udanym zalogowaniu, po lewej stronie, widoczne będzie menu zawierające 8 pozycji. Po prawej stronie widoczne będą informacje i instrukcje, odpowiadające aktualnie wybranej opcji.

Informacje
Szybka konfiguracja
Ustawienia zaawansowane
Sieć bezprzewodowa
Sieć dla gości
Diagnostyka
Zarządzanie
Wyloguj

Dalsza część rozdziału zawiera opis poszczególnych funkcji z menu.

4.2 Informacje

Po wybraniu opcji „**Informacje**”, wyświetlone zostanie 6 dodatkowych pozycji: **Podsumowanie**, **WAN**, **Statystyki**, **Routing**, **ARP** oraz **DHCP**. Zawierają one informacje dotyczące aktualnych ustawień routera oraz parametrów połączenia.

Po wybraniu opcji „**Informacje**”→„**Podsumowanie**” wyświetlony zostanie ekran Podsumowania (pokazany na Rysunku 4-1). Pierwsza tabela zawiera informacje na temat wersji firmware oraz wersji sprzętowej routera. Pozostałe tabele zawierają informacje o połączeniu. Od ustawień routera, wprowadzonych z użyciem narzędzia Szybkiej konfiguracji lub w menu Ustawienia zaawansowane, zależy jakie tabele wyświetlane będą na tej stronie.

Informacje o urządzeniu		
Wersje		
Wersja Firmware:	1.1.1 Build 141013 Rel.41664	
Wersja sprzętowa:	TD-W8960N V5 0x00000001	
Czas działania systemu:	0 Dni 00:09:42	
Informacje o sieci LAN		
IPv4	Adres LAN IP:	192.168.1.1
	Adres MAC LAN:	02:10:18:01:00:01
IPv6	Adres/długość prefiksu IPV6:	NULL
	Autokonfiguracja:	RADVD&DHCPv6
Informacje o sieci ADSL		
Stan linii:	Brak połączenia	
Prędkość linii – Wysyłanie (Kb/s):	0	
Prędkość linii – Pobieranie (Kb/s):	0	
Informacje o połączeniu z Internetem		
IPv4	Status:	Niepołączony
	Typ WAN:	ATM WAN
	Interfejs warstwy 2:	atm0(0/35)
	Typ połączenia:	PPPoE
	Adres WAN IP:	0.0.0.0
	Skrót:	Kliknij tutaj aby wyświetlić status interfejsów WAN i informacje o rozwiązywaniu problemów.

Rysunek 4-1

Uwaga:

Po wybraniu pozostałych opcji z menu **Informacje**, wyświetlone zostaną informacje dotyczące połączenia **WAN**, **Statystyk połączeń**, **Routingu**, **ARP** oraz **DHCP**.

4.3 Szybka konfiguracja

Działanie menu **Szybka konfiguracja** opisane jest w sekcji [3.2 Instrukcja szybkiej instalacji](#).

4.4 Ustawienia zaawansowane

Po wybraniu opcji „**Ustawienia zaawansowane**” wyświetlone zostanie menu zawierające wiele pozycji. **Interfejs warstwy 2**, **Usługi WAN**, **LAN** są widoczne zawsze, a inne pozycje wyświetlane są w zależności od skonfigurowanych wcześniej funkcji. Wybranie jednej z opcji powoduje przejście do ekranu konfiguracji, odpowiadającej jej funkcji.

Ustawienia zaawansowane
+ Interfejs warstwy 2
+ Usługi WAN
+ Klonowanie MAC
+ LAN
+ NAT
+ Bezpieczeństwo
+ Kontrola rodzicielska
+ Quality of Service
+ Kontrola przepustowości
+ Routing
+ DNS
+ DSL
+ UPnP
+ Grupowanie interfejsów
+ Tunel IP
+ IPsec
+ Multicast

Poniżej znajduje się dokładny opis konfiguracji poszczególnych, zaawansowanych funkcji routera.

Uwaga:

Aby skonfigurować wszystkie parametry połączenia WAN routera należy najpierw wybrać parametry Interfejsu warstwy drugiej ([4.4.1 Interfejs warstwy 2](#)), zgodnie z posiadanym łączem internetowym, a następnie skonfigurować pozostałe parametry WAN ([4.4.2 Usługi WAN](#)).

4.4.1 Interfejs warstwy 2

Po wybraniu opcji „Ustawienia zaawansowane” → „Interfejs warstwy 2” możesz wybrać interfejs dla usług WAN (interfejs warstwy drugiej) – **Interfejs ATM** lub **Interfejs ETH**.

- **Interfejs ATM:** Służy do korzystania z połączenia ADSL. W przypadku takiego połączenia dostawca Internetu zapewnia ustawienia VPI (Virtual Path Identifier), VCI (Virtual Channel Identifier) oraz interfejs DSL z gniazdem RJ11. (Rysunek 4-2)
- **Interfejs ETH:** Służy do korzystania z połączenia Ethernet. W przypadku takiego połączenia dostawca Internetu zapewnia szerokopasmowe łącze internetowe z gniazdem RJ45.

4.4.1.1 Interfejs ATM

Po wybraniu opcji „Ustawienia zaawansowane” → „Interfejs warstwy 2” → „Interfejs ATM” pojawi się okno konfiguracji interfejsu ATM, pokazane poniżej.

Konfiguracja interfejsu DSL ATM

Wybierz Dodaj lub Usuń aby skonfigurować interfejs DSL ATM.

Interfejs	Vpi	Vci	Typ łącza	Enkapsulacja	Kategoria	Maksymalna prędkość transmisji komórek	Średnia prędkość transmisji komórek	Maks. Rozmiar Paczki	Tryb połączenia	IP QoS	Algorytm	Waga kolejki	Pierwszeństwo grupy	Usuń
atm0	0	35	EoA	LLC	UBR				Tryb VLANMux	Włączone	WRR	1	8	<input type="checkbox"/>

Rysunek 4-2

- **Usuń:** Zaznacz opcję w kolumnie Usuń, a następnie naciśnij przycisk „**Usuń**”. Odpowiedni interfejs zostanie usunięty z tabeli.

 **Uwaga:**

Jeżeli interfejs został skonfigurowany do użycia, zgodnie z punktem [4.4.2 Usługi WAN](#), przed usunięciem interfejsu należy najpierw usunąć odpowiadającą mu usługę WAN.

- **Dodaj:** Naciśnij ten przycisk, aby przejść do ekranu dodawania interfejsu.

Konfiguracja PVC ATM

Na tym ekranie można skonfigurować identyfikator PVC ATM (VPI oraz VCI), wybrać opóźnienie DSL, wybrać kategorię usługi. Można też wybrać istniejące interfejsy poprzez zaznaczenie odpowiedniego pola.

VPI: [0-255]

VCI: [32-65535]

Wybierz typ połączenia DSL (EoA dla PPPoE, IPoE, oraz Bridge.)

EoA
 PPPoA
 IPoA

Tryb enkapsulacji:

Kategoria usługi:

Wybierz algorytm nadawania priorytetów IP QoS

Weighted Round Robin (WRR)
 Weighted Fair Queuing (WFQ)

Wartość wagi domyślnej kolejki: [1-63]

Pierwszeństwo grupy MPAAL:

Rysunek 4-3

- **VPI/VCI:** wartości VPI oraz VCI należy wprowadzać według zaleceń dostawcy Internetu.
- **Typ połączenia DSL:** Wybierz typ połączenia DSL według zalecenia dostawcy Internetu. Dostępne opcje to **EoA** (dla połączeń PPPoE, IPoE oraz Bridge), **PPPoA** (PPP over ATM) oraz **IPoA** (IP over ATM).
- **Tryb enkapsulacji:** Tryb przetwarzania danych dla wybranego połączenia należy konfigurować według zaleceń dostawcy Internetu.
- **Kategoria usługi:** Wybierz typ usługi ustalony przez dostawcę Internetu. Domyślne ustawienie to **UBR bez PCR**.

 **Uwaga:**

Na tej stronie można również uruchomić algorytm nadawania priorytetów QoS dla danego PVC. Zwiększa on wydajność niektórych usług, ale zużywa zasoby systemu, co powoduje zmniejszenie liczby dostępnych jednocześnie obwodów PVC. Ponadto funkcja QoS nie może być używana z połączeniami typu CBR oraz VBR w czasie rzeczywistym. Jeżeli wybierzesz usługę QoS, w menu

routera pojawi się dodatkowa pozycja, Quality of Service. Sposób jej konfigurowania opisany jest w punkcie [4.4.8 Quality of Service](#).

4.4.1.2 Interfejs ETH

Po wybraniu opcji „Ustawienia zaawansowane” → „Interfejs warstwy 2” → „Interfejs ETH”, możesz skonfigurować interfejs ETH WAN.

Konfiguracja interfejsu ETH WAN

Wybierz dodaj lub usuń aby skonfigurować interfejs ETH WAN.
Wykorzystaj jeden z interfejsów ETH jako interfejs WAN warstwy 2.

Interfejs/(Nazwa)	Tryb połączenia	Usuń
-------------------	-----------------	------

Rysunek 4-4

➤ **Dodaj:** Naciśnij ten przycisk, aby przejść do ekranu dodawania interfejsu.

Konfiguracja ETH WAN

Na tym ekranie można skonfigurować port ETH.

Wybierz port ETH: eth3/(LAN4/WAN) ▾

Rysunek 4-5

➤ **Port ETH:** Wybierz port ETH, który ma pełnić rolę portu WAN.

Po naciśnięciu przycisku „Zapisz/Zastosuj”, wyświetlony zostanie ekran pokazany na Rysunku 4-6.

Konfiguracja interfejsu ETH WAN

Wybierz dodaj lub usuń aby skonfigurować interfejs ETH WAN.
Wykorzystaj jeden z interfejsów ETH jako interfejs WAN warstwy 2.

Interfejs/(Nazwa)	Tryb połączenia	Usuń
eth3/(LAN4/WAN)	Domyślny	<input type="checkbox"/>

Rysunek 4-6

➤ **Usuń:** Zaznacz opcję w kolumnie Usuń, a następnie naciśnij przycisk „Usuń”. Odpowiedni interfejs zostanie usunięty z tabeli.

Uwaga:

Tylko jeden port Ethernet może pełnić funkcję interfejsu WAN.

4.4.2 Usługi WAN

Po wybraniu „Ustawienia zaawansowane” → „Usługi WAN”, pojawi się pokazana na Rysunku 4-7 tabelka z informacją o portach WAN. Po dodaniu nowego interfejsu warstwy 2, należy dodać interfejs WAN, postępując według poniższej instrukcji. Dostępnych jest pięć różnych konfiguracji dla różnego typu połączeń: PPPoE, IPoE, Bridge, PPPoA, oraz IPoA. Typ konfiguracji uwarunkowany jest wymaganiami dostawcy Internetu.

Konfiguracja usługi WAN (Wide Area Network)

Wybierz Dodaj, Usuń lub Edytuj aby skonfigurować usługę WAN dla wybranego interfejsu.

Interfejs	Opis	Typ	Vlan8021p	VlanMuxId	Igmp	NAT	Firewall	IPv6	Mld	Usuń	Edytuj
atm0.1	br_0_0_35	Bridge	N/A	N/A	Włączony	Wyłączony	Wyłączony	Wyłączony	Wyłączony	<input type="checkbox"/>	<input type="button" value="Edytuj"/>

Rysunek 4-7

Uwaga:

W poniższej sekcji, przy konfiguracji różnych typów połączeń, przedstawione są różne konfiguracje VPI oraz VCI. Jeżeli chcesz zmienić wartości VPI oraz VCI, przejdź do poprzedniej sekcji ([4.4.1 Interfejs warstwy 2](#)).

4.4.2.1 ATM-EoA-PPPoE

Jeżeli twój dostawca Internetu zapewnia połączenie **PPPoE** i używasz interfejsu ATM, skonfiguruj połączenie WAN według poniższej instrukcji:

1. Dodaj **nowy** interfejs ATM i wybierz opcję **EoA** jako Typ połączenia DSL ([4.4.1.1 Interfejs ATM](#)).
2. Naciśnij przycisk „**Dodaj**” pokazany na Rysunku 4-7. Pojawi się ekran pokazany na Rysunku 4-8. Naciśnij przycisk „**Dalej**”.

Konfiguracja interfejsu usługi WAN

Wybierz interfejs warstwy 2 dla tej usługi

Uwaga: Dla interfejsu ATM deskryptor to (portId_vpi_vci)

Interfejs Warstwy 2:

Rysunek 4-8

3. Na ekranie pokazanym na Rysunku 4-9 wybierz **typ usługi WAN**. Jeżeli twój dostawca zapewnia połączenie PPPoE zaznacz opcję **PPPoE**. Możesz też wprowadzić **opis usługi** lub pozostawić wartość domyślną. Naciśnij przycisk **Dalej**.

Konfiguracja usługi WAN

Wybierz typ usługi WAN:

PPPoE (PPP over Ethernet)

na przykład dynamiczne IP

Bridge

Wprowadź opis usługi:

Dla połączenia tagowanego wprowadź prawidłowy priorytet 802.1P oraz identyfikator VLAN 802.1Q.
Dla połączenia nietagowanego wprowadź wartość -1 w pola priorytet 802.1P oraz identyfikator VLAN 802.1Q.

Wprowadź priorytet 802.1P [0-7]:

Wprowadź identyfikator VLAN 802.1Q [0-4094]:

Wybór protokołu sieciowego:
Tylko IPV4

Rysunek 4-9

4. Wprowadź poniższe parametry i naciśnij przycisk „Dalej”.

Nazwa użytkownika i hasło PPP

Połączenie PPP najczęściej wymaga podania nazwy użytkownika i hasła do nawiązania połączenia. W poniższe pola wpisz nazwę użytkownika i hasło otrzymane od dostawcy Internetu.

Nazwa użytkownika PPP:

Hasło PPP:

Nazwa usługi PPPoE:

Tryb uwierzytelniania:

MTU (bajty): (Domyślna wartość 1480, nie należy zmieniać jeżeli nie jest to konieczne.)

Włącz funkcję NAT

Włącz funkcję Fullcone NAT

Połączenie na żądanie (z ograniczonym czasem nieaktywności)

Rozszerzenie IP PPP

Używaj statycznego adresu IPv4

Włącz tryb Debug dla PPP

Połączenie bridge dla ramek PPPoE pomiędzy portem WAN a portami LAN

Proxy Multicast

Włącz proxy IGMP Multicast

Rysunek 4-10

- **Nazwa użytkownika/hasło PPP:** Wprowadź nazwę użytkownika oraz hasło otrzymane od dostawcy Internetu. Obie wartości należy wprowadzać z uwzględnieniem wielkości liter.
- **Nazwa usługi PPPoE:** Wprowadź nazwę usługi PPPoE jeżeli otrzymałeś ją od dostawcy Internetu. Jeżeli pole pozostanie puste, nazwa będzie taka sama jak wprowadzony na poprzednim ekranie **opis usługi**.
- **Typ uwierzytelniania:** Wybierz **Typ uwierzytelniania** lub pozostaw domyślne ustawienie **AUTO**.

 **Uwaga:**

Jeżeli nie jesteś pewien czy wybrać takie opcje jak **Rozszerzenie IP PPP**, **Włącz tryb Debug dla PPP** itd., pozostaw je niezaznaczone.

- **MTU:** Maksymalny rozmiar wysyłanych pakietów. Domyślna wartość **MTU** to 1480 bajtów. Nie należy jej zmieniać jeżeli dostawca Internetu nie zaleci inaczej.
 - **Włącz funkcję NAT:** zaznaczenie tej opcji pozwala na zmianę adresów IP sieci lokalnej na inny adres, umożliwiając połączenie internetowe. Jeżeli ten router/modem zapewnia dostęp do Internetu w ramach twojej sieci, zaznacz tę funkcję. Jeżeli z siecią połączony jest także inny router, funkcja nie musi być włączona.
 - **Włącz funkcję Fullcone NAT:** Funkcja pozostaje wyłączona, o ile dostawca Internetu nie zaleci inaczej.
 - **Połączenie na żądanie (z ograniczonym czasem nieaktywności):** Włączenie tej funkcji wiąże się z zerwaniem połączenia Internetowego w przypadku długiej nieaktywności oraz automatyczne nawiązanie przy ponownej próbie uzyskania dostępu do Internetu. Funkcja ta jest użyteczna jeżeli dostawca Internetu pobiera opłaty za czas trwania połączenia z Internetem.
 - **Rozszerzenie IP PPP:** Wybierz tę opcję, aby twój komputer PC otrzymał publiczny adres IP z serwera PPP. Spowoduje to wyłączenie NAT oraz Firewall SPI. Działa to podobnie jak połączenie bridge, z dodatkowym uwierzytelnianiem PPP poprzez router. Funkcja ta używana jest przez nielicznych dostawców Internetu i nie należy jej włączać bez zalecenia.
 - **Używaj statycznego adresu IPv4:** Jeżeli otrzymałeś od dostawcy Internetu statyczny **adres IP**, adres **Bramy** oraz adresy serwerów **DNS** zaznacz tą opcję, aby wprowadzić je ręcznie.
 - **Włącz tryb Debug dla PPP:** Zaznacz tą opcję aby włączyć tryb debug dla uwierzytelniania PPP. Zdarzenia związane z uwierzytelnianiem PPP będą wtedy widoczne w dzienniku systemowym.
 - **Połączenie bridge dla ramek PPPoE pomiędzy portem WAN a portami LAN:** Zaznacz tę opcję jeżeli chcesz nawiązywać ręcznie połączenie PPP za pomocą komputera w sieci LAN.
 - **Włącz proxy IGMP Multicast:** IGMP (Internet Group Management Protocol) używany jest do zarządzania transmisjami multicast w sieciach TCP/IP. Niektórzy dostawcy Internetu używają protokołu IGMP do zdalnej konfiguracji urządzeń klienckich, takich jak routery. Domyślnie funkcja ta jest wyłączona. Aby dowiedzieć się czy konieczne jest jej włączenie, skontaktuj się z dostawcą Internetu.
5. Wybierz odpowiedni interfejs do działania w roli **bramy domyślnej**, tak jak to pokazano na Rysunku 4-11 i naciśnij przycisk „Dalej”.

Routing -- Brama domyślna

Na liście interfejsów bramy domyślnej może znajdować się wiele interfejsów WAN ale w danym momencie używany będzie tylko jeden z interfejsów o najwyższym priorytecie, jeżeli tylko dany interfejs WAN jest połączony. Priorytet interfejsów może zostać zmieniony poprzez usunięcie i ponowne dodanie interfejsów.

<p>Wybrane interfejsy bramy domyślnej</p> <div style="border: 1px solid gray; padding: 5px; min-height: 80px;">ppp0.2</div>	<p>></p> <p><</p>	<p>Dostępne interfejsy WAN</p> <div style="border: 1px solid gray; min-height: 80px;"></div>
--	-------------------------	---

Rysunek 4-11

6. Na poniższym ekranie skonfiguruj adresy serwerów DNS i naciśnij przycisk „Dalej”.

Konfiguracja serwerów DNS

Wybierz serwer DNS jednego z dostępnych interfejsów WAN LUB wprowadź statyczne adresy serwerów DNS. W trybie ATM, jeżeli skonfigurowany jest tylko 1 PVC z protokołem IPoA lub statyczne IPoE, należy wprowadzić statyczne adresy IP serwerów DNS.

Interfejsy DNS mogą korzystać z wielu interfejsów WAN jako serwerów DNS, ale w danym momencie używany będzie tylko jeden z interfejsów o najwyższym priorytecie, jeżeli tylko dany interfejs WAN jest połączony. Priorytet interfejsów może zostać zmieniony poprzez usunięcie i ponowne dodanie interfejsów.

Wybierz interfejs DNS z dostępnych interfejsów WAN:

Wybierz interfejsy - serwery DNS Dostępne interfejsy WAN

ppp0.2

Użyj następujących statycznych adresów IP serwerów DNS:

Preferowany serwer DNS:

Alternatywny serwer DNS:

Rysunek 4-12

- **Wybierz interfejs DNS z dostępnych interfejsów WAN:** Router będzie pobierał informacje DNS poprzez wybrany interfejs WAN.
- **Użyj następujących statycznych adresów IP serwerów DNS:** Zaznacz tę opcję jeżeli chcesz ręcznie wprowadzić adresy serwerów DNS.

👉 Uwaga:

Jeżeli skonfigurowany jest tylko jeden obwód PVC z wybranym połączeniem IPoA, należy wprowadzić statyczne adresy serwerów DNS.

7. Na następnym ekranie wyświetli się podsumowanie wprowadzonych ustawień. Naciśnij przycisk „Zapisz/Zastosuj”, aby zachować wprowadzone ustawienia.

Konfiguracja WAN - Podsumowanie

Upewnij się, że wprowadzone ustawienia są zgodne z zaleceniami dostawcy Internetu.

Typ połączenia:	PPPoE
NAT:	Włączone
Full Cone NAT:	Wyłączone
Firewall:	Włączone
IGMP Multicast:	Włączone
Quality Of Service:	Wyłączone

Naciśnij przycisk "Zapisz/Zastosuj" aby aktywować ten interfejs. Aby zmienić ustawienia naciśnij przycisk "Cofnij".

Rysunek 4-13

8. Na kolejnym ekranie widoczna będzie tabela konfiguracji portów WAN, zawierająca również nowo wprowadzoną konfigurację.

Konfiguracja usługi WAN (Wide Area Network)

Wybierz Dodaj, Usuń lub Edytuj aby skonfigurować usługę WAN dla wybranego interfejsu.

Interfejs	Opis	Typ	Vlan8021p	VlanMuxId	Igmp	NAT	Firewall	IPv6	Mld	Usuń	Edytuj
ppp0.2	pppoe_0_0_35	PPPoE	N/A	N/A	Włączony	Włączony	Włączony	Wyłączony	Wyłączony	<input type="checkbox"/>	<input type="button" value="Edytuj"/>

Rysunek 4-14

- **Usuń wszystkie:** Naciśnij przycisk „**Usuń wszystkie**”, aby usunąć wszystkie interfejsy z tabeli.
- **Usuń:** Zaznacz opcję w kolumnie Usuń, a następnie naciśnij przycisk „**Usuń**”. Odpowiedni interfejs zostanie usunięty z tabeli.

4.4.2.2 ATM-EoA-IPoE

Jeżeli twój dostawca Internetu zapewnia połączenie **IPoE** i używasz interfejsu ATM, skonfiguruj połączenie WAN według poniższej instrukcji:

1. Dodaj **nowy** interfejs ATM i wybierz opcję **EoA** jako Typ połączenia DSL ([4.4.1.1 Interfejs ATM](#)).
2. Naciśnij przycisk „**Dodaj**”, pokazany na Rysunku 4-7. Pojawi się ekran pokazany na Rysunku 4-8. Naciśnij przycisk „**Dalej**”.
3. Na ekranie pokazanym na Rysunku 4-9 wybierz **typ usługi WAN**. Jeżeli twój dostawca zapewnia połączenie IPoE zaznacz opcję **IPoE**. Naciśnij przycisk „**Dalej**”.
4. Wprowadź poniższe parametry i naciśnij przycisk „**Dalej**”.

Ustawienia IP WAN

Aby skonfigurować ustawienia WAN IP wprowadź parametry podane przez dostawcę Internetu.
 Uwaga: Jeżeli wybierzesz opcję „Uzyskaj adres IP automatycznie”, dla danego PVC w trybie IPoE adres IP będzie pobierany z DHCP.
 Jeżeli wybierzesz opcję „Użyj następującego statycznego adresu IP” należy wprowadzić adres IP WAN, maskę podsieci oraz bramę domyślną ręcznie.

Uzyskaj adres IP automatycznie

Identyfikator Vendor ID opcji 60:

Identyfikator IAID opcji 61: (8 znaków szesnastkowych)

Identyfikator DUID opcji 61: (znaki szesnastkowe)

Opcja 125: Wyłącz Włącz

Użyj następującego statycznego adresu IP:

Adres IP WAN:

Maska podsieci WAN:

Adres IP bramy WAN:

MTU (bajty): 1500 (opcjonalnie)

Rysunek 4-15

- **Uzyskaj adres IP automatycznie:** Gdy wybierzesz tę opcję, router automatycznie uzyska adres IP z serwera DHCP w sieci dostawcy Internetu.

Uwaga:

- 1) Odpowiedź od serwera DHCP zawiera pewną liczbę parametrów konfiguracyjnych (opcji DHCP), przeznaczonych dla routera. Mogą one zawierać ustawienia IP oraz inne parametry konfiguracyjne, zależne od producenta sprzętu. W niektórych przypadkach router może wykonywać specyficzne działania, zdefiniowane przez użytkownika (tak jak to opisano poniżej).
- 2) Jeżeli router działa jako klient DHCP, musi identyfikować się w każdym komunikacie DHCP w opcji 61. DUID/IAID jest częścią opcji 61.
 - **Identyfikator Vendor ID opcji 60:** Opcja 60 określa klasę producenta sprzętu.
 - **Identyfikator IAID opcji 61:** IAID (Identity Association ID) przydziela identyfikator do poszczególnych interfejsów. W przypadku gdy urządzenie działa jako pojedynczy klient DHCP, powinno używać IAID o wartości 1 dla wszystkich operacji DHCP. Jeżeli urządzenie posiada kilka interfejsów-klientów DHCP, wartość IAID dla pierwszego interfejsu powinna wynosić 1, dla kolejnego 2, itd. Alternatywnie można użyć identyfikatora IAID o wartości 1 dla obwodu wirtualnego, odpowiadającego pierwszemu połączeniu, a wartości 2 dla drugiego połączenia.
 - **Identyfikator DUID opcji 61:** Określa nazwę interfejsu, którego adres warstwy drugiej ma służyć serwerowi jako niepowtarzalny identyfikator DHCP - DUID (DHCP Unique Identifier). Aby serwer został uruchomiony, należy wprowadzić wartość w tym polu. W przypadku uruchomienia serwera, identyfikator DUID zostaje zapisany w dzienniku systemowym.
 - **Opcja 125:** Opcja 125 umożliwia wstępną konfigurację serwera DHCP tak, by obsługiwał określone klasy urządzeń, według określonych zasad, bez konieczności odczytywania indywidualnych identyfikatorów klientów przez serwer.
- **Używaj następującego statycznego adresu IP:** Zaznacz tę opcję jeżeli twój dostawca Internetu wymaga stosowania statycznego adresu IP/bramy domyślnej, a następnie wprowadź ręcznie **Adres IP WAN**, **Maskę podsieci WAN** oraz **Adres IP bramy WAN**.
5. Po naciśnięciu przycisku „Dalej”, wyświetlony zostanie poniższy ekran. Możesz na nim włączyć **NAT**, **Firewall SPI**, oraz **IGMP Multicast**. Jeżeli nie jesteś pewien, które z tych ustawień należy włączyć, pozostaw wartości domyślne i naciśnij przycisk „Dalej”.

Ustawienia NAT (Network Address Translation)

Funkcja NAT (Network Address Translation - translacja adresów sieciowych) umożliwia korzystanie z jednego adresu IP WAN (Wide Area Network) przez wiele urządzeń w sieci lokalnej (LAN).

Włącz NAT

Włącz funkcję Fullcone NAT

Włącz Firewall

IGMP Multicast

Włącz IGMP Multicast

Rysunek 4-16

- **Włącz NAT:** Funkcja NAT tłumaczy adresy IP urządzeń w sieci lokalnej na adres IP, używany w sieci Internet. Jeżeli ten router jest urządzeniem służącym do połączenia z Internetem –

zaznacz tę opcję. Jeżeli do połączenia z Internetem używany jest inny router możesz pozostawić tę opcję niezaznaczoną.

- **Włącz Firewall:** Firewall SPI zwiększa bezpieczeństwo połączenia. Zaznacz tę opcję, jeżeli uznasz to za stosowne.
- **Włącz IGMP Multicast:** Opcja ta jest domyślnie włączona. Takie ustawienie pozwala na przesyłanie pakietów IGMP (Internet Group Management Protocol) do sieci LAN. Protokół IGMP używany jest do zarządzania transmisjami multicast w sieciach TCP/IP. W przypadku większości połączeń, opcję tę można pozostawić wyłączoną. Niektórzy dostawcy Internetu używają protokołu IGMP do zdalnych zmian konfiguracji urządzeń klienckich, takich jak routery i inne. Jeżeli nie jesteś pewien czy włączyć tę funkcję, skontaktuj się z dostawcą Internetu.

 **Uwaga:**

Po zaznaczeniu opcji **Włącz NAT**, do menu routera zostanie dodana opcja **NAT**. Szczegółowy opis jej konfigurowania znajduje się w punkcie [4.4.5 NAT](#).

6. Wybierz interfejs **WAN**, który ma pełnić rolę bramy domyślnej i naciśnij przycisk „Dalej”.

Routing -- Brama domyślna

Na liście interfejsów bramy domyślnej może znajdować się wiele interfejsów WAN ale w danym momencie używany będzie tylko jeden z interfejsów o najwyższym priorytecie, jeżeli tylko dany interfejs WAN jest połączony. Priorytet interfejsów może zostać zmieniony poprzez usunięcie i ponowne dodanie interfejsów.

Wybrane interfejsy bramy domyślnej Dostępne interfejsy WAN

atm0.1	-> <-	
--------	----------	--

Rysunek 4-17

7. Na poniższym ekranie skonfiguruj adresy serwerów DNS.

Konfiguracja serwerów DNS

Wybierz serwer DNS jednego z dostępnych interfejsów WAN LUB wprowadź statyczne adresy serwerów DNS. W trybie ATM, jeżeli skonfigurowany jest tylko 1 PVC z protokołem IPoA lub statyczne IPoE, należy wprowadzić statyczne adresy IP serwerów DNS.
Interfejsy DNS mogą korzystać z wielu interfejsów WAN jako serwerów DNS, ale w danym momencie używany będzie tylko jeden z interfejsów o najwyższym priorytecie, jeżeli tylko dany interfejs WAN jest połączony. Priorytet interfejsów może zostać zmieniony poprzez usunięcie i ponowne dodanie interfejsów.

Wybierz interfejs DNS z dostępnych interfejsów WAN:

Wybierz interfejsy - serwery DNS Dostępne interfejsy WAN

atm0.1

Użyj następujących statycznych adresów IP serwerów DNS:

Preferowany serwer DNS:

Alternatywny serwer DNS:

Rysunek 4-18

Uwaga:

Jeżeli skonfigurowany jest tylko jeden obwód PVC z wybranym połączeniem IPoA, należy wprowadzić statyczne adresy serwerów DNS.

8. Na następnym ekranie wyświetli się podsumowanie wprowadzonych ustawień. Naciśnij przycisk „**Zapisz/Zastosuj**”, aby zachować wprowadzone ustawienia.

Konfiguracja WAN - Podsumowanie

Upewnij się, że wprowadzone ustawienia są zgodne z zaleceniami dostawcy Internetu.

Typ połączenia:	IPoE
NAT:	Włączone
Full Cone NAT:	Wyłączone
Firewall:	Wyłączone
IGMP Multicast:	Włączone
Quality Of Service:	Włączone

Naciśnij przycisk "Zapisz/Zastosuj" aby aktywować ten interfejs. Aby zmienić ustawienia naciśnij przycisk "Cofnij".

Rysunek 4-19

4.4.2.3 ATM-EoA-Bridge

Jeżeli chcesz skorzystać z połączenia **Bridge**, a używasz interfejsu ATM, skonfiguruj połączenie WAN według poniższej instrukcji:

1. Dodaj **nowy** interfejs ATM i wybierz opcję **EoA** jako Typ połączenia DSL ([4.4.1.1 Interfejs ATM](#)).
2. Naciśnij przycisk „**Dodaj**” pokazany na Rysunku 4-7, pojawi się ekran pokazany na Rysunku 4-8. Naciśnij przycisk „**Dalej**”.

3. Na ekranie pokazanym na Rysunku 4-9 wybierz **Bridge** jako **typ usługi WAN**. Naciśnij przycisk „**Dalej**”.
4. Na następnym ekranie wyświetli się podsumowanie wprowadzonych ustawień. Naciśnij przycisk „**Zapisz/Zastosuj**”, aby zachować wprowadzone ustawienia.

4.4.2.4 ATM-PPPoA

Jeżeli twój dostawca Internetu zapewnia połączenie **PPPoA** i używasz interfejsu ATM, skonfiguruj połączenie WAN według poniższej instrukcji:

1. Dodaj **nowy** interfejs ATM i wybierz opcję **PPPoA** jako Typ połączenia DSL ([4.4.1.1 Interfejs ATM](#)).
2. Naciśnij przycisk „**Dodaj**”, pokazany na Rysunku 4-7, a następnie postępuj podobnie jak przy konfiguracji połączenia **PPPoE** (według sekcji [4.4.2.1 ATM-EoA-PPPoE](#)). Jediną różnicą jest to, że nie należy wprowadzać **Nazwy usługi PPPoE** ani konfigurować opcji **Połączenie bridge dla ramek PPPoE pomiędzy portem WAN a portami LAN** na ekranie pokazanym na Rysunku 4-10.

4.4.2.5 ATM-IPoA

Jeżeli twój dostawca Internetu zapewnia połączenie **IPoA** i używasz interfejsu ATM, skonfiguruj połączenie WAN według poniższej instrukcji.

1. Dodaj **nowy** interfejs ATM i wybierz opcję **IPoA** jako Typ połączenia DSL ([4.4.1.1 Interfejs ATM](#)).
2. Naciśnij przycisk „**Dodaj**” pokazany na Rysunku 4-7, a następnie postępuj podobnie jak przy konfiguracji połączenia **IPoE** (według sekcji [4.4.2.2 ATM-EoA-IPoE](#)). Jediną różnicą jest to, że należy wprowadzić statyczny adres IP na ekranie pokazanym na Rysunku 4-15, oraz statyczny adres serwera DNS na ekranie pokazanym na Rysunku 4-18.

Uwaga:

Usługi ETH oraz ATM nie mogą być skonfigurowane jednocześnie. Po skonfigurowaniu usługi WAN korzystającej z interfejsu ATM nie można skonfigurować takiej usługi na interfejsie ETH bez uprzedniego usunięcia usługi ATM.

4.4.2.6 ETH-PPPoE

Jeżeli twój dostawca Internetu zapewnia połączenie **PPPoE** i używasz interfejsu ETH, skonfiguruj połączenie WAN według poniższej instrukcji:

1. Dodaj nowy interfejs **ETH** ([4.4.1.2 Interfejs ETH](#)).
2. Naciśnij przycisk „**Dodaj**”, pokazany na Rysunku 4-7, a następnie postępuj podobnie jak przy konfiguracji połączenia **PPPoE** na łączu **ATM** ([4.4.2.1 ATM-EoA-PPPoE](#)).

4.4.2.7 ETH-IPoE

Jeżeli twój dostawca Internetu zapewnia połączenie **IPoE** i używasz interfejsu ETH, skonfiguruj połączenie WAN według poniższej instrukcji:

1. Dodaj nowy interfejs **ETH** ([4.4.1.2 Interfejs ETH](#)).

2. Naciśnij przycisk „**Dodaj**”, pokazany na Rysunku 4-7, a następnie postępuj podobnie jak przy konfiguracji połączenia **IPoE** na łączu ATM (według sekcji [4.4.2.2 ATM-EoA-IPoE](#)).

4.4.2.8 ETH-Bridge

Jeżeli chcesz używać połączenia **Bridge** i używasz interfejsu ETH, skonfiguruj połączenie WAN według poniższej instrukcji:

Dodaj nowy interfejs **ETH** ([4.4.1.2 Interfejs ETH](#)).

Naciśnij przycisk „**Dodaj**” pokazany na Rysunku 4-7, a następnie postępuj podobnie jak przy konfiguracji połączenia **IPoE** na łączu ATM ([4.4.2.3 ATM-EoA-Bridge](#)).

4.4.3 Klonowanie MAC

Po wybraniu opcji „**Ustawienia zaawansowane**” → „**Klonowanie MAC**” możesz skonfigurować adres MAC interfejsu WAN, tak jak pokazano to poniżej.

Wyświetlona zostanie lista interfejsów WAN, skonfigurowanych według punktu [4.4.1 Interfejs warstwy 2](#), oraz ich domyślnych adresów MAC. Jeżeli nie skonfigurowałeś usług WAN dla żadnego z interfejsów (według punktu [4.4.2 Usługi WAN](#)), wyświetlony zostanie komunikat „Brak interfejsów WAN”.

Ostatnia pozycja w tabeli zawiera Adres MAC aktualnie używanego komputera PC.

Klonowanie adresu MAC

Ustaw określony adres MAC dla wybranego interfejsu WAN.

Klonuj adres MAC dla ppp0.2:	Niesklonowany	Przywróć domyślny
Adres MAC aktualnego PC:	d4:3d:7e:bf:61:5f	Klonuj do ppp0.2 ▾

Uwaga: Funkcja klonowania adresów MAC może być używana tylko dla portów WAN. Sklonowane adresy MAC **NIE MOGĄ** być takie same.

Rysunek 4-20

Wprowadź nowy adres MAC, który ma być używany dla interfejsu. Możesz również użyć domyślnie wprowadzonego adresu komputera PC.

Następnie wybierz odpowiedni interfejs WAN i naciśnij przycisk „**Klonuj**”.

Aby przywrócić domyślny adres MAC interfejsu WAN naciśnij przycisk „**Przywróć domyślny**”.

Uwaga:

Funkcja klonowania adresów MAC może być używana tylko dla portów WAN. Sklonowane adresy MAC nie mogą być takie same.

4.4.4 LAN

Po wybraniu opcji „Ustawienia zaawansowane” → „LAN” możesz skonfigurować ustawienia sieci LAN (Rysunek 4-21).

Konfiguracja sieci lokalnej - LAN (Local Area Network)

Skonfiguruj adres IP oraz maskę podsieci routera dla interfejsu LAN. Nazwa Grupy: Domyślna

Adres IP: 192.168.1.1

Maska podsieci: 255.255.255.0

Włącz IGMP Snooping

Tryb standardowy

Tryb blokujący

Wyłącz serwer DHCP

Włącz serwer DHCP

Początkowy adres IP: 192.168.1.100

Końcowy adres IP: 192.168.1.200

Czas przydzielenia (godzin): 24 (1-48)

Rezerwacja adresów IP: (Maksymalnie 32 wpisów)

Adres MAC	Adres IP	Status	Wyłącz/Włącz	Edytuj	Usuń
<input type="radio"/> Włącz funkcję DHCP Relay					
Adres IP serwera DHCP: 					
Uwaga: Musisz wyłączyć NAT dla połączenia WAN, inaczej funkcja DHCP Relay może nie działać!					

Skonfiguruj drugi adres IP oraz maskę podsieci dla interfejsu LAN

Zapisz/Zastosuj

Rysunek 4-21

- **Adres IP:** Możesz skonfigurować adres IP oraz maskę podsieci dla interfejsu LAN.
 - **Adres IP:** Wprowadź adres IP routera. Domyślny adres to 192.168.1.1. Po zmianie adresu IP należy logować się do strony konfiguracyjnej routera używając nowego adresu IP.
 - **Maska podsieci:** Wprowadź Maskę podsieci LAN routera. Domyślna maska to 255.255.255.0.
- **Włącz IGMP Snooping:** Po wybraniu tej opcji należy wybrać tryb działania usługi IGMP: standardowy lub blokujący.
- **Serwer DHCP:** Ustawienia umożliwiają konfigurację funkcji serwera DHCP (Dynamic Host Configuration Protocol). Domyślnie serwer DHCP sieci LAN routera jest włączony. Usługa DHCP służy do nadawania parametrów IP komputerom i urządzeniom skonfigurowanym tak, by automatycznie otrzymywały adresy IP, podłączanym do sieci LAN routera. Po włączeniu serwera DHCP router automatycznie przekazuje klientom DHCP adres LAN routera, jako adres bramy domyślnej. Należy pamiętać, że przy zmianie adresu IP LAN routera konieczna jest również zmiana zakresu przydzielanych przez serwer DHCP adresów IP.
 - **Początkowy adres IP:** Wprowadź wartość od jakiej serwer DHCP ma rozpocząć przydzielanie adresów. Domyślnym początkowym adresem IP jest **192.168.1.100**. Jeżeli adres IP routera to 192.168.1.1, początkowym adresem IP może być dowolny adres z przedziału od 192.168.1.2 do 192.168.1.254.
 - **Końcowy adres IP:** Wprowadź wartość, na jakiej serwer DHCP ma zakończyć przydzielanie adresów IP. Jeżeli adres IP routera to 192.168.1.1, adres końcowy nie może być większy niż 192.168.1.254. Domyślny adres końcowy to **192.168.1.200**.

- **Czas przydzielenia (godzin):** Czas przydzielenia adresu jest czasem, na jaki podłączonemu do routera urządzeniu zostaje nadany dynamiczny adres IP. Wprowadź wartość, w godzinach, na jaką zostanie nadany adres. Po wygaśnięciu adresu urządzenie automatycznie otrzyma nowy dynamiczny adres IP. Domyślnie czas przydzielenia adresu wynosi **24** godziny.
- **Rezerwacja adresów IP:** Funkcja ta umożliwia zarezerwowanie określonego adresu IP dla urządzenia w sieci LAN. Urządzenie to za każdym razem będzie otrzymywało od serwera DHCP ten sam, zarezerwowany dla niego adres IP. Rezerwacja adresów IP jest niezbędna dla serwerów i innych urządzeń wymagających używania stałych adresów IP. Naciśnij pokazany na Rysunku 4-21 przycisk „**Dodaj**”, a wyświetlony zostanie ekran rezerwacji adresu IP.

Rezerwacja adresu DHCP

Wprowadź adres MAC i adres IP i naciśnij przycisk "Zapisz/Zastosuj".

Adres MAC:

Adres IP:

Rysunek 4-22

- **Adres MAC:** Adres MAC urządzenia w sieci LAN, dla którego będzie zarezerwowany adres IP.
 - **Adres IP:** Adres jaki chcesz zarezerwować dla tego urządzenia.
- **Skonfiguruj drugi adres IP oraz maskę podsieci dla interfejsu LAN:** Używając tej opcji możesz skonfigurować drugi adres IP oraz maskę podsieci interfejsu LAN, dzięki którym możesz również uzyskać dostęp do strony konfiguracyjnej routera.

4.4.4.1 Konfiguracja LAN IPv6

Po wybraniu opcji „Ustawienia zaawansowane” → „LAN” → „Konfiguracja LAN IPv6” możesz skonfigurować ustawienia sieci LAN IPv6 (Rysunek 4-23).

Autokonfiguracja LAN IPv6

Uwaga: Adresy nadawane przez DHCPv6 są obsługiwane w oparciu o długość prefiksu mniejszą niż 64. Identyfikator interfejsu NIE obsługuje kompresji zer "...". Wprowadź adres w całkowitej, nieskróconej postaci. Przykładowo: Wprowadź "0:0:0:2" a nie "::2".

Stacyczna konfiguracja adresu LAN IPv6

Adres interfejsu (wymagana długość prefiksu):

Aplikacje LAN IPv6

Włącz Serwer DHCPv6

Bezstanowe

Stanowe

Początkowy identyfikator interfejsu:

Końcowy identyfikator interfejsu:

Czas przydzielenia (godziny):

Włącz RADVD

Włącz rozgłaszanie prefiksu ULA

Generuj losowo

Konfiguruj statycznie

Prefiks:

Preferowany czas życia (godzin):

Ważny czas życia (godzin):

Rysunek 4-23

- **Adres interfejsu (wymagana długość prefiksu):** Tu wprowadź długość prefiksu adresu interfejsu.
- **Aplikacje LAN IPv6:** Wybierz sposób przydzielania adresów IPv6 komputerom w sieci LAN. Dostępne opcje to Serwer DHCPv6 oraz RADVD.

Serwer DHCPv6:

- 1) Jeżeli wybrana jest opcja **Bezstanowe**, nie należy wprowadzać dodatkowej konfiguracji.
- 2) Jeżeli wybrana jest opcja **Stanowe**, należy wprowadzić następujące parametry:

Włącz Serwer DHCPv6

Bezstanowe

Stanowe

Początkowy identyfikator interfejsu:

Końcowy identyfikator interfejsu:

Czas przydzielenia (godziny):

- **Początkowy identyfikator interfejsu:** Wprowadź wartość, od jakiej serwer DHCP ma rozpocząć przydzielanie adresów IPv6.
- **Końcowy identyfikator interfejsu:** Wprowadź wartość, na jakiej serwer DHCP ma zakończyć przydzielanie adresów IPv6.

- **Czas przydzielenia (godziny):** Czas przydzielenia adresu jest czasem, na jaki podłączonemu do routera urządzeniu zostaje nadany dynamiczny adres IPv6. Wprowadź wartość, w godzinach, na jaką zostanie nadany adres. Po wygaśnięciu adresu urządzenie automatycznie otrzyma nowy dynamiczny adres IPv6. Domyślnie czas przydzielenia adresu wynosi **24** godziny.

Dla RADVD:

- 1) Jeżeli wybrana zostanie opcja **Generuj losowo**, nie należy wprowadzać dodatkowej konfiguracji.
- 2) Jeżeli wybrana zostanie opcja **Konfiguruj statycznie**, należy wprowadzić następujące parametry:

<input checked="" type="checkbox"/>	Włącz RADVD	
<input checked="" type="checkbox"/>	Włącz rozgłaszanie prefiksu ULA	
<input type="radio"/>	Generuj losowo	
<input checked="" type="radio"/>	Konfiguruj statycznie	
	Prefiks:	<input type="text"/>
	Preferowany czas życia (godzin):	<input type="text" value="-1"/>
	Ważny czas życia (godzin):	<input type="text" value="-1"/>

- **Prefiks:** Wprowadź wartość prefiksu.

Naciśnij przycis „**Zapisz/Zastosuj**”, aby zapisać wprowadzone ustawienia.

4.4.5 NAT

Funkcja NAT (Network Address Translation) umożliwia udostępnianie pojedynczego adresu IP WAN (Wide Area Network) wielu urządzeniom podłączonym w sieci lokalnej LAN (Local Area Network).

Uwaga:

Jeżeli wybierzesz **PPPoA** lub **PPPoE** w konfiguracji interfejsu WAN, lub jeżeli zaznaczysz opcję **Włącz NAT** dla połączeń **IPoA** oraz **IPoE** ([4.4.2 Usługi WAN](#)), na stronie konfiguracji routera widoczna będzie opcja **NAT** (pokazana na Rysunku 4-24).

NAT -- Konfiguracja serwerów wirtualnych										
<small>Funkcja serwerów wirtualnych umożliwia przekierowanie transmisji przychodzącej od strony WAN (określonej poprzez protokół i port zewnętrzny) na wewnętrzny serwer o prywatnym adresie IP znajdujący się w sieci lokalnej. Określenie portów wewnętrznych jest wymagane tylko wtedy, gdy wewnętrzny port używany w sieci lokalnej ma być inny niż port zewnętrzny. Różnie można skonfigurować maksymalnie 32 wpisy. Urządzenia korzystające z usługi UPnP mogą dodać maksymalnie 64 wpisów.</small>										
Nazwa serwera	Początkowy port zewnętrzny	Końcowy port zewnętrzny	Protokół	Początkowy port wewnętrzny	Końcowy port wewnętrzny	Adres IP serwera	Interfejs WAN	Status	Włącz/Wyłącz	Edytuj Usuń
<input type="button" value="Dodaj"/> <input type="button" value="Włącz wszystkie"/> <input type="button" value="Wybierz wszystkie"/> <input type="button" value="Usuń"/>										

Rysunek 4-24

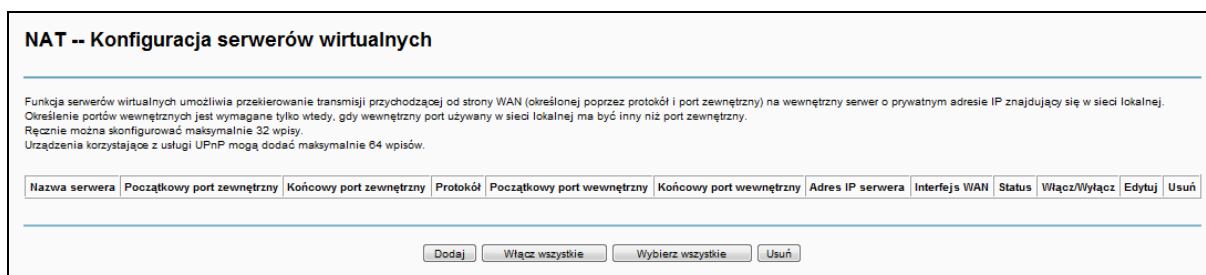
Po wybraniu opcji „**Ustawienia zaawansowane**” → „**NAT**” pojawią się cztery dodatkowe opcje: **Serwery wirtualne**, **Port Triggering**, **Host DMZ** oraz **ALG**. Wybranie jednej z nich powoduje przejście do ekranu konfiguracji odpowiadającej jej funkcji.



4.4.5.1 Serwery wirtualne

Po wybraniu opcji „**Ustawienia zaawansowane**” → „**NAT**” → „**Serwery wirtualne**” możesz skonfigurować usługę serwery wirtualne (Rysunek 4-25).

Serwery wirtualne używane są do udostępniania poprzez Internet usług uruchomionych na serwerach w sieci LAN. Mogą to być usługi takie jak serwer WWW, zdalny pulpit, serwer pocztowy, serwer FTP i inne. Serwer wirtualny definiuje się przez wyznaczenie portu usługi oraz adresu IP urządzenia w sieci LAN. Wszelkie zapytania do określonego portu, których źródłem jest Internet, będą przekierowywane na urządzenie o określonym adresie IP. Urządzenia zdefiniowane jako serwery wirtualne muszą używać statycznych lub zarezerwowanych adresów IP, w przeciwnym wypadku, jeżeli otrzymają od serwera DHCP inne adresy IP niż adresy określone jako serwery wirtualne, usługi nie będą działać.



Rysunek 4-25

- **Tabela serwerów wirtualnych:** w tabeli wyświetlane są informacje o zdefiniowanych serwerach wirtualnych.
 - **Nazwa serwera:** Nazwa **serwera wirtualnego**. Nazwy te nie mogą się powtarzać.
 - **Początkowy port zewnętrzny:** Początkowy port z zakresu portów zewnętrznych.
 - **Końcowy port zewnętrzny:** Końcowy port z zakresu portów zewnętrznych.
 - **Protokół:** Protokół używany dla danej usługi, **TCP**, **UDP** lub **TCP/UDP**.
 - **Początkowy port wewnętrzny:** Początkowy port z zakresu portów wewnętrznych.
 - **Końcowy port wewnętrzny:** Końcowy port z zakresu portów wewnętrznych. Możesz wprowadzić wartość portu lub pozostawić to pole puste.
 - **Adres IP serwera:** Adres IP urządzenia, na którym będzie uruchomiona określona usługa.
 - **Interfejs:** Interfejs WAN, poprzez który będzie udostępniana usługa.
- **Dodaj:** Naciśnij przycisk „**Dodaj**” żeby dodać nowy wpis.
- **Usuń:** Zaznacz opcję w kolumnie **Usuń** (Rysunek 4-25), a następnie naciśnij przycisk „**Usuń**”. Odpowiedni wpis zostanie usunięty z tabeli.

router umożliwia zdalnemu urządzeniu nawiązywanie nowych połączeń z aplikacją po stronie LAN, z użyciem portów usługi. Można skonfigurować maksymalnie 32 wpisy.

NAT -- konfiguracja Port Triggering

Niektóre aplikacje takie jak gry, konferencje wideo, aplikacje zdalnego dostępu wymagają otwarcia określonych portów w celu umożliwienia dostępu zdalnego. Funkcja Port Triggering umożliwia dynamiczne otwarcie portu opisanego jako 'Port usługi' w momencie gdy aplikacja działająca po stronie LAN nawiązuje połączenie TCP/UDP do znajdującego się w Internecie serwera aplikacji po jednym z portów otwierających. Po otwarciu portu router przekierowuje połączenia przychodzące z zewnątrz po 'porcie usługi' na urządzenie w sieci LAN które jako pierwsze nawiązało połączenie wychodzące po 'porcie otwierającym'. Maksymalnie można skonfigurować 32 wpisów.

Nazwa usługi	Otwierający		Usługi		Interfejs WAN	Status	Włącz/Wyłącz	Edytuj	Usuń		
	Protokół	Zakres portów		Protokół						Zakres portów	
		Początek	Koniec							Początek	Koniec
<input type="button" value="Dodaj"/> <input type="button" value="Włącz wszystkie"/> <input type="button" value="Wybierz wszystkie"/> <input type="button" value="Usuń"/>											

Rysunek 4-27

- **Tabela Port Triggering:** W tabeli wyświetlane są informacje o zdefiniowanych wpisach Port Triggering.
- **Nazwa usługi:** Nazwa wpisu **Port Triggering**. Nazwy te nie mogą się powtarzać.
 - **Otwierający:** Zawiera protokół oraz wartość początkową i końcową zakresu portów.
 - **Usługi:** Zawiera protokół oraz wartość początkową i końcową zakresu portów.
 - **Interfejs WAN:** Interfejs WAN, dla którego zdefiniowana jest reguła.
- **Dodaj:** Naciśnij przycisk „Dodaj”, żeby dodać nowy wpis.
- **Usuń:** Zaznacz opcję w kolumnie Usuń (pokazaną na Rysunku 4-27), a następnie naciśnij przycisk „Usuń”. Odpowiedni wpis zostanie usunięty z tabeli.

Aby dodać nowy wpis Port Triggering:

1. Naciśnij przycisk „Dodaj”, pokazany na Rysunku 4-27. Pojawi się ekran dodawania wpisu **Port Triggering**, pokazany na Rysunku 4-28.

NAT -- Port Triggering

Niektóre aplikacje takie jak gry, konferencje wideo, aplikacje zdalnego dostępu i inne wymagają otwarcia określonych portów do działania aplikacji. Na tym ekranie możesz skonfigurować ustawienia tych portów wybierając aplikację z menu lub definiując własną (Własna aplikacja) naciskając przycisk "Zapisz/Zastosuj".

Ilość pozostałych wpisów do skonfigurowania: 32

Użyj interfejsu:

Nazwa aplikacji:

Wybierz aplikację:

Własna aplikacja:

Początkowy port otwierający	Końcowy port otwierający	Protokół otwierający	Początkowy port usługi	Końcowy port usługi	Protokół usługi
		TCP ▼			TCP ▼
		TCP ▼			TCP ▼
		TCP ▼			TCP ▼
		TCP ▼			TCP ▼
		TCP ▼			TCP ▼
		TCP ▼			TCP ▼
		TCP ▼			TCP ▼
		TCP ▼			TCP ▼
		TCP ▼			TCP ▼

Rysunek 4-28

- Wybierz z listy interfejs, którego chcesz używać.
- Wybierz aplikację z listy domyślnie zdefiniowanych usług. Jeżeli usługa nie znajduje się na liście, zaznacz opcję Własna Aplikacja i wprowadź nazwę aplikacji.
- Wprowadź Początkowy port otwierający, Końcowy port otwierający, Początkowy port usługi oraz Końcowy port usługi do tabeli, a następnie wybierz protokół: **TCP**, **UDP** lub **TCP/UDP**.
- Naciśnij przycisk „**Zapisz/Zastosuj**”, aby włączyć Port Triggering. Wprowadzone ustawienie wyświetli się w tabeli pokazanej na Rysunku 4-27.

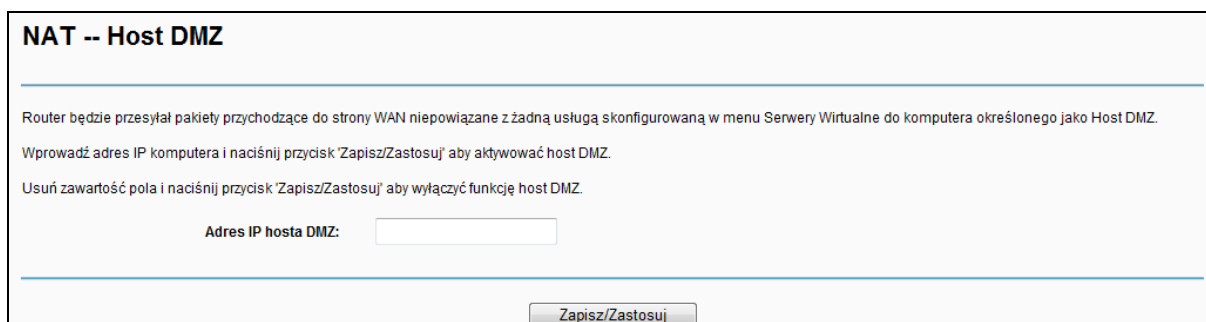
 **Uwaga:**

Jeżeli wybierzesz usługę z listy usług, pola Początkowy port otwierający, Końcowy port otwierający, Początkowy port usługi, Końcowy port usługi oraz Protokół wypełnione zostaną automatycznie.

4.4.5.3 Host DMZ

Po wybraniu opcji „**Ustawienia zaawansowane**” → „**NAT**” → „**Host DMZ**”, możesz skonfigurować usługę Host DMZ (Rysunek 4-29).

Funkcja hosta DMZ pozwala wystawić hosta z sieci lokalnej poza firewall routera dla specjalnych zastosowań, takich jak np. gry online lub konferencje wideo.



NAT -- Host DMZ

Router będzie przysyłał pakiety przychodzące do strony WAN niepowiązane z żadną usługą skonfigurowaną w menu Serwery Wirtualne do komputera określonego jako Host DMZ.

Wprowadź adres IP komputera i naciśnij przycisk 'Zapisz/Zastosuj' aby aktywować host DMZ.

Usuń zawartość pola i naciśnij przycisk 'Zapisz/Zastosuj' aby wyłączyć funkcję host DMZ.

Adres IP hosta DMZ:

Zapisz/Zastosuj

Rysunek 4-29

Aby dodać nowego hosta DMZ:

Wprowadź adres IP komputera, a następnie naciśnij przycisk „**Zapisz/Zastosuj**”, aby włączyć usługę.

 **Uwaga:**

Host DMZ przekierowuje wszystkie porty na podany adres IP. Komputer, który jest hostem DMZ powinien mieć ustawiony statyczny adres IP.

4.4.5.4 ALG

Po wybraniu opcji „**Ustawienia zaawansowane**” → „**NAT**” → „**ALG**”, możesz skonfigurować funkcję ALG (Rysunek 4-30).

ALG

Wybierz funkcje ALG.

- FTP włączony
- TFTP włączony
- SIP włączony
- H.323 włączony
- RTSP włączony
- IRC włączony

Rysunek 4-30

Naciśnij przycisk „**Zapisz/Zastosuj**”, aby zapisać ustawienia.

4.4.6 Bezpieczeństwo

Po wybraniu opcji „**Ustawienia zaawansowane**”→„**Bezpieczeństwo**”, lista po lewej stronie rozwinie się i pojawią się dwie dodatkowe opcje do wyboru: **Filtrowanie IP** oraz **Filtrowanie MAC** (tylko przy włączonym interfejsie WAN Bridge).



4.4.6.1 Filtrowanie IP

Filtrowanie adresów IP pozwala administratorom sieci na kontrolę ruchu wychodzącego, bazując na adresie IP użytkownika.

Po wybraniu opcji „**Ustawienia Zaawansowane**”→„**Bezpieczeństwo**”→„**Filtrowanie IP**”, możesz skonfigurować filtry wychodzących adresów IP (Rysunek 4-31).

Konfiguracja filtru wychodzących adresów IP, pozwala kontrolować ruch wychodzący z konkretnych adresów IP z sieci LAN. Domyślnie cały ruch IP wychodzący z sieci LAN jest przepuszczany, można jednak **ZABLOKOWAĆ** część ruchu, konfigurując filtry.

Konfiguracja filtru wychodzących adresów IP

Domyślnie cały ruch IP wychodzący z sieci LAN jest przepuszczany, można jednak **ZABLOKOWAĆ** część ruchu konfigurując filtry.

Naciśnij przycisk Dodaj lub Usuń aby skonfigurować filtry wychodzących adresów IP. Maksymalnie można skonfigurować 36 filtrów.

Nazwa filtru	Wersja IP	Protokół	Źródłowe IP/Dł.prefiksu	Port źródł.	Docelowe IP/Dł.prefiksu	Port doc.	Usuń
filtr-wysyłania	4	TCP or UDP	192.168.1.222		210.77.150.40	25	<input type="button" value="X"/>

Rysunek 4-31

Aby dodać filtr IP dla połączeń wychodzących:

1. Naciśnij przycisk „Dodaj” (Rysunek 4-31), a pojawi się ekran dodawania filtra (Rysunek 4-32).

Dodaj filtr IP -- Wychodzące

Na tej stronie możesz utworzyć regułę filtrowania wychodzących pakietów poprzez nadanie nazwy reguły i określenie co najmniej jednego warunku. Wszystkie warunki określone w regule muszą być spełnione aby filtrowanie zadziałało. Aby zapisać i aktywować filtr naciśnij przycisk Zapisz/Zastosuj.

Nazwa filtra:	<input type="text" value="filtr-wysylania"/>
Wersja IP:	<input type="text" value="IPv4"/>
Protokół:	<input type="text" value="TCP/UDP"/>
Źródłowy adres IP [długość prefiksu]:	<input type="text" value="192.168.1.222"/>
Port źródłowy (port lub zakres port:port):	<input type="text"/>
Docelowy adres IP [długość prefiksu]:	<input type="text" value="210.77.150.40"/>
Port docelowy (port lub zakres port:port):	<input type="text" value="25"/>

Rysunek 4-32

2. Wprowadź **Nazwę filtra** dla reguły. Nazwy te nie mogą się powtarzać.
3. Wybierz protokół dla połączenia: **TCP/UDP**, **TCP**, **UDP** lub **ICMP** z listy.
4. Wprowadź **Źródłowy adres IP**, a następnie **Port źródłowy** (port lub zakres port:port) w odpowiednich polach.
5. Wprowadź **Docelowy adres IP**, a następnie **Port docelowy** (port lub zakres port:port) w odpowiednich polach.
6. Naciśnij przycisk „Zapisz/Zastosuj”, aby zapisać filtr.

Uwaga:

Przy dodawaniu filtra należy ustalić przynajmniej jeden warunek oprócz nazwy filtra. Jeżeli pole protokół nie będzie wprowadzone, reguła będzie odnosić się do wszystkich protokołów. Jeżeli pola adres źródłowy lub docelowy nie będą wprowadzone, reguła będzie odnosić się do wszystkich adresów źródłowych lub docelowych. Jeżeli pola port źródłowy lub docelowy nie będą wprowadzone, reguła będzie odnosić się do wszystkich portów źródłowych lub docelowych.

4.4.6.2 Filtrowanie MAC

Po wybraniu opcji „Ustawienia Zaawansowane”→„Bezpieczeństwo”→„Filtrowanie MAC”, możesz skonfigurować filtry MAC (Rysunek 4-33). Funkcja ta pozwala na kontrolę dostępu do Internetu bazując na adresach MAC użytkowników.

Uwaga:

Filtrowanie adresów MAC działa jedynie dla połączeń ATM PVC działających w trybie Bridge.

Konfiguracja filtrowania MAC

Filtrowanie adresów MAC działa jedynie dla połączeń ATM PVC działających w trybie Bridge. **PRZEPUSZCZAJ** oznacza że wszystkie ramki warstwy MAC będą **PRZEPUSZCZANE** z wyjątkiem tych spełniających reguły określone w poniższej tabeli. **BLOKUJ** oznacza że wszystkie ramki warstwy MAC będą **BLOKOWANE**, z wyjątkiem tych spełniających reguły określone w poniższej tabeli.

Zasady filtrowania MAC dla każdego Interfejsu:

UWAGA: Zmiana zasad filtrowania dla danego interfejsu spowoduje AUTOMATYCZNE USUNIĘCIE wszystkich reguł zdefiniowanych dla tego Interfejsu! Konieczne będzie zdefiniowanie nowych reguł.

Interfejs	Zasady	Zmiana
atm0.1	PRZEPUSZCZAJ	<input type="checkbox"/>

Zmiana zasad

Naciśnij przycisk Dodaj lub Usuń aby skonfigurować reguły filtrowania adresów MAC. Można skonfigurować maksymalnie 36 filtrów MAC.

Interfejs	Protokół	Docelowy MAC	Źródłowy MAC	Usuń
atm0.1	IGMP	00:11:22:33:44:AA	00:11:22:33:44:BB	<input type="checkbox"/>

Dodaj Usuń

Rysunek 4-33

- **Zmiana zasad:** Dostępne są dwie zasady dla filtrów MAC: **PRZEPUSZCZAJ** oraz **BLOKUJ**. Zaznacz **Zmiana** a następnie naciśnij przycisk „Zmiana zasad”, aby przełączać się pomiędzy zasadami. **PRZEPUSZCZAJ** oznacza że wszystkie ramki warstwy MAC będą **PRZEPUSZCZANE**, z wyjątkiem tych spełniających reguły określone w poniższej tabeli. **BLOKUJ** oznacza, że wszystkie ramki warstwy MAC będą **BLOKOWANE**, z wyjątkiem tych spełniających reguły określone w poniższej tabeli.
- **Dodaj:** Naciśnij przycisk „Dodaj”, aby dodać nowy filtr MAC (Rysunek 4-33).
- **Usuń:** Zaznacz pole **Usuń** w tabelce (Rysunek 4-33), a następnie naciśnij przycisk „Usuń”, aby usunąć wybraną regułę.

Aby dodać nowy filtr MAC:

1. Naciśnij przycisk „Dodaj” (Rysunek 4-33), a pojawi się ekran dodawania filtru MAC (Rysunek 4-34).

Dodaj filtr MAC

Utwórz filtr identyfikujący ramki warstwy MAC poprzez spełnianie co najmniej jednego z poniższych warunków. Sprawdzane są wszystkie określone warunki. Naciśnij przycisk „Zapisz/Zastosuj” aby zapisać i aktywować filtr.

Typ protokołu:

Docelowy adres MAC:

Źródłowy adres MAC:

Interfejsy WAN (tylko te które są skonfigurowane w trybie Bridge):

Zapisz/Zastosuj

Rysunek 4-34

2. Wybierz **Typ protokołu** z rozwijanej listy.
3. Wprowadź **Docelowy adres MAC** oraz **Źródłowy adres MAC** w odpowiednie pola.
4. Wybierz **Interfejs WAN** z listy.
5. Naciśnij przycisk „Zapisz/Zastosuj”, aby zapisać filtr. Pojawi się on w tabeli (Rysunek 4-34).

4.4.7 Kontrola rodzicielska

Wybierz opcję „Ustawienia zaawansowane” → „Kontrola rodzicielska”. Na tym ekranie możesz skonfigurować funkcję Kontroli rodzicielskiej (Rysunek 4-35). Ograniczenie czasu dostępu pozwala ustawić terminy, w których dostęp do Internetu będzie ograniczony. Filtr URL ogranicza dostęp wszystkich komputerów do konkretnych stron internetowych. Opcje te działają niezależnie.

Ograniczenie czasu dostępu

Można skonfigurować maksymalnie 16 wpisów.

Nazwa użytkownika	MAC	Dni							Czas		Status	Włącz/Wyłącz	Edytuj	Usuń	
		Pon	Wto	Śro	Czw	Pią	Sob	Nie	Start	Stop					

Rysunek 4-35

4.4.7.1 Ograniczenie czasu dostępu

Opcja ta pozwala na ograniczenie dostępu dla danych komputerów z sieci LAN w ustalonych porach.

Ograniczenie czasu dostępu

Można skonfigurować maksymalnie 16 wpisów.

Nazwa użytkownika	MAC	Dni							Czas		Status	Włącz/Wyłącz	Edytuj	Usuń
		Pon	Wto	Śro	Czw	Pią	Sob	Nie	Start	Stop				
child-1	00:11:22:33:44:cc						x	x	18:00	21:00	Włączone	<input type="button" value="Wyłącz"/>	<input type="button" value="Edytuj"/>	<input type="checkbox"/>

Rysunek 4-36

Aby dodać Ograniczenie czasu dostępu:

- Naciśnij przycisk „Dodaj” (Rysunek 4-36), a pojawi się ekran dodawania reguły (Rysunek 4-37).

Ograniczenia czasu dostępu

Ta strona umożliwia dodanie ograniczenia czasu dostępu do routera dla określonych urządzeń łączących się z routerem. Pole "Twój adres MAC" wyświetla adres MAC komputera na którym wyświetlona jest strona konfiguracyjna.
Aby ograniczyć dostęp dla innego urządzenia w sieci LAN naciśnij przycisk "Inny adres MAC" i wprowadź adres MAC innego urządzenia.
Aby sprawdzić adres MAC komputera wyposażonego w system Windows uruchom wiersz poleceń i wprowadź komendę "ipconfig /all".

Nazwa użytkownika:

Twój adres MAC:

Inny adres MAC (xx:xx:xx:xx:xx:xx):

Dni tygodnia:	Pon	Wto	Śro	Czw	Pią	Sob	Nie
Kliknij, aby wybrać:	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Początkowy czas blokowania (gg:mm):

Końcowy czas blokowania (gg:mm):

Rysunek 4-37

2. Wprowadź **Nazwę użytkownika** urządzenia podłączonego do sieci LAN routera.
3. Aby ograniczyć dostęp urządzeniu, które aktualnie zalogowane jest do strony konfiguracyjnej routera, wybierz opcję **Twój adres MAC**. Adres MAC zostanie wypełniony automatycznie. Aby ograniczyć dostęp dla innego urządzenia, wybierz opcję **Inny adres MAC**, a następnie wprowadź adres MAC tego urządzenia.
4. Wybierz dni, dla których reguła ma być aktywna.
5. Wprowadź **Początkowy czas blokowania** oraz **Końcowy czas blokowania** w polach poniżej. Urządzenie nie będzie mogło połączyć się z Internetem pomiędzy danymi godzinami.
6. Naciśnij przycisk „**Zapisz/Zastosuj**”, aby zapisać regułę. Pojawi się ona w tabeli (Rysunek 4-36).

Uwaga:

Ograniczenie czasu dostępu nie będzie działało prawidłowo zanim funkcja „**Zarządzanie → Pobieranie czasu**” nie zostanie skonfigurowana na routerze.

4.4.7.2 Filtr URL

Funkcja ta pozwala skonfigurować filtry, które ograniczają dostęp wszystkich urządzeń w sieci LAN do usług na wybranych portach. Filtr URL i Ograniczenie czasu są od siebie niezależne.

Filtr URL

Wybierz typ listy a następnie skonfiguruj wpisy. Maksymalnie można skonfigurować 200 adresów URL.

Typ listy URL: Wyłącz Zezwalaj Blokuj

LAN IP	Port	Adres	Status	Wyłącz/Włącz	Edytuj	Usuń
	80	www.google.com	Włączony	Wyłącz	Edytuj	<input type="checkbox"/>

Rysunek 4-38

Istnieją trzy możliwe reguły dla filtra URL.

- **Wyłącz:** Filtr URL jest nieaktywny.
- **Zezwalaj:** Pozwól komputerom na dostęp tylko do określonych adresów URL.
- **Blokuj:** Blokuj komputerom dostęp do określonych adresów URL.

Aby dodać nowy filtr URL:

1. Zaznacz **Zezwalaj** lub **Blokuj**. W przykładzie wybrana została opcja **Blokuj**.
2. Naciśnij przycisk „**Dodaj**” (Rysunek 4-38), a pojawi się ekran dodawania filtra URL (Rysunek 4-39). Wprowadź Adres URL i Numer portu.

Kontrola rodzicielska -- filtr URL Dodaj

Wprowadź adres i naciśnij przycisk "Zapisz/Zastosuj" aby dodać wpis filtra URL. Możesz dodać adres LAN IP aby wpis dotyczył określonego urządzenia w sieci lokalnej.

Zakres LAN IP: - (opcjonalnie)

Numer portu: (Jeżeli pole pozostanie puste użyta będzie domyślna wartość - 80.)

Adres:

Rysunek 4-39

- Naciśnij przycisk „**Zapisz/Zastosuj**”, aby dodać wpis. Pojawi się on w tabeli (Rysunek 4-38). Dostęp do wybranej strony zostanie zablokowany dla wszystkich komputerów podłączonych do routera.

4.4.8 Quality of Service

Wybierając opcję „**Ustawienia zaawansowane**” → „**Quality of Service**” możesz włączyć funkcję QoS (Zarządzanie kolejkami). QoS pozwala ustawić priorytet dla danych. Poprzez dołączenie specjalnych identyfikatorów do nagłówek przychodzących pakietów, QoS decyduje, do której kolejki trafi pakiet. Jest to użyteczne w przypadku kiedy chce się nadać wyższy priorytet pewnym typom pakietów, np. pakietom komunikacji głosowej.

QoS - Konfiguracja zarządzania kolejkami

Jeżeli pole Włącz QoS jest zaznaczone, wybierz domyślne oznaczenie DSCP które będzie automatycznie nadawane przychodzącym pakietom bez odwoływania się do konkretnego klasyfikatora. Naciśnij przycisk 'Zapisz/Zastosuj' aby zapisać ustawienie.

Uwaga: Jeżeli pole Włącz QoS nie jest zaznaczone funkcja QoS będzie wyłączona dla wszystkich interfejsów.

Uwaga: Domyślne oznaczenie DSCP jest używane aby oznaczyć wszystkie pakiety wychodzące nie spełniające żadnej z reguł klasyfikacji.

Włącz QoS

Wybierz domyślne oznaczenie DSCP

Rysunek 4-40

Zaznacz „**Włącz QoS**”, żeby włączyć QoS dla wszystkich interfejsów.

Wybierz **domyślne oznaczenie DSCP**, które będzie automatycznie nadawane przychodzącym pakietom bez odwoływania się do konkretnego klasyfikatora.

Naciśnij przycisk „**Zapisz/Zastosuj**”, aby zapisać ustawienia.

Uwaga:

Domyślne oznaczenie DSCP jest stosowane do oznaczania wszystkich pakietów wychodzących, ale nie spełniających żadnej z reguł klasyfikacji.

4.4.8.1 Konfiguracja kolejek

Po wybraniu opcji „Ustawienia zaawansowane” → „Quality of Service” → „Konfiguracja kolejek”, możesz skonfigurować kolejki QoS.

Konfiguracja kolejki QoS

W trybie ATM można skonfigurować maksymalnie 8 kolejek.
 W trybie PTM można skonfigurować maksymalnie 8 kolejek.
 Dla każdego interfejsu Ethernet można skonfigurować maksymalnie 4 kolejki.
 Dla każdego interfejsu Ethernet WAN można skonfigurować maksymalnie 4 kolejki.
 Aby dodać kolejkę naciśnij przycisk Dodaj.
 Aby usunąć kolejki zaznacz odpowiednie pola a następnie naciśnij przycisk Usuń.
 Naciśnięcie przycisku Włącz spowoduje sprawdzenie wszystkich kolejek w tabeli. Kolejki z zaznaczonym polem włącz zostaną włączone. Reguły z niezaznaczonym polem włącz zostaną wyłączone.
 Pole włącz pokazuje również status każdej kolejki po odświeżeniu strony.
 Jeżeli funkcja WMM na stronie ustawień bezprzewodowych zostanie wyłączona kolejki dotyczące połączeń bezprzewodowych nie będą funkcjonowały.

Nazwa	Klucz	Interfejs	Identyfikator	Pierw/Alg/Waga	Opóźnienie DSL	Priorytet PTM	Min. Prędkość(b/s)	Okr. Prędkość(b/s)	Rozmiar serii(bajtów)	Włącz	Usuń
WMM - priorytet głosowy	1	wi0	1	1/SP						Włączono	
WMM - priorytet głosowy	2	wi0	2	2/SP						Włączono	
WMM - priorytet wideo	3	wi0	3	3/SP						Włączono	
WMM - priorytet wideo	4	wi0	4	4/SP						Włączono	
WMM Best Effort	5	wi0	5	5/SP						Włączono	
WMM – tło	6	wi0	6	6/SP						Włączono	
WMM – tło	7	wi0	7	7/SP						Włączono	
WMM Best Effort	8	wi0	8	8/SP						Włączono	
Kolejka domyślna	33	atm0	1	8/WRR/1	Path0					<input checked="" type="checkbox"/>	
Kolejka TCP ACK	34	atm0	2	7/WRR/1	Path0					<input checked="" type="checkbox"/>	<input type="checkbox"/>

Rysunek 4-41

Naciśnij przycisk „Dodaj” (Rysunek 4-41), aby skonfigurować nową kolejkę na kolejnym ekranie (Rysunek 4-42).

Konfiguracja kolejki QoS

Na tej stronie możesz skonfigurować kolejkę QoS i dodać ją do wybranego interfejsu warstwy 2.

Nazwa:

Włącz:

Interfejs:

Pierwszeństwo kolejki: (niższa wartość oznacza wyższy priorytet)

- Lista pierwszeństwa pokazuje algorytm ustalania kolejności dla każdego poziomu pierwszeństwa.
 - Kolejkom o równym pierwszeństwie będzie nadana kolejność na podstawie algorytmu.
 - Kolejkom o różnym pierwszeństwie będzie nadana kolejność w oparciu o algorytm SP.

Algorytm nadawania kolejności

Weighted Round Robin
 Weighted Fair Queuing

Waga kolejki: [1-63]

Opóźnienie DSL:

Rysunek 4-42

- **Nazwa:** Wprowadź nazwę kolejki
- **Włącz:** Wybierz Włącz, aby kolejka była aktywna
- **Interfejs:** Wybierz interfejs, dla którego obowiązywać ma kolejka
- **Pierwszeństwo kolejki:** Wybierz priorytet dla kolejki QoS

- **Opóźnienie DSL:** Wybierz ścieżkę opóźnienia dla danego typu danych. Dla tego routera dostępna jest tylko opcja Path0.

Po wprowadzeniu warunków, naciśnij przycisk „**Zapisz/Zastosuj**”, aby zatwierdzić wpis. Pojawi się on w tabeli (Rysunek 4-41).

 **Uwaga:**

- 1) Niższa wartość pierwszeństwa oznacza wyższy priorytet w stosunku do pozostałych pakietów.
- 2) Zapisana kolejka QoS zostanie użyta przez klasyfikator, aby odpowiednio przydzielić pakiety przychodzące.

4.4.8.2 Klasyfikacja QoS

Po wybraniu opcji „**Ustawienia zaawansowane**” → „**Quality of Service**” → „**Klasyfikacja QoS**”, możesz skonfigurować dodatkowe reguły dla klasyfikacji QoS.

Reguła składa się z nazwy klasy oraz przynajmniej jednego warunku. Wszystkie z ustalonych warunków muszą zostać spełnione, aby reguła zadziałała.

Konfiguracja klasyfikacji QoS – można skonfigurować maksymalnie 32 reguł.

Aby dodać nową regułę naciśnij przycisk Dodaj.
Aby usunąć reguły zaznacz odpowiednie pola a następnie naciśnij przycisk Usuń.
Naciśnięcie przycisku Włącz spowoduje sprawdzenie wszystkich reguł w tabeli. Reguły z zaznaczonym polem włącz zostaną włączone. Reguły z niezaznaczonym polem włącz zostaną wyłączone.
Pole włącz pokazuje również status każdej reguły po odświeżeniu strony.
Jeżeli funkcja WMM na stronie ustawień bezprzewodowych zostanie wyłączona reguły dotyczące połączeń bezprzewodowych nie będą funkcjonowały

Nazwa klasy	Kolejność	KRYTERIA KLASYFIKACJI											REZULTATY KLASYFIKACJI			Usun			
		Interfejs	EtherType	ŹrMAC/Maska	DocMAC/Maska	ŹrIP/DługośćPrefiks	DocIP/DługośćPrefiks	Proto	ŹrPort	DocPort	DSCP Spr	802.1P Spr	Klucz kolejki	Ozn. DSCP	Ozn. 802.1P		Włącz		
klasa-ftp	1	LAN			00:11:22:33:44:AA										1	AF12		<input checked="" type="checkbox"/>	<input type="checkbox"/>

Rysunek 4-43

Naciśnij przycisk „**Dodaj**” (Rysunek 4-43), aby skonfigurować regułę klasyfikacji QoS.

Reguły nadawania klasy przesyłania danych

Na tym ekranie możesz utworzyć regułę określania klasy przesyłanych danych i nadawania im określonego priorytetu, oraz, opcjonalnie, nadania pakietom oznaczeń priorytetów lub DSCP. Naciśnij przycisk 'Zapisz/Zastosuj' aby zapisać i aktywować regułę.

Nazwa klasy przesyłanych danych:

Porządek reguły:

Status Reguły:

Określ kryteria klasyfikacji (Puste pole oznacza że kryterium nie jest używane do klasyfikacji.)

Interfejs klasy:

Typ ramki Ethernet:

Źródłowy adres MAC:

Źródłowa maska MAC:

Docelowy adres MAC:

Docelowa maska MAC:

Określ reguły klasyfikacji (Puste pole oznacza brak operacji.)

Określ kolejkę klasy (Wymagane):

Nadawanie oznaczeń DSCP (Differentiated Service Code Point):

Nadawanie oznaczeń priorytetu 802.1p:

- Pakiety danej klasy nieoznaczone tagami vlan wychodzące przez interfejs nienależący do żadnej sieci vlan będą oznaczone identyfikatorem VID 0 i bitami priorytetu odpowiednimi dla reguły danej klasy.
- Pakiety danej klasy oznaczone tagami vlan wychodzące przez interfejs nienależący do żadnej sieci vlan będą oznaczone bitami priorytetu odpowiednimi dla reguły danej klasy. Oznaczenia vlan nie zostaną dodane.
- Pakiety danej klasy nieoznaczone tagami vlan wychodzące przez interfejs należący do sieci vlan będą oznaczone identyfikatorem VID odpowiednim dla vlan interfejsu oraz bitami priorytetu odpowiednimi dla reguły danej klasy.
- Pakiety danej klasy oznaczone tagami vlan wychodzące przez interfejs należący do sieci vlan będą dodatkowo oznaczone identyfikatorem VID odpowiednim dla vlan interfejsu oraz bitami priorytetu odpowiednimi dla reguły danej klasy.

Rysunek 4-44

Po wprowadzeniu warunków, naciśnij przycisk „Zapisz/Zastosuj”, aby zatwierdzić wpis.

4.4.9 Kontrola przepustowości

Po wybraniu opcji „Ustawienia zaawansowane” → „Kontrola przepustowości”, możesz włączyć funkcję kontroli przepustowości i ustalić Całkowitą przepustowość wysyłania/pobierania (Rysunek 4-45).

Kontrola przepustowości

Na tej stronie możesz wyłączyć lub włączyć funkcję Kontroli przepustowości. Poniższe ustawienia działają jedynie wtedy, gdy opcja "Włącz Kontrolę przepustowości" jest zaznaczona. Naciśnij przycisk "Zapisz/Zastosuj" aby zapisać ustawienia.

Uwaga:
Jeżeli opcja nie jest zaznaczona, wszystkie wprowadzone reguły Kontroli przepustowości będą nieaktywne.
Jeżeli używasz linii ADSL upewnij się, że całkowita przepustowość wysyłania/pobierania nie jest większa niż prędkość wysyłania/pobierania linii ADSL, inaczej funkcja Kontroli przepustowości może nie działać.

Włącz Kontrolę przepustowości

Typ linii: ADSL Inna

Całkowita przepustowość wysyłania: Kb/s

Całkowita przepustowość pobierania: Kb/s

Rysunek 4-45

- **Włącz Kontrolę przepustowości:** Zaznacz tą opcję, żeby włączyć funkcję Kontroli przepustowości.
- **Całkowita przepustowość wysyłania(Kbps):** Wprowadź prędkość wysyłania na porcie WAN.
- **Całkowita przepustowość pobierania(Kbps):** Wprowadź prędkość pobierania na porcie

WAN.

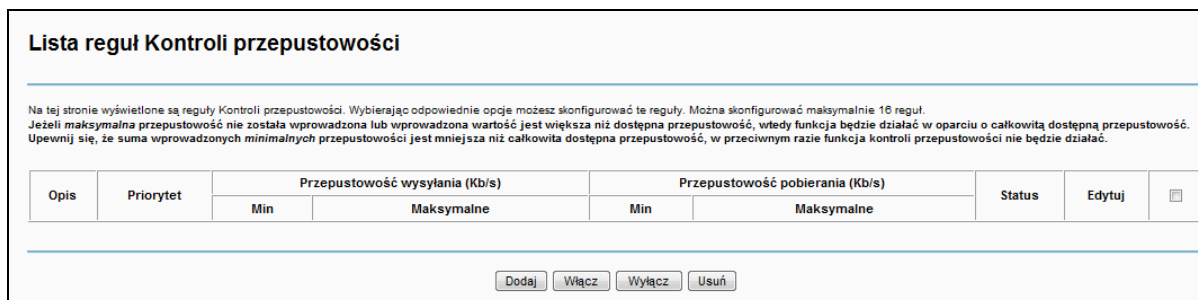
- **Zapisz/Zastosuj:** Naciśnij ten przycisk, żeby zapisać ustawienia.

 **Uwaga:**

Całkowita prędkość wysyłania oraz Całkowita prędkość pobierania muszą być skonfigurowane.

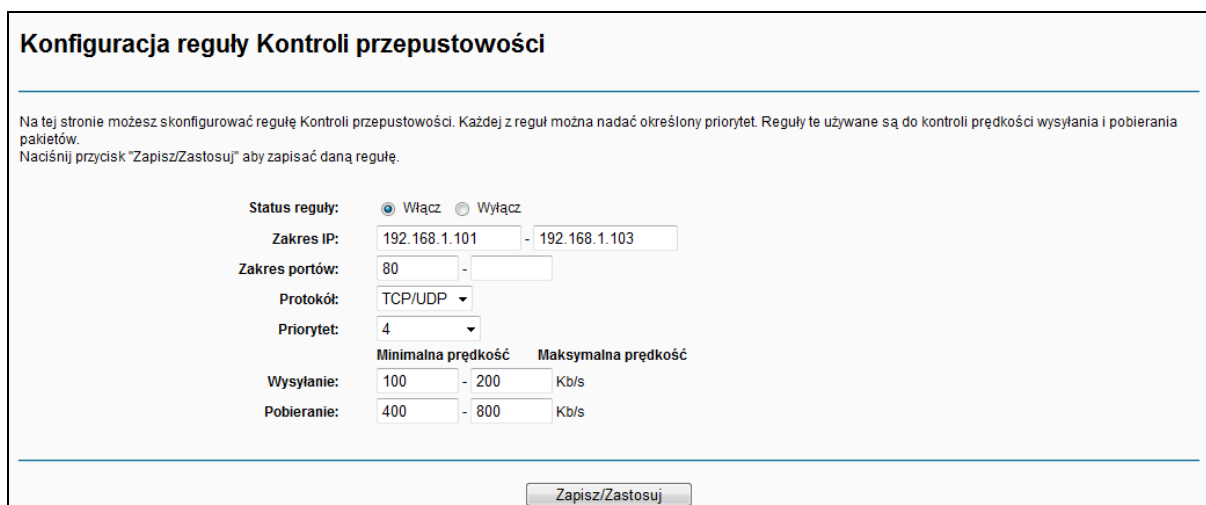
4.4.9.1 Lista reguł

Wybierz opcję „**Ustawienia zaawansowane**” → „**Kontrola przepustowości**” → „**Lista reguł**” w celu dodania lub edycji reguł Kontroli przepustowości (Rysunek 4-46).



Rysunek 4-46

Aby dodać nową regułę, naciśnij przycisk „**Dodaj**”. Pojawi się ekran konfiguracji reguły Kontroli przepustowości (Rysunek 4-47).



Rysunek 4-47

- **Status reguły:** Wybierz odpowiedni status, aby włączyć lub wyłączyć regułę
- **Zakres IP:** Wprowadź pojedynczy adres IP lub zakres adresów IP
- **Zakres portów:** Wprowadź pojedynczy port lub zakres portów
- **Protokół:** Wybierz protokół z listy. Dostępne są protokoły TCP, UDP oraz TCP/UDP.
- **Priorytet:** Wybierz priorytet z listy. Dostępne są opcje: Najwyższy, 1, 2, 3, 4, 5, 6, Najniższy. Domyślnie wybrany jest priorytet 4.
- **Wysyłanie:** Wprowadź minimalną oraz maksymalną prędkość wysyłania przez port WAN.
- **Pobieranie:** Wprowadź minimalną oraz maksymalną prędkość pobierania przez port WAN.

Po zakończeniu konfiguracji, naciśnij przycisk „**Zapisz/Zastosuj**”. Na liście pojawi się nowy wpis (Rysunek 4-48). W celu modyfikacji reguły naciśnij przycisk „**Edytuj**”. Aby usunąć regułę, zaznacz opcję w ostatniej kolumnie i naciśnij przycisk „**Usuń**”.

Lista reguł Kontroli przepustowości								
Opis	Priorytet	Przepustowość wysyłania (Kb/s)		Przepustowość pobierania (Kb/s)		Status	Edytuj	<input type="checkbox"/>
		Min	Maksymalne	Min	Maksymalne			
192.168.1.101-192.168.1.103, 80, TCP/UDP	4	100	200	400	800	Włączona	<input type="button" value="Edytuj"/>	<input type="checkbox"/>

Rysunek 4-48

Uwaga:

Reguły działają na zasadzie przydzielania wolnego pasma. W pierwszej kolejności przydzielane jest ono regułom z najwyższym priorytetem, pozostałe reguły dostają resztę pasma niewykorzystaną przez reguły z wyższym priorytetem. Dla reguł o takim samym priorytecie pasmo dzielone jest według ustalonej dla nich minimalnej prędkości wysyłania/pobierania. Im wyższa minimalna prędkość, tym większą część pasma dostaje reguła.

4.4.10 Routing

Zakładka „**Advanced Setup**”→„**Routing**” zawiera trzy opcje: **Brama domyślna**, **Routing statyczny** oraz **RIP**. Opis każdej z nich znajduje się poniżej.



4.4.10.1 Brama domyślna

Po wybraniu opcji „**Ustawienia zaawansowane**”→„**Routing**”→„**Brama domyślna**” pojawi się ekran konfiguracji Bramy domyślnej (Rysunek 4-49).

Routing -- Brama domyślna

Lista interfejsów bramy domyślnej może zawierać wiele interfejsów WAN, ale w danym momencie używany będzie tylko jeden z połączonych interfejsów o najwyższym priorytecie. Priorytet interfejsów może zostać zmieniony poprzez usunięcie i ponowne dodanie interfejsów.

Wybrane interfejsy bramy domyślnej

ppp0.1

Dostępne interfejsy WAN

Wybierz preferowany interfejs WAN jako domyślną bramę IPv6.

Wybrany interfejs WAN: Brak skonfigurowanych interfejsów

Zapisz/Zastosuj

Rysunek 4-49

4.4.10.2 Routing statyczny

Po wybraniu opcji „**Ustawienia zaawansowane**” → „**Routing**” → „**Routing statyczny**” pojawi się ekran konfiguracji tras statycznych (Rysunek 4-50). Trasa statyczna to predefiniowana ścieżka, którą dane muszą pokonać, aby dotrzeć do określonego hosta lub sieci.

Routing -- dodawanie trasy statycznej

Można skonfigurować maksymalnie 32 wpisy.

Wersja IP	Docelowe IP/Długość prefiksu	Brama	Interfejs	Metryka	Status	Włącz/Wyłącz	Edytuj	Usuń
<p>Dodaj Włącz wszystkie Wyłącz wszystkie Usuń</p>								

Rysunek 4-50

Aby dodać nową trasę statyczną:

- Naciśnij przycisk „**Dodaj**” (Rysunek 4-50), a pojawi się ekran dodawania nowej trasy (Rysunek 4-51).

Routing -- Trasa statyczna Dodaj

Wprowadź adres sieci docelowej, maskę podsieci, bramę I/LUB dostępny interfejs WAN a następnie naciśnij przycisk "Zapisz/Zastosuj" aby dodać wpis do tablicy routingu.

Wersja IP: IPv4

Docelowy adres IP/długość prefiksu: 210.17.155.203

Interfejs: LAN/br0

Adres IP bramy domyślnej: 255.255.255.0

(opcjonalnie: wartość metryki powinna być większa lub równa zero)

Metryka:

Zapisz/Zastosuj

Rysunek 4-51

2. Wprowadź poniższe dane:

Wersja IP: Wybierz wersję protokołu IP.

Docelowy adres IP/długość prefiksu: Docelowy adres IP to adres sieci lub hosta, do którego będzie przypisana statyczna trasa.

Interfejs: Wybierz interfejs z listy. W innym wypadku użyty zostanie interfejs domyślny.

Adres IP bramy domyślnej: Jeżeli jako **Interfejs** wybrany zostanie IPoE lub IPoA, wpisz poprawny Adres IP bramy domyślnej. Drugi z **Interfejsów** automatycznie przyjmie tą wartość jako bramę domyślną.

3. Naciśnij przycisk „**Zapisz/Zastosuj**”, aby zapisać ustawienia. Trasa pojawi się w tabeli (Rysunek 4-50).

Aby usunąć trasę statyczną:

1. Zaznacz opcję **Usuń** w odpowiednim wierszu (Rysunek 4-50).

2. Naciśnij przycisk „**Usuń**”, aby usunąć wpis.

Uwaga:

Jeżeli wybrany został protokół bazujący na IP (IPoE, IPoA), adres IP bramy domyślnej musi być skonfigurowany poprawnie.

4.4.10.3 RIP

Po wybraniu opcji „**Ustawienia zaawansowane**” → „**Routing**” → „**RIP**” pojawi się ekran konfiguracji RIP (Rysunek 4-52).

Routing – Konfiguracja RIP

UWAGA: RIP NIE MOŻE BYĆ SKONFIGUROWANY na interfejsie WAN z aktywnym NAT (np. PPPoE).

Aby włączyć protokół RIP dla interfejsu WAN wybierz określoną wersję i sposób działania RIP i zaznacz pole 'Włączono'. Aby wyłączyć protokół RIP dla interfejsu WAN odznacz pole 'Włączono'. Naciśnij przycisk 'Zapisz/Zastosuj' aby włączyć/wyłączyć RIP i zapisać konfigurację.

Interfejs	Wersja	Działanie	Włączono
atm0.1	2	Pasywny	<input type="checkbox"/>

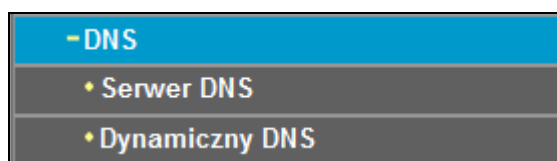
Rysunek 4-52

Uwaga:

RIP nie może zostać skonfigurowany dla usług WAN, które mają włączony NAT (np. PPPoE).

4.4.11 DNS

Jeżeli wybrany typ połączenia WAN to **PPPoE**, **PPPoA** lub **IPoA**, w menu po lewej stronie dostępna będzie zakładka **DNS**. Zawiera ona dwie opcje: **Serwer DNS** oraz **Dynamiczny DNS**.



4.4.11.1 Serwer DNS

Po wybraniu opcji „Ustawienia zaawansowane”→„DNS”→„Serwer DNS” pojawi się ekran **Konfiguracji serwerów DNS** (Rysunek 4-53).

Konfiguracja serwerów DNS

Wybierz serwer DNS jednego z dostępnych interfejsów WAN LUB wprowadź statyczne adresy serwerów DNS. W trybie ATM, jeżeli skonfigurowany jest tylko 1 PVC z protokołem iPoA lub statyczne iPoE, należy wprowadzić statyczne adresy IP serwerów DNS.
Interfejsy DNS mogą korzystać z wielu interfejsów WAN jako serwerów DNS, ale w danym momencie używany będzie tylko jeden z interfejsów o najwyższym priorytecie, jeżeli tylko dany interfejs WAN jest połączony. Priorytet interfejsów może zostać zmieniony poprzez usunięcie i ponowne dodanie interfejsów.

Wybierz interfejs DNS z dostępnych interfejsów WAN:

Wybierz interfejsy - serwery DNS

ppp0.1

Dostępne interfejsy WAN

Użyj następujących statycznych adresów IP serwerów DNS:

Preferowany serwer DNS:

Alternatywny serwer DNS:

Wybierz skonfigurowany interfejs WAN IPv6 jako interfejs DNS lub wprowadź statyczne adresy serwerów DNS IPv6.
Uwaga: wybranie interfejsu WAN IPv6 spowoduje włączenie funkcji Klient DHCPv6 dla tego interfejsu.

Uzyskaj informacje DNS IPv6 z interfejsu WAN:

Wybrany interfejs WAN: BRAK SKONFIGUROWANYCH INTERFEJSÓW

Użyj następujących statycznych adresów DNS IPv6:

Preferowany serwer DNS IPv6:

Alternatywny serwer DNS IPv6:

Zapisz/Zastosuj

Rysunek 4-53

Dla połączeń PPPoA lub PPPoE, zaznacz opcję **Wybierz interfejs DNS z dostępnych interfejsów WAN**. Podczas nawiązywania połączenia, router otrzyma adres serwera DNS z wybranego interfejsu WAN.

Dla połączeń iPoA oraz statycznego protokołu iPoE, zaznacz opcję **Użyj następujących statycznych adresów IP serwerów DNS** i wprowadź adres preferowanego i/lub alternatywnego serwera DNS, otrzymany od dostawcy Internetu.

Możesz również wybrać skonfigurowany interfejs WAN, z którego pobrany zostanie adres IPv6 serwera DNS lub wprowadzić adres IPv6 serwera DNS, otrzymany od dostawcy Internetu.

Naciśnij przycisk „**Zapisz/Zastosuj**”, aby zapisać ustawienia.

4.4.11.2 Dynamiczny DNS

Po wybraniu opcji „**Ustawienia zaawansowane**” → „**DNS**” → „**Dynamiczny DNS**” pojawi się ekran konfiguracji usługi **Dynamiczny DNS** (Rysunek 4-54).

Router umożliwia skonfigurowanie usługi Dynamicznego DNS (**DDNS**). Dynamiczny DNS pozwala na przypisanie dynamicznego adresu IP do statycznego adresu domenowego, co ułatwia dostęp do routera z dowolnego miejsca w Internecie.

Nazwa hosta	Nazwa użytkownika	Usługa	Interfejs	Usuń
-------------	-------------------	--------	-----------	------

Rysunek 4-54

Aby dodać nowy DDNS:

1. Naciśnij przycisk „**Dodaj**” (Rysunek 4-54), a pojawi się ekran dodawania Dynamicznego DNS (Rysunek 4-55).

Dostawca D-DNS: No-IP

Nazwa hosta:

Interfejs: pppoe_0_0_35/ppp0.2

Ustawienia No-IP

Nazwa użytkownika:

Hasło:

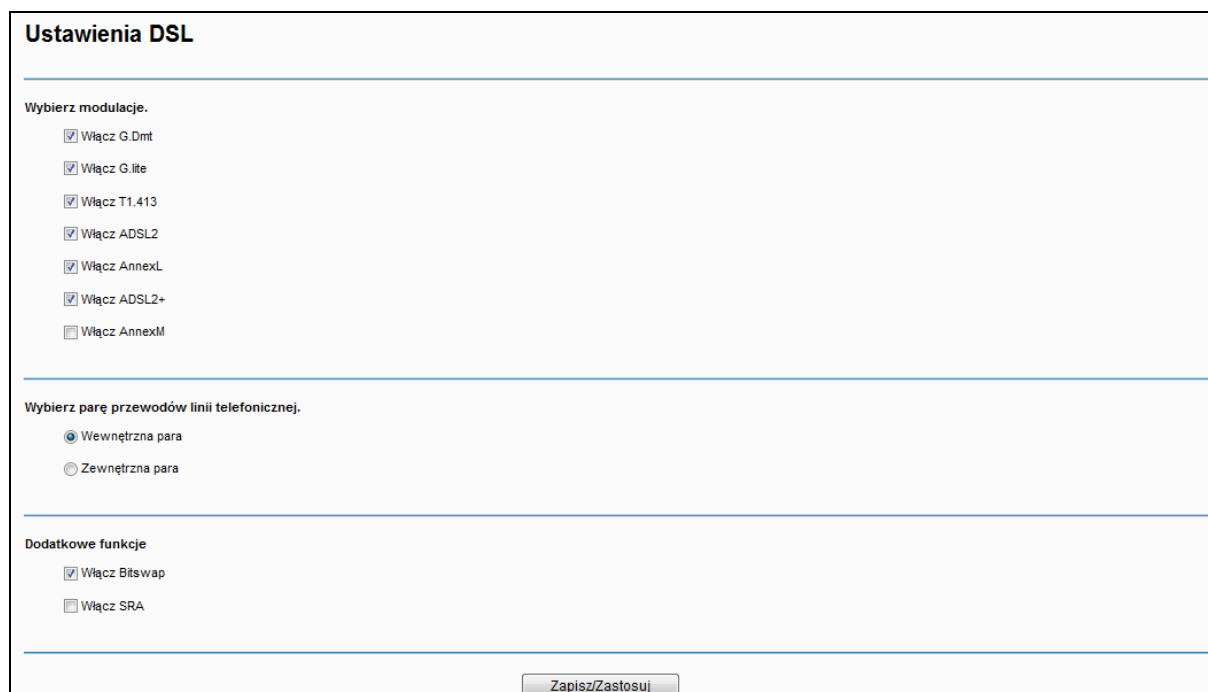
Rysunek 4-55

2. Wybierz **Dostawcę D-DNS** z listy.
3. Wprowadź **Nazwę hosta** dla wybranego serwera oraz wybierz odpowiedni **Interfejs** z listy.
4. Wprowadź **Nazwę użytkownika** oraz **Hasło** do swojego konta DDNS.

Naciśnij przycisk „**Zapisz/Zastosuj**”, aby zapisać ustawienia.

4.4.12 DSL

Po wybraniu opcji „**Ustawienia zaawansowane**”→„**DSL**” pojawi się ekran konfiguracji **Ustawień DSL** (Rysunek 4-56).



The screenshot shows the 'Ustawienia DSL' (DSL Settings) page. It is divided into three sections:

- Wybierz modulacje.** (Choose modulation): A list of checkboxes for different modulation types: Włącz G.Dmt, Włącz G.lite, Włącz T1.413, Włącz ADSL2, Włącz AnnexL, Włącz ADSL2+, and Włącz AnnexM. The first six are checked, and the last one is unchecked.
- Wybierz parę przewodów linii telefonicznej.** (Choose a pair of telephone lines): Two radio buttons: Wewnętrzna para (selected) and Zewnętrzna para (unselected).
- Dodatkowe funkcje** (Additional functions): Two checkboxes: Włącz Bitswap (checked) and Włącz SRA (unchecked).

At the bottom of the page is a button labeled 'Zapisz/Zastosuj' (Save/Apply).

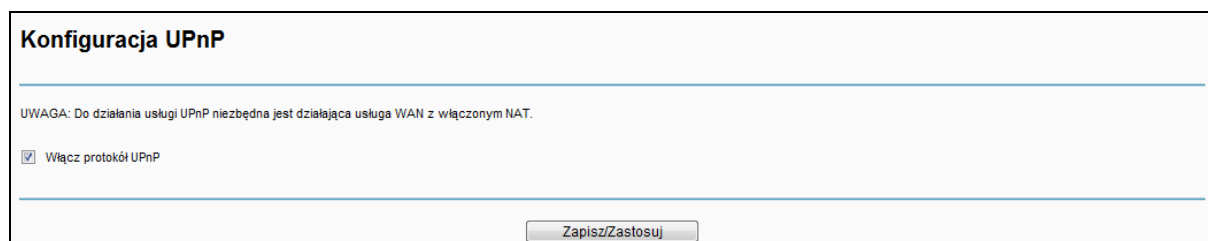
Rysunek 4-56

Możesz wybrać typ modulacji, parę przewodów linii telefonicznej oraz funkcje Bitswap i SRA. Po wybraniu odpowiednich opcji, naciśnij przycisk „**Zapisz/Zastosuj**”, aby zapisać ustawienia.

4.4.13 UPnP

Po wybraniu opcji „**Ustawienia zaawansowane**”→„**UPnP**” pojawi się ekran konfiguracji **Konfiguracji UPnP**. Możesz tutaj włączyć lub wyłączyć protokół UPnP (Universal Plug and Play).

UPnP (Universal Plug and Play) jest architekturą rozproszoną, otwartą i współpracuje z protokołami TCP/IP oraz HTTP. Urządzenie obsługujące UPnP automatycznie łączy się do sieci, pobiera adres IP, przekazuje informacje o swoich usługach i pobiera informacje o innych urządzeniach w sieci. Może również automatycznie rozłączyć się z siecią, kiedy nie jest używane. UPnP obsługiwane jest tylko dla połączeń przewodowych.



The screenshot shows the 'Konfiguracja UPnP' (UPnP Configuration) page. It features a warning message: 'UWAGA: Do działania usługi UPnP niezbędna jest działająca usługa WAN z włączonym NAT.' Below the warning is a single checkbox labeled 'Włącz protokół UPnP', which is checked. At the bottom of the page is a button labeled 'Zapisz/Zastosuj' (Save/Apply).

Rysunek 4-57

Zaznacz opcję **Włącz protokół UPnP** i naciśnij przycisk „**Zapisz/Zastosuj**”, aby włączyć UPnP.

4.4.14 Grupowanie interfejsów

Po wybraniu opcji „Ustawienia zaawansowane” → „Grupowanie interfejsów” pojawi się opcja konfiguracji Grupowania interfejsów. Umożliwia ona przyporządkowanie kilku portów do określonego PVC. Każda grupa działa jako niezależna sieć.

Grupowanie interfejsów

Grupowanie interfejsów umożliwia przyporządkowanie kilku portów do określonego PVC. Każda grupa działa jako niezależna sieć. Aby użyć tej funkcji należy utworzyć grupy przyporządkowania interfejsów zawierające określone interfejsy LAN oraz WAN za pomocą przycisku Dodaj. Przycisk Usuń służy do usuwania interfejsów z grup i dodawania ich do grupy domyślnej. Tylko domyślna grupa posiada interfejs IP. Maksymalnie można utworzyć 16 grup.

Nazwa grupy	Usuń	Interfejs WAN	Interfejsy LAN	Identyfikator DHCP Vendor ID
Domyślne	<input type="checkbox"/>	ppp0.1	LAN1 LAN2 LAN3 WLAN1	

Rysunek 4-58

Aby skorzystać z tej funkcji należy utworzyć grupy przyporządkowania interfejsów, zawierające określone interfejsy LAN oraz WAN za pomocą przycisku „Dodaj”. Przycisk „Usuń” służy do usuwania interfejsów z grup i dodawania ich do grupy domyślnej. Tylko domyślna grupa posiada interfejs IP.

Aby utworzyć nową grupę interfejsów:

1. Naciśnij przycisk „Dodaj”, a pojawi się ekran dodawania nowej grupy (Rysunek 4-59).

Konfiguracja grupowania interfejsów

Aby stworzyć nową grupę interfejsów:

1. Utwórz nazwę grupy (nazwy nie mogą się powtarzać) i wprowadź jej konfigurację zgodnie z punktem 2. (dynamiczna) lub 3. (statyczna) poniżej:
2. Jeżeli chcesz aby określone klienti DHCP po stronie LAN byli automatycznie dodawani do grupy i otrzymywali adresy z interfejsu WAN wprowadź określone identyfikatory DHCP vendor ID. Po wprowadzeniu identyfikatora DHCP vendor ID klient DHCP o określonym identyfikatorze vendor ID (DHCP opcja 80) nie otrzyma adresu z lokalnego serwera DHCP.
3. Wybierz interfejsy z listy dostępnych interfejsów i dodaj je do listy zgrupowanych interfejsów z użyciem przycisków-strzałek aby przyporządkować określone porty do grupy.
Uwaga: Tacy klienci mogą otrzymywać publiczne adresy IP
4. Naciśnij przycisk Zapisz/Zastosuj aby ustawienia zostały w życie
UWAGA Po wprowadzeniu identyfikatora vendor ID dla danego urządzenia, należy ZRESTARTOWAĆ to urządzenie aby umożliwić mu otrzymanie odpowiedniego adresu IP.

Nazwa grupy:

Interfejs WAN:

Zgrupowane interfejsy LAN

Dostępne interfejsy LAN

LAN1
LAN2
LAN3
WLAN1

Automatycznie dodawaj klientów o następujących identyfikatorach DHCP Vendor ID

Rysunek 4-59

2. Wprowadź nazwę grupy. Nazwy nie mogą się powtarzać.

Uwaga:

Jeżeli chcesz, aby określone klienci DHCP po stronie LAN byli automatycznie dodawani do grupy i otrzymywali adresy z interfejsu WAN, wprowadź określone identyfikatory DHCP vendor ID. Po wprowadzeniu identyfikatora DHCP vendor ID, klient DHCP o określonym identyfikatorze vendor ID (DHCP opcja 60) nie otrzyma adresu z lokalnego serwera DHCP.

- Wybierz interfejs z listy dostępnych interfejsów i dodaj je do listy zgrupowanych interfejsów, z użyciem przycisków-strzałek, aby przyporządkować określone porty do grupy.

Uwaga:

Tacy klienci mogą otrzymywać publiczne adresy IP.

- Naciśnij przycisk „**Zapisz/Zastosuj**”, aby ustawienia weszły w życie.

Uwaga:

Po wprowadzeniu identyfikatora vendor ID dla danego urządzenia, należy **ZRESTARTOWAĆ** to urządzenie, aby umożliwić mu otrzymanie odpowiedniego adresu IP.

4.4.15 Tunel IP

Tunelowanie IP pozwala hostom obsługującym tylko IPv6 dostęp do usług IPv4 oraz umożliwia odizolowanym hostom IPv6 na komunikację poprzez sieć IPv4. Jest to tymczasowe rozwiązanie dla sieci, które nie posiadają możliwości równoległej, niezależnej pracy sieci IPv4 i IPv6.

Zakładka „**Ustawienia zaawansowane**” → „**Tunel IP**” zawiera dwie opcje: **IPv6 w IPv4** oraz **IPv4 w IPv6**.

4.4.15.1 IPv6 w IPv4

Po wybraniu opcji „**Ustawienia zaawansowane**” → „**Tunel IP**” → „**IPv6 w IPv4**” pojawi się ekran **konfiguracji tunelu 6do4**, który pozwala na skonfigurowanie statycznych tras (Rysunek 4-60).

Tunelowanie IP – konfiguracja tunelu 6do4

Nazwa	WAN	LAN	Dynamiczna	Długość maski IPv4	Prefiks 6rd	Adres przekaźnika brzegowego	Usuń
<input type="button" value="Dodaj"/> <input type="button" value="Usuń wszystkie"/> <input type="button" value="Usuń"/>							

Rysunek 4-60

Naciśnij przycisk „**Dodaj**” (Rysunek 4-60), aby dodać nowy tunel. Pojawi się ekran **konfiguracji tunelu 6w4** (Rysunek 4-61).

Tunelowanie IP -- konfiguracja tunelu 6w4

Aktualnie obsługiwana jest tylko konfiguracja 6rd.

Nazwa tunelu:

Mechanizm: 6RD

Powiązany interfejs WAN:

Powiązany interfejs LAN: LAN/br0

Ręczna Automatyczna

Długość maski IPv4:

Prefiks 6rd z długością prefiksu:

Adres IPv4 przekaźnika sieciowego:

Zapisz/Zastosuj

Rysunek 4-61

- **Mechanizm:** 6RD, używany jest gdy połączenie WAN używa IPv4, a sieć LAN używa IPv6.
- **Powiązany interfejs WAN:** Wybierz interfejs WAN z listy. Tylko aktualnie podłączone interfejsy będą znajdować się na liście.
- **Powiązany interfejs LAN:** Wybierz interfejs LAN z listy. Tylko aktualnie podłączone interfejsy będą znajdować się na liście.
- **Długość maski IPv4:** Długość maski IPv4 wybranego interfejsu WAN.
- **Prefiks 6rd z długością prefiksu:** Długość prefiksu 6rd.
- **Adres IPv4 przekaźnika sieciowego:** Adres IPv4 przekaźnika sieciowego tunelu 6RD.

Naciśnij przycisk „Zapisz/Zastosuj”, aby zapisać ustawienia.

 **Uwaga:**

Dla tego typu tunelu nie powinno być żadnych połączeń WAN IPv6. Jeżeli istnieją połączenia WAN IPv6, zostanie wyświetlony komunikat o konieczności ich usunięcia przed stworzeniem tunelu.

4.4.15.2 IPv4 w IPv6

Po wybraniu opcji „Ustawienia zaawansowane” → „Tunel IP” → „IPv4 w IPv6” pojawi się ekran **konfiguracji tunelu 4do6**, który pozwala na skonfigurowanie statycznych tras (Rysunek 4-62).

Tunelowanie IP – konfiguracja tunelu 4do6

Nazwa	WAN	LAN	Dynamiczna	AFTR	Usuń

Dodaj Usuń wszystkie Usuń

Rysunek 4-62

Naciśnij przycisk „Dodaj” (Rysunek 4-62), aby dodać nowy tunel. Pojawi się ekran **konfiguracji tunelu 4w6** (Rysunek 4-63).

Tunelowanie IP -- konfiguracja tunelu 4w6

Aktualnie obsługiwane są jedynie tunele DS-Lite.

Nazwa tunelu:

Mechanizm: DS-Lite

Powiązany interfejs WAN:

Powiązany interfejs LAN: LAN/br0

Ręcznie Automatycznie

AFTR:

Rysunek 4-63

- **Mechanizm:** DS-Lite, używany jest gdy połączenie WAN używa IPv6, a sieć LAN używa IPv4.
- **Powiązany interfejs WAN:** Wybierz interfejs WAN z listy. Tylko aktualnie podłączone interfejsy będą znajdować się na liście.
- **Powiązany interfejs LAN:** Wybierz interfejs LAN z listy. Tylko aktualnie podłączone interfejsy będą znajdować się na liście.
- **AFTR:** Wprowadź adres IPv6 lokalizacji zdalnej.

Naciśnij przycisk „**Zapisz/Zastosuj**”, aby zapisać ustawienia.

Uwaga:

Dla tego typu tunelu nie powinno być żadnych połączeń WAN IPv4. Jeżeli istnieją połączenia WAN IPv4, zostanie wyświetlony komunikat o konieczności ich usunięcia przed stworzeniem tunelu.

4.4.16 IPSec

Po wybraniu opcji „**Ustawienia zaawansowane**” → „**IPSec**” pojawi się ekran konfiguracji **tunelów IPSec**. Na tej stronie możesz dodawać, usuwać, włączać oraz wyłączać połączenia tunelowe IPSec (Rysunek 4-64).

Połączenia tunelowe IPSec

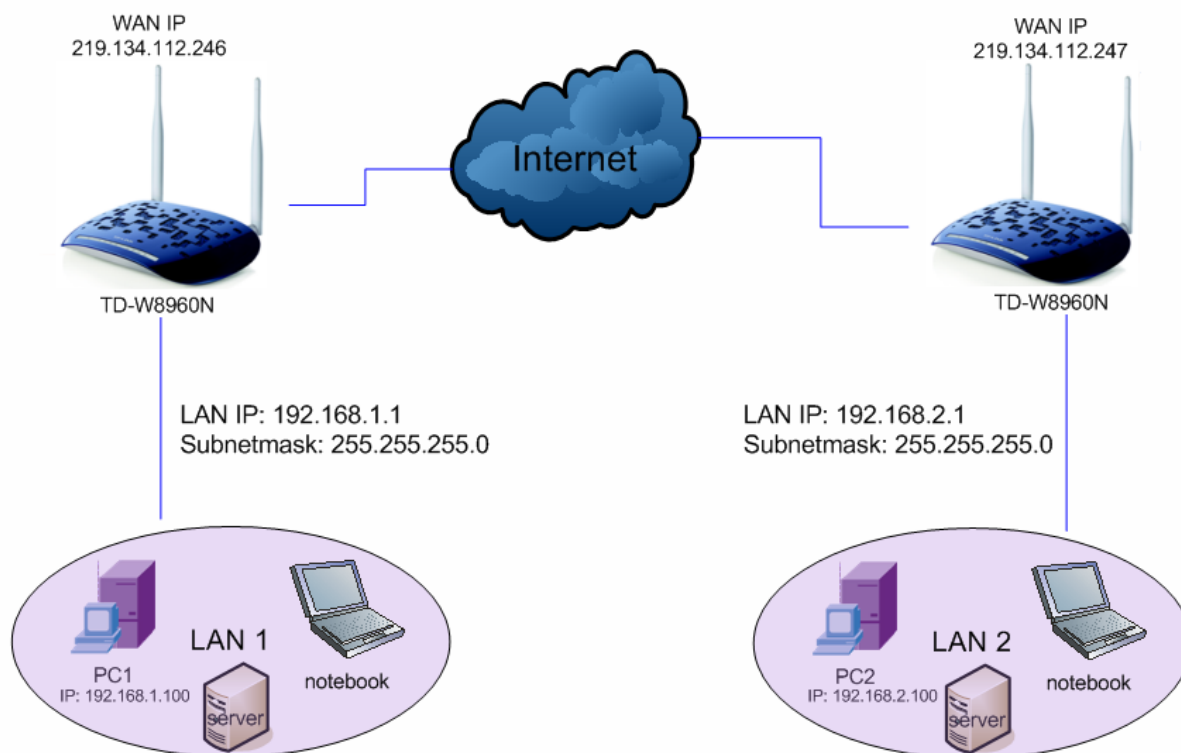
Na tej stronie możesz dodawać, usuwać, włączać oraz wyłączać połączenia tunelowe IPSec.

DPD (Dead Peer Detection) (Uwaga! Może powodować niestabilność transmisji)

Nazwa połączenia	Brama zdalna	Adresy lokalne	Adresy zdalne	Status	Włącz/Wyłącz	Edytuj	Usuń
<input type="button" value="Dodaj nowe połączenie"/> <input type="button" value="Włącz wszystkie"/> <input type="button" value="Wybierz wszystkie"/> <input type="button" value="Usuń"/>							

Rysunek 4-64

Poniższa sekcja przedstawia tworzenie tunelu pomiędzy dwoma TD-W8960N. Topologia sieci przedstawiona jest na rysunku:



Uwaga:

Możesz również użyć innych routerów VPN do zestawienia tunelu z TD-W8960N. TD-W8960N obsługuje do 10 połączeń VPN jednocześnie.

Naciśnij przycisk „**Dodaj nowe połączenie**”, a pojawi się ekran Ustawień IPsec (Rysunek 4-65).

Ustawienia IPsec

Nazwa połączenia IPsec:	<input type="text" value="nowe połączenie"/>
Adres zdalnej bramy IPsec (URL/IPv4):	<input type="text" value="0.0.0.0"/>
Dostęp tunelowany z lokalnych adresów IP:	<input type="text" value="Podsieć"/>
Adres IP VPN:	<input type="text" value="0.0.0.0"/>
Maska podsieci:	<input type="text" value="255.255.255.0"/>
Dostęp tunelowany dla zdalnych adresów IP:	<input type="text" value="Podsieć"/>
Adres IP VPN:	<input type="text" value="0.0.0.0"/>
Maska podsieci:	<input type="text" value="255.255.255.0"/>
Tryb wymiany kluczy:	<input type="text" value="Automatyczna(IKE)"/>
Tryb uwierzytelniania:	<input type="text" value="Klucz współdzielony"/>
Klucz współdzielony:	<input type="text" value="klucz"/>
PFS (Perfect Forward Secrecy):	<input type="text" value="Wyłącz"/>
Zaawansowane ustawienia IKE:	<input type="button" value="Pokaż ustawienia zaawansowane"/>

Rysunek 4-65

- **Nazwa połączenia IPsec:** Wprowadź nazwę dla VPN.
- **Adres zdalnej bramy IPsec (URL/IPv4):** Wprowadź adres IP docelowej bramy. Będzie to adres WAN IP lub adres domenowy routera z drugiej strony tunelu.

- **Dostęp tunelowy z lokalnych adresów IP:** Wybierz **Podsiec** jeżeli chcesz dołączyć do VPN całą sieć lokalną lub **Pojedynczy adres**, jeżeli chcesz dołączyć do VPN tylko jedno urządzenie.
- **Adres IP VPN:** Wprowadź adres IP LAN (np. Wpisz **192.168.1.1** dla **Routera1**, **192.168.2.1** dla **Routera2**).
- **Maska podsieci:** Wprowadź maskę podsieci sieci lokalnej (np. Wpisz **255.255.255.0** dla **Routera1** i **Routera2**).
- **Dostęp tunelowy dla zdalnych adresów IP:** Wybierz **Podsiec** jeżeli chcesz dołączyć do VPN całą sieć lokalną zdalnej lokalizacji lub **Pojedynczy adres** jeżeli chcesz dołączyć do VPN tylko jedno urządzenie.
- **Adres IP VPN:** Wprowadź adres IP LAN zdalnej lokalizacji (np. Wpisz **192.168.2.1** dla **Routera1**, **192.168.1.1** dla **Routera2**).
- **Maska podsieci:** Wprowadź maskę podsieci sieci lokalnej zdalnej lokalizacji (np. Wpisz **255.255.255.0** dla **Routera1** i **Routera2**).
- **Tryb wymiany kluczy:** Wybierz **Automatyczna (IKE)** lub **Ręczna**.
- **Tryb uwierzytelniania:** Wybierz **Klucz współdzielony** (zalecane).
- **Klucz współdzielony:** Wprowadź klucz uwierzytelniania (np. 12345678).
- **PFS (Perfect Forward Secrecy):** PFS to dodatkowy protokół zabezpieczeń.

Zalecane jest pozostawienie wartości domyślnych dla ustawień zaawansowanych.

Po skonfigurowaniu połączenia i naciśnięciu przycisku „**Zapisz/Zastosuj**” na obydwu routerach, urządzenia z LAN1 będą mogły komunikować się z urządzeniami z LAN2 (np. możesz wysłać ping na adres lokalny PC2 z PC1).

Uwaga:

Serwery VPN na obydwu końcach tunelu muszą używać tych samych kluczy uwierzytelniania i ustawień PFS.

Naciśnij przycisk „**Pokaż ustawienia zaawansowane**”, aby skonfigurować ustawienia zaawansowane.

Zaawansowane ustawienia IKE:		Ukryj ustawienia zaawansowane
Faza 1	Tryb:	Główny
	Typ lokalnego identyfikatora:	Lokalny adres Wan IP
	Lokalny identyfikator:	
	Typ zdalnego identyfikatora:	Zdalny adres Wan IP
	Zdalny identyfikator:	
	Algorytm szyfrowania:	3DES
	Algorytm integralności:	MD5
	Wybierz grupę Diffiego-Hellmana dla wymiany kluczy:	1024bit
	Czas życia klucza:	3600 Sekund
Faza 2	Algorytm szyfrowania:	3DES
	Algorytm integralności:	MD5
	Czas życia klucza:	3600 Sekund

- **Tryb Główny:** Wybierz Tryb Główny, aby skonfigurować parametry negocjacji fazy 1 IKE.
- **Tryb Agresywny:** Wybierz Tryb Agresywny, aby skonfigurować parametry negocjacji fazy 1 IKE i skrócić czas negocjacji (niezalecane – jest to mniej bezpieczne).

 **Uwaga:**

Różnica pomiędzy trybami polega na tym, że tryb agresywny przekazuje więcej informacji w mniejszej ilości pakietów, co zwiększa prędkość nawiązania połączenia kosztem zmniejszenia bezpieczeństwa transmisji. Przy korzystaniu z trybu agresywnego grupa Diffiego-Hellmana oraz PFS nie będą negocjowane, przez co konfiguracja tych parametrów na obydwu routerach musi być taka sama.

➤ **Czas życia klucza:**

Wprowadź czas utrzymywania połączenia w sekundach. Jest to czas, który musi upłynąć przed ustanowieniem nowego powiązania IPsec z punktem zdalnym. Domyślna wartość to 3600 sekund.

 **Uwaga:**

Jeżeli zmienisz domyślne wartości ustawień zaawansowanych, upewnij się, że obydwa serwery VPN używają takiego samego **Algorytmu szyfrowania**, **Algorytmu integralności**, **Grupy Diffiego-Hellmana** oraz **Czasu życia klucza dla Fazy 1 i Fazy 2**.

4.4.17 Multicast

Po wybraniu opcji „**Ustawienia zaawansowane**” → „**Multicast**” pojawi się ekran konfiguracji **Konfiguracji IGMP**.

Konfiguracja IGMP

Poniżej znajdują się parametry konfiguracyjne usługi IGMP.

Domyślna wersja:	<input type="text" value="3"/>
Interwał kwerendy:	<input type="text" value="125"/>
Interwał odpowiedzi na kwerendę:	<input type="text" value="10"/>
Interwał kwerendy ostatniego członka grupy:	<input type="text" value="10"/>
Zmienna niezawodności:	<input type="text" value="2"/>
Maksymalna ilość grup multicast:	<input type="text" value="25"/>
Maksymalna liczba źródeł multicast dla IGMPv3 : (1 - 24):	<input type="text" value="10"/>
Maksymalna ilość członków grup Multicast:	<input type="text" value="25"/>
Włącz szybkie opuszczanie:	<input checked="" type="checkbox"/>
Włącz multicast LAN to LAN (Intra LAN):	<input type="checkbox"/>

Rysunek 4-66

Naciśnij przycisk „**Zapisz/Zastosuj**”, aby zapisać ustawienia.

4.5 Sieć bezprzewodowa

Zakładka „**Sieć bezprzewodowa**” zawiera siedem opcji. Opis każdej z nich znajduje się poniżej.



4.5.1 Podstawowe

Po wybraniu opcji „**Sieć bezprzewodowa**”→„**Podstawowe**” pojawi się ekran konfiguracji ustawień podstawowych (Rysunek 4-67).

Sieć bezprzewodowa -- Ustawienia podstawowe

Na tej stronie możesz skonfigurować podstawowe ustawienia sieci bezprzewodowej. Możesz włączyć lub wyłączyć sieć bezprzewodową, ukryć rozgłaszanie nazwy sieci, zmienić nazwę sieci bezprzewodowej (nazywaną też SSID) oraz dostosować parametry sieci zgodnie z wymaganiami prawnymi kraju w którym używany jest router. Naciśnij przycisk "Zapisz/Zastosuj" aby zapisać konfigurację.

Włącz sieć bezprzewodową
 Wyłącz rozgłaszanie SSID
 Izolacja Klientów

SSID1:
BSSID: 02:10:18:01:00:01
Kraj:

Rysunek 4-67

Na tej stronie możesz skonfigurować podstawowe ustawienia sieci WiFi routera, takie jak nazwa sieci bezprzewodowej, rozgłaszanie nazwy sieci bezprzewodowej oraz wybrać dostępne kanały sieci bezprzewodowej, ustawiając odpowiedni kraj. Możesz również włączyć lub wyłączyć sieć bezprzewodową.

- **Włącz sieć bezprzewodową:** Aby korzystać z WiFi, opcja ta musi być zaznaczona. Po jej odznaczeniu wszystkie poniższe ustawienia będą nieaktywne.
- **Wyłącz rozgłaszanie SSID:** Zaznacz tą opcję, aby ukryć nazwę sieci bezprzewodowej.
- **Izolacja klientów:** Zaznacz tą opcję, aby urządzenia podłączone do sieci bezprzewodowej nie mogły komunikować się między sobą.
- **SSID:** Nazwa sieci bezprzewodowej musi być identyczna na wszystkich urządzeniach podłączonych do sieci WiFi. Nazwa nie może przekraczać 32 znaków. Wielkość liter ma znaczenie.
- **BSSID:** Adres MAC interfejsu WiFi routera.
- **Kraj:** Wybór kraju warunkuje dostępne kanały i moc nadawania sieci bezprzewodowej.

Naciśnij przycisk „**Zapisz/Zastosuj**”, aby zapisać ustawienia.

4.5.2 Zabezpieczenia

Po wybraniu opcji „Sieć beprzewodowa” → „Zabezpieczenia” pojawi się ekran konfiguracji zabezpieczeń sieci bezprzewodowej (Rysunek 4-68). Możesz skonfigurować zabezpieczenia ręcznie lub skorzystać z opcji WPS.

Sieć bezprzewodowa -- Zabezpieczenia

Na tej stronie możesz skonfigurować zabezpieczenia sieci bezprzewodowej routera.
Możesz skonfigurować zabezpieczenia ręcznie lub nawiązać zabezpieczone połączenie używając przycisku WPS

WPS

Włącz WPS:

Połącz Urządzenie (Funkcja ta jest dostępna tylko jeżeli wybrane są następujące typy zabezpieczeń: WPA-PSK, WPA2-PSK lub Otwarte)

Przycisk
 PIN

PIN urządzenia: [Pomoc](#)

Ręczna konfiguracja

Aby zabezpieczyć sieć przed niepożądanymi użytkownikami zalecane jest wybranie jednego z dostępnych typów zabezpieczeń. Poniżej możesz skonfigurować typ uwierzytelniania, szyfrowanie, określić klucz wymagany do połączenia z siecią oraz ustalić siłę szyfrowania.

Uwaga: nie zalecamy używania szyfrowania WEP jeżeli router pracuje w trybie 11n. Maksymalna prędkość transmisji przy użyciu szyfrowania WEP spada do 54Mb/s.

Wskazówka: Tryb Tylko 11n nie jest obsługiwany kiedy szyfrowanie WEP jest "Włączone" lub kiedy typ szyfrowania WPA to "TKIP".

Wskazówka: "Szyfrowanie WPA" nie może być ustawione w tryb "TKIP" jeżeli urządzenie działa w trybie 11n.

Po zakończeniu naciśnij przycisk "Zapisz/Zastosuj".

Typ uwierzytelniania:

Hasło: (nazywane też kluczem sieciowym)
[Kliknij aby wyświetlić](#)
 (Możesz wprowadzić od 8 do 63 znaków ASCII lub 64 znaków szesnastkowych.)

Interwał aktualizacji klucza WPA grupy: (opcjonalnie)

Szyfrowanie WPA:

Szyfrowanie WEP:

Rysunek 4-68

4.5.2.1 Ustawienia WPS

Poniższa sekcja przeprowadzi cię przez dodawanie nowego urządzenia do sieci, przy użyciu funkcji **WPS (QSS)**.

Uwaga:

- 1) Opcja ta dostępna jest dla trybów zabezpieczeń: Otwarte, WPA-Personal, WPA2-Personal oraz Mieszany WPA2/WPA-PSK Personal.
- 2) Aby nawiązać połączenie, należy skonfigurować WPS na urządzeniu, które będzie dodane do sieci.

I. Za pomocą przycisku

Jeżeli adapter WiFi obsługuje połączenie za pomocą przycisku, zaznacz opcję **Przycisk** (Rysunek 4-69).

Sieć bezprzewodowa -- Zabezpieczenia

Na tej stronie możesz skonfigurować zabezpieczenia sieci bezprzewodowej routera.
Możesz skonfigurować zabezpieczenia ręcznie lub nawiązać zabezpieczone połączenie używając przycisku WPS

WPS

Włącz WPS:

Połącz Urządzenie (Funkcja ta jest dostępna tylko jeżeli wybrane są następujące typy zabezpieczeń: WPA-PSK, WPA2-PSK lub Otwarte)

Przycisk
 PIN

 [Pomoc](#)

PIN urządzenia:

Ręczna konfiguracja

Aby zabezpieczyć sieć przed niepożądanymi użytkownikami zalecane jest wybranie jednego z dostępnych typów zabezpieczeń. Poniżej możesz skonfigurować typ uwierzytelniania, szyfrowanie, określić klucz wymagany do połączenia z siecią oraz ustalić siłę szyfrowania.

Uwaga: nie zalecamy używania szyfrowania WEP jeżeli router pracuje w trybie 11n. Maksymalna prędkość transmisji przy użyciu szyfrowania WEP spada do 54Mb/s.

Wskazówka: Tryb Tylko 11n nie jest obsługiwany kiedy szyfrowanie WEP jest "Włączone" lub kiedy typ szyfrowania WPA to "TKIP".
Wskazówki: "Szyfrowanie WPA" nie może być ustawione w tryb "TKIP" jeżeli urządzenie działa w trybie 11n.
Po zakończeniu naciśnij przycisk "Zapisz/Zastosuj".

Typ uwierzytelniania:

Hasło: (nazywane też kluczem sieciowym)

[Kliknij aby wyświetlić](#)
(Możesz wprowadzić od 8 do 63 znaków ASCII lub 64 znaków szesnastkowych.)

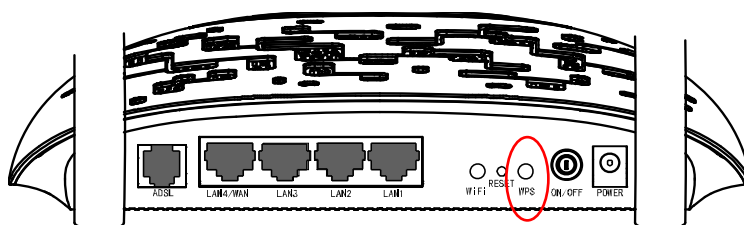
Interwał aktualizacji klucza WPA grupy: (opcjonalnie)

Szyfrowanie WPA:

Szyfrowanie WEP:

Rysunek 4-69

Krok 1: Naciśnij przycisk WPS znajdujący się z tyłu routera.



Krok 2: Naciśnij i przytrzymaj około 2 sekund przycisk WPS na adapterze WiFi.



II. Za pomocą kodu PIN

Jeżeli adapter obsługuje WPS za pomocą kodu PIN, możesz skorzystać z poniższej metody.

Sposób pierwszy: Wprowadź kod PIN adaptera na routerze.

Krok 1: Zaznacz opcję **PIN** i wprowadź kod PIN adaptera, a następnie naciśnij przycisk „**Dodaj urządzenie**” (Rysunek 4-70).

Sieć bezprzewodowa -- Zabezpieczenia

Na tej stronie możesz skonfigurować zabezpieczenia sieci bezprzewodowej routera.
Możesz skonfigurować zabezpieczenia ręcznie lub nawiązać zabezpieczone połączenie używając przycisku WPS

WPS

Włącz WPS:

Połącz Urządzenie (Funkcja ta jest dostępna tylko jeżeli wybrane są następujące typy zabezpieczeń: WPA-PSK, WPA2-PSK lub Otwarte)

Przycisk PIN

[Pomoc](#)

PIN urządzenia: [Pomoc](#)

Ręczna konfiguracja

Aby zabezpieczyć sieć przed niepowołanymi użytkownikami zalecane jest wybranie jednego z dostępnych typów zabezpieczeń.
Poniżej możesz skonfigurować typ uwierzytelniania, szyfrowanie, określić klucz wymagany do połączenia z siecią oraz ustalić siłę szyfrowania.
Uwaga: nie zalecamy używania szyfrowania WEP, jeżeli router pracuje w trybie 11n. Maksymalna prędkość transmisji przy użyciu szyfrowania WEP spada do 54Mb/s.
Wskazówka: Tryb Tylko 11n nie jest obsługiwany kiedy szyfrowanie WEP jest "Włączone" lub kiedy typ szyfrowania WPA to "TKIP".
Wskazówka: "Szyfrowanie WPA" nie może być ustawione w tryb "TKIP" jeżeli urządzenie działa w trybie 11n.
Po zakończeniu naciśnij przycisk "Zapisz/Zastosuj".

Typ uwierzytelniania:

Hasło: (nazywane też kluczem sieciowym)
[Kliknij aby wyświetlić](#)
(Możesz wprowadzić od 8 do 63 znaków ASCII lub 64 znaków szesnastkowych.)

Interwał aktualizacji klucza WPA grupy: (opcjonalnie)

Szyfrowanie WPA:

Szyfrowanie WEP:

Rysunek 4-70

Uwaga:

Kod PIN adaptera powinien znajdować się na urządzeniu.

Krok 2: Przy konfiguracji WPS adaptera WiFi wybierz opcję wprowadzenia kodu PIN na routerze.

Sposób drugi: Wprowadź kod PIN routera na adapterze.

Sprawdź kod PIN wygenerowany przez router. Możesz nacisnąć przycisk „**Generuj nowy PIN**”, w celu wygenerowania nowego kodu.

Sieć bezprzewodowa -- Zabezpieczenia

Na tej stronie możesz skonfigurować zabezpieczenia sieci bezprzewodowej routera.
Możesz skonfigurować zabezpieczenia ręcznie lub nawiązać zabezpieczone połączenie używając przycisku WPS

WPS

Włącz WPS:

Połącz Urządzenie(Funkcja ta jest dostępna tylko jeżeli wybrane są następujące typy zabezpieczeń: WPA-PSK, WPA2-PSK lub Otwarte)

Przycisk PIN

PIN urządzenia: [Pomoc](#)

Ręczna konfiguracja

Aby zabezpieczyć sieć przed niepowołanymi użytkownikami zalecane jest wybranie jednego z dostępnych typów zabezpieczeń.
Poniżej możesz skonfigurować typ uwierzytelniania, szyfrowanie, określić klucz wymagany do połączenia z siecią oraz ustalić siłę szyfrowania.
Uwaga: nie zalecamy używania szyfrowania WEP jeżeli router pracuje w trybie 11n. Maksymalna prędkość transmisji przy użyciu szyfrowania WEP spada do 54Mb/s.
Wskazówka: Tryb Tylko 11n nie jest obsługiwany kiedy szyfrowanie WEP jest "Włączone" lub kiedy typ szyfrowania WPA to "TKIP".
Wskazówka: "Szyfrowanie WPA" nie może być ustawione w tryb "TKIP" jeżeli urządzenie działa w trybie 11n.
Po zakończeniu naciśnij przycisk "Zapisz/Zastosuj".

Typ uwierzytelniania:

Hasło: (nazywane też kluczem sieciowym)
[Kliknij aby wyświetlić](#)
(Możesz wprowadzić od 8 do 63 znaków ASCII lub 64 znaków szesnastkowych.)

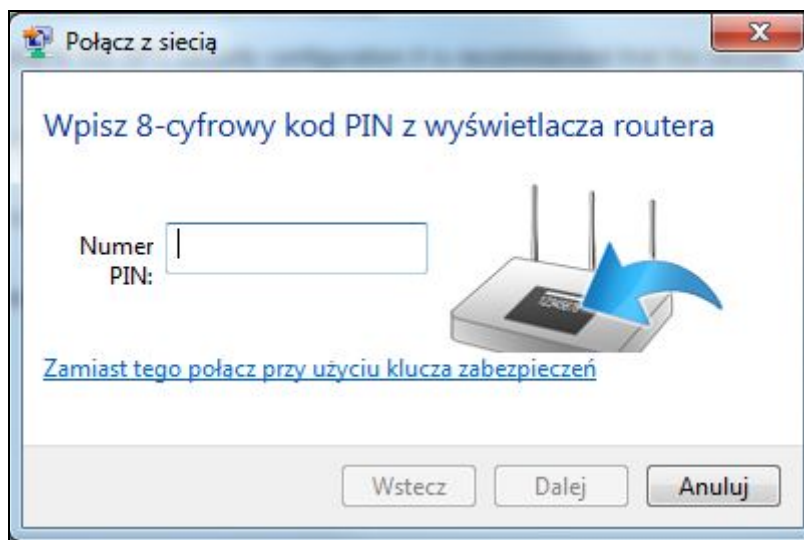
Interwał aktualizacji klucza WPA grupy: (opcjonalnie)

Szyfrowanie WPA:

Szyfrowanie WEP:

Rysunek 4-71

Przy łączeniu adaptera wprowadź kod PIN routera, a następnie naciśnij przycisk „**Dalej**”.



Rysunek 4-72. Screen z łączenia wps z pinem

4.5.2.2 Ręczna konfiguracja

Możesz tutaj ręcznie skonfigurować zabezpieczenia sieci bezprzewodowej: typ uwierzytelniania oraz rodzaj i siłę szyfrowania klucza zabezpieczeń.

Sieć bezprzewodowa -- Zabezpieczenia

Na tej stronie możesz skonfigurować zabezpieczenia sieci bezprzewodowej routera.
Możesz skonfigurować zabezpieczenia ręcznie lub nawiązać zabezpieczone połączenie używając przycisku WPS

WPS

Włącz WPS:

Połącz Urządzenie(Funkcja ta jest dostępna tylko jeżeli wybrane są następujące typy zabezpieczeń: WPA-PSK, WPA2-PSK lub Otwarte)

Przycisk PIN

PIN urządzenia: [Pomoc](#)

Ręczna konfiguracja

Aby zabezpieczyć sieć przed niepowołanymi użytkownikami zalecane jest wybranie jednego z dostępnych typów zabezpieczeń. Poniżej możesz skonfigurować typ uwierzytelniania, szyfrowanie, określić klucz wymagany do połączenia z siecią oraz ustalić siłę szyfrowania.

Uwaga: nie zalecamy używania szyfrowania WEP jeżeli router pracuje w trybie 11n. Maksymalna prędkość transmisji przy użyciu szyfrowania WEP spada do 54Mb/s.

Wskazówka: Tryb Tylko 11n nie jest obsługiwany kiedy szyfrowanie WEP jest "Włączone" lub kiedy typ szyfrowania WPA to "TKIP".
Wskazówka: "Szyfrowanie WPA" nie może być ustawione w tryb "TKIP" jeżeli urządzenie działa w trybie 11n.
Po zakończeniu naciśnij przycisk "Zapisz/Zastosuj".

Typ uwierzytelniania:

Hasło: (nazywane też kluczem sieciowym)
[Kliknij aby wyświetlić](#)
(Możesz wprowadzić od 8 do 63 znaków ASCII lub 64 znaków szesnastkowych.)

Interwał aktualizacji klucza WPA grupy: (opcjonalnie)

Szyfrowanie WPA:

Szyfrowanie WEP:

Rysunek 4-73

- **Typ uwierzytelniania:** Wybierz typ uwierzytelniania z listy. Dostępne są: Otwarty, Współdzielony, WPA-Enterprise, WPA-Personal, WPA2-Enterprise, WPA2-Personal, Mieszany WPA2/WPA-Enterprise oraz Mieszany WPA2/WPA-Personal.

Uwaga:

Zalecamy pozostawienie ustawień domyślnych, gdyż zmiany mogą wpłynąć negatywnie na funkcjonowanie sieci bezprzewodowej. W pewnych warunkach mogą jednak wpłynąć na funkcjonowanie sieci pozytywnie, dlatego przed wprowadzeniem zmian radzimy zapoznać się dokładnie z opisem odpowiednich ustawień.

1. WEP

WEP to najprostszy typ uwierzytelniania. Posiada opcję wyboru siły szyfrowania: 64 bity oraz 128 bitów. Można go ustawić na dwa sposoby:

- Wybierz typ uwierzytelniania **Otwarte (brak zabezpieczeń)**, a następnie w polu Szyfrowanie WEP wybierz z listy pozycję **Włączone** (Rysunek 4-74).
- Wybierz typ uwierzytelniania **Współdzielone**. Przy tym typie uwierzytelniania szyfrowanie WEP jest domyślnie włączone (Rysunek 4-75).

Ręczna konfiguracja

Aby zabezpieczyć sieć przed niepożądanymi użytkownikami zalecane jest wybranie jednego z dostępnych typów zabezpieczeń. Poniżej możesz skonfigurować typ uwierzytelniania, szyfrowanie, określić klucz wymagany do połączenia z siecią oraz ustalić siłę szyfrowania.

Uwaga: nie zalecamy używania szyfrowania WEP jeżeli router pracuje w trybie 11n. Maksymalna prędkość transmisji przy użyciu szyfrowania WEP spada do 54Mb/s.

Wskazówka: Tryb Tylko 11n nie jest obsługiwany kiedy szyfrowanie WEP jest "Włączone" lub kiedy typ szyfrowania WPA to "TKIP".

Wskazówki: "Szyfrowanie WPA" nie może być ustawione w tryb "TKIP" jeżeli urządzenie działa w trybie 11n.

Po zakończeniu naciśnij przycisk "Zapisz/Zastosuj".

Typ uwierzytelniania:

Szyfrowanie WEP:

Siła szyfrowania:

Aktualny klucz sieciowy:

Klucz sieciowy 1:

Klucz sieciowy 2:

Klucz sieciowy 3:

Klucz sieciowy 4:

Wprowadź 13 znaków ASCII lub 26 znaków szesnastkowych jako 128-bitowy klucz
Wprowadź 5 znaków ASCII lub 10 znaków szesnastkowych jako 64-bitowy klucz

Rysunek 4-74

Ręczna konfiguracja

Aby zabezpieczyć sieć przed niepożądanymi użytkownikami zalecane jest wybranie jednego z dostępnych typów zabezpieczeń. Poniżej możesz skonfigurować typ uwierzytelniania, szyfrowanie, określić klucz wymagany do połączenia z siecią oraz ustalić siłę szyfrowania.

Uwaga: nie zalecamy używania szyfrowania WEP jeżeli router pracuje w trybie 11n. Maksymalna prędkość transmisji przy użyciu szyfrowania WEP spada do 54Mb/s.

Wskazówka: Tryb Tylko 11n nie jest obsługiwany kiedy szyfrowanie WEP jest "Włączone" lub kiedy typ szyfrowania WPA to "TKIP".

Wskazówki: "Szyfrowanie WPA" nie może być ustawione w tryb "TKIP" jeżeli urządzenie działa w trybie 11n.

Po zakończeniu naciśnij przycisk "Zapisz/Zastosuj".

Typ uwierzytelniania:

Szyfrowanie WEP:

Siła szyfrowania:

Aktualny klucz sieciowy:

Klucz sieciowy 1:

Klucz sieciowy 2:

Klucz sieciowy 3:

Klucz sieciowy 4:

Wprowadź 13 znaków ASCII lub 26 znaków szesnastkowych jako 128-bitowy klucz
Wprowadź 5 znaków ASCII lub 10 znaków szesnastkowych jako 64-bitowy klucz

Rysunek 4-75

- **Siła szyfrowania:** Wybierz odpowiednią siłę szyfrowania: 64-bit lub 128-bit.
- **Aktualny klucz sieciowy:** Wybierz, który z wprowadzonych poniżej kluczy jest aktualnie używany.
- **Klucz sieciowy 1-4:** Wprowadź klucze sieciowe w poniższe pola.

Konfiguracja ustawień WEP (Rysunek 4-76)

- 1) W polu **Typ uwierzytelniania** wybierz **Współdzielone**.
- 2) W polu **Siła szyfrowania** wybierz **64-bit**.
- 3) W polu **Aktualny klucz sieciowy** wybierz „1”.
- 4) Wprowadź hasło w polu **Klucz sieciowy 1**.
- 5) Naciśnij przycisk „**Zapisz/Zastosuj**”, aby zapisać ustawienia.

Ręczna konfiguracja

Aby zabezpieczyć sieć przed niepożądanymi użytkownikami zalecane jest wybranie jednego z dostępnych typów zabezpieczeń. Poniżej możesz skonfigurować typ uwierzytelniania, szyfrowanie, określić klucz wymagany do połączenia z siecią oraz ustalić siłę szyfrowania.

Uwaga: nie zalecamy używania szyfrowania WEP jeżeli router pracuje w trybie 11n. Maksymalna prędkość transmisji przy użyciu szyfrowania WEP spada do 54Mb/s.

Wskazówka: Tryb Tylko 11n nie jest obsługiwany kiedy szyfrowanie WEP jest "Włączone" lub kiedy typ szyfrowania WPA to "TKIP".

Wskazówki: "Szyfrowanie WPA" nie może być ustawione w tryb "TKIP" jeżeli urządzenie działa w trybie 11n.

Po zakończeniu naciśnij przycisk "Zapisz/Zastosuj".

Typ uwierzytelniania:

Szyfrowanie WEP:

Siła szyfrowania:

Aktualny klucz sieciowy:

Klucz sieciowy 1:

Klucz sieciowy 2:

Klucz sieciowy 3:

Klucz sieciowy 4:

Wprowadź 13 znaków ASCII lub 26 znaków szesnastkowych jako 128-bitowy klucz
Wprowadź 5 znaków ASCII lub 10 znaków szesnastkowych jako 64-bitowy klucz

Rysunek 4-76

Uwaga:

W powyższym przykładzie użyte zostały opcje: **Typ uwierzytelniania** - Współdzielone, **Siła szyfrowania** – 64-bit, **Aktualny klucz sieciowy** – „1”, **Klucz sieciowy 1** – „1234567890” (Rysunek 4-76).

2. WPA-Enterprise

Uwierzytelnianie WPA powstało w celu poprawienia pewnych niedociągnięć WEP. WPA-Enterprise łączy generowanie klucza sieciowego z serwerem uwierzytelniającym RADIUS.

Ręczna konfiguracja

Aby zabezpieczyć sieć przed niepożądanymi użytkownikami zalecane jest wybranie jednego z dostępnych typów zabezpieczeń. Poniżej możesz skonfigurować typ uwierzytelniania, szyfrowanie, określić klucz wymagany do połączenia z siecią oraz ustalić siłę szyfrowania.

Uwaga: nie zalecamy używania szyfrowania WEP jeżeli router pracuje w trybie 11n. Maksymalna prędkość transmisji przy użyciu szyfrowania WEP spada do 54Mb/s.

Wskazówka: Tryb Tylko 11n nie jest obsługiwany kiedy szyfrowanie WEP jest "Włączone" lub kiedy typ szyfrowania WPA to "TKIP".

Wskazówki: "Szyfrowanie WPA" nie może być ustawione w tryb "TKIP" jeżeli urządzenie działa w trybie 11n.

Po zakończeniu naciśnij przycisk "Zapisz/Zastosuj".

Typ uwierzytelniania:

Interwał aktualizacji klucza WPA grupy: (opcjonalnie)

Adres IP serwera RADIUS:

Port RADIUS: (1-65535)

Hasło RADIUS: (opcjonalnie)

(Możesz wprowadzić od 8 do 63 znaków ASCII lub 64 znaków szesnastkowych.)

Szyfrowanie WPA:

Szyfrowanie WEP:

Rysunek 4-77

- **Interwał aktualizacji klucza WPA grupy:** Wprowadź czas odnawiania klucza, po upływie którego router będzie odnawiał klucz sieciowy.
- **Adres IP serwera RADIUS:** Wprowadź adres IP serwera RADIUS.
- **Port RADIUS:** Wprowadź port serwera RADIUS. Domyślna wartość to 1812.
- **Hasło RADIUS:** Wprowadź hasło do serwera RADIUS.
- **Szyfrowanie WPA:** Wybierz szyfrowanie, którego chcesz użyć (AES jest silniejsze niż TKIP).

Konfiguracja ustawień WPA (Rysunek 4-78)

1. W polu **Typ uwierzytelniania** wybierz **WPA-Enterprise**.
2. Zmień **Interwał aktualizacji klucza WPA grupy**.
3. W polu **Adres IP serwera RADIUS** wprowadź adres IP używanego serwera RADIUS.
4. Wprowadź **Port RADIUS** jeżeli port serwera różni się od wartości domyślnej.
5. W polu **Hasło RADIUS** wprowadź hasło.
6. W polu **Szyfrowanie WPA** wybierz **AES**.
7. Naciśnij przycisk „**Zapisz/Zastosuj**”, aby zapisać ustawienia.

Ręczna konfiguracja

Aby zabezpieczyć sieć przed niepowołanymi użytkownikami zalecane jest wybranie jednego z dostępnych typów zabezpieczeń. Poniżej możesz skonfigurować typ uwierzytelniania, szyfrowanie, określić klucz wymagany do połączenia z siecią oraz ustalić siłę szyfrowania.
Uwaga: nie zalecamy używania szyfrowania WEP jeżeli router pracuje w trybie 11n. Maksymalna prędkość transmisji przy użyciu szyfrowania WEP spada do 54Mb/s.
Wskazówka: Tryb Tylko 11n nie jest obsługiwany kiedy szyfrowanie WEP jest "Włączone" lub kiedy typ szyfrowania WPA to "TKIP".
Wskazówka: "Szyfrowanie WPA" nie może być ustawione w tryb "TKIP" jeżeli urządzenie działa w trybie 11n.
Po zakończeniu naciśnij przycisk "Zapisz/Zastosuj".

Typ uwierzytelniania:

Interwał aktualizacji klucza WPA grupy: (opcjonalnie)

Adres IP serwera RADIUS:

Port RADIUS: (1-65535)

Hasło RADIUS: (opcjonalnie)
(Możesz wprowadzić od 8 do 63 znaków ASCII lub 64 znaków szesnastkowych.)

Szyfrowanie WPA:

Szyfrowanie WEP:

Rysunek 4-78

3. WPA-Personal

Uwierzytelnianie WPA-Personal wymaga wprowadzenia klucza sieciowego i nie używa dodatkowego serwera uwierzytelniającego. Klucz sieciowy może być w formacie ASCII lub szesnastkowym.

Ręczna konfiguracja

Aby zabezpieczyć sieć przed niepowołanymi użytkownikami zalecane jest wybranie jednego z dostępnych typów zabezpieczeń. Poniżej możesz skonfigurować typ uwierzytelniania, szyfrowanie, określić klucz wymagany do połączenia z siecią oraz ustalić siłę szyfrowania.
Uwaga: nie zalecamy używania szyfrowania WEP jeżeli router pracuje w trybie 11n. Maksymalna prędkość transmisji przy użyciu szyfrowania WEP spada do 54Mb/s.
Wskazówka: Tryb Tylko 11n nie jest obsługiwany kiedy szyfrowanie WEP jest "Włączone" lub kiedy typ szyfrowania WPA to "TKIP".
Wskazówka: "Szyfrowanie WPA" nie może być ustawione w tryb "TKIP" jeżeli urządzenie działa w trybie 11n.
Po zakończeniu naciśnij przycisk "Zapisz/Zastosuj".

Typ uwierzytelniania:

Hasło: (nazywane też kluczem sieciowym)
[Kliknij aby wyświetlić](#)
(Możesz wprowadzić od 8 do 63 znaków ASCII lub 64 znaków szesnastkowych.)

Interwał aktualizacji klucza WPA grupy: (opcjonalnie)

Szyfrowanie WPA:

Szyfrowanie WEP:

Rysunek 4-79

- **Hasło:** Wprowadź hasło sieci bezprzewodowej. Możesz wprowadzić od 8 do 63 znaków ASCII lub od 8 do 64 znaków szesnastkowych.
- **Kliknij aby wyświetlić:** Po kliknięciu linku wyświetli się hasło.

Konfiguracja ustawień WPA-Personal (Rysunek 4-80)

1. W polu **Typ uwierzytelniania**, wybierz **WPA-Personal**.
2. WPA-Personal wymaga wprowadzenia klucza sieciowego. Wprowadź klucz sieciowy w odpowiednim polu. Klucz sieciowy może być w formacie ASCII lub szesnastkowym.
3. W polu **Interwał aktualizacji klucza WPA grupy**, wprowadź odpowiednią wartość lub pozostaw ustawienia domyślne.
4. Naciśnij przycisk „**Zapisz/Zastosuj**”, aby zapisać ustawienia.

Ręczna konfiguracja

Aby zabezpieczyć sieć przed niepożądanymi użytkownikami zalecane jest wybranie jednego z dostępnych typów zabezpieczeń. Poniżej możesz skonfigurować typ uwierzytelniania, szyfrowanie, określić klucz wymagany do połączenia z siecią oraz ustalić siłę szyfrowania.

Uwaga: nie zalecamy używania szyfrowania WEP jeżeli router pracuje w trybie 11n. Maksymalna prędkość transmisji przy użyciu szyfrowania WEP spada do 54Mb/s.

Wskazówka: Tryb Tylko 11n nie jest obsługiwany kiedy szyfrowanie WEP jest "Włączone" lub kiedy typ szyfrowania WPA to "TKIP".

Wskazówki: "Szyfrowanie WPA" nie może być ustawione w tryb "TKIP" jeżeli urządzenie działa w trybie 11n.

Po zakończeniu naciśnij przycisk "Zapisz/Zastosuj".

Typ uwierzytelniania: WPA-Personal (zalecane)

Hasło: ●●●●●●●● (nazywane też Kluczem sieciowym)
[Kliknij aby wyświetlić](#)
(Możesz wprowadzić od 8 do 63 znaków ASCII lub 64 znaków szesnastkowych.)

Interwał aktualizacji klucza WPA grupy: 30 (opcjonalnie)

Szyfrowanie WPA: AES

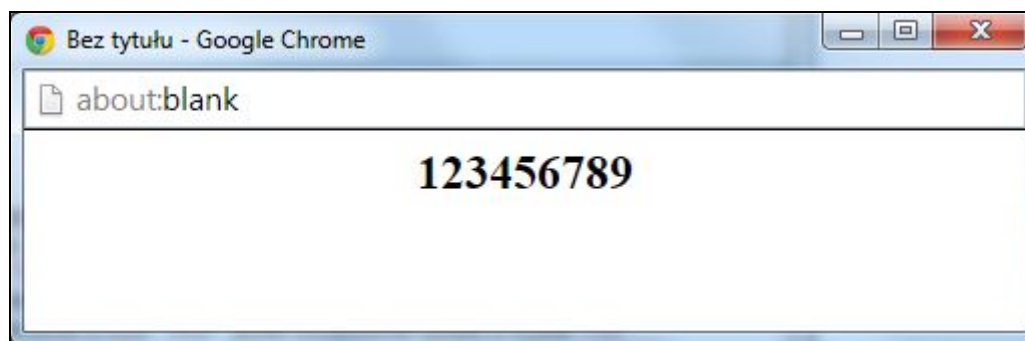
Szyfrowanie WEP: Wyłączone

Zapisz/Zastosuj

Rysunek 4-80

Uwaga:

Po wybraniu opcji „Kliknij aby wyświetlić” pojawi się ekran (Rysunek 4-81) z wprowadzonym hasłem. Jeżeli na którymś z końców hasła znajdują się białe znaki, nie będą one tutaj wyświetlone.



Rysunek 4-81

4. WPA2-Enterprise

Aby skonfigurować ustawienia WPA2-Enterprise, wybierz WPA2-Enterprise z listy. Konfiguracja przebiega w taki sam sposób, jak w przypadku konfiguracji WPA-Enterprise, poza dwoma opcjami przedstawionymi poniżej.

Ręczna konfiguracja

Aby zabezpieczyć sieć przed niepowołanymi użytkownikami zalecane jest wybranie jednego z dostępnych typów zabezpieczeń. Poniżej możesz skonfigurować typ uwierzytelniania, szyfrowanie, określić klucz wymagany do połączenia z siecią oraz ustalić siłę szyfrowania. **Uwaga: nie zalecamy używania szyfrowania WEP jeżeli router pracuje w trybie 11n. Maksymalna prędkość transmisji przy użyciu szyfrowania WEP spada do 54Mb/s.** Wskazówka: Tryb Tylko 11n nie jest obsługiwany kiedy szyfrowanie WEP jest "Włączone" lub kiedy typ szyfrowania WPA to "TKIP". Wskazówki: "Szyfrowanie WPA" nie może być ustawione w tryb "TKIP" jeżeli urządzenie działa w trybie 11n. Po zakończeniu naciśnij przycisk "Zapisz/Zastosuj".

Typ uwierzytelniania: WPA2-Enterprise

Wstępne uwierzytelnianie WPA2: Wylączone

Interwał ponownego uwierzytelniania: 36000 (opcjonalnie)

Interwał aktualizacji klucza WPA grupy: 0 (opcjonalnie)

Adres IP serwera RADIUS: 0.0.0.0

Port RADIUS: 1812 (1-65535)

Hasło RADIUS: (opcjonalnie)
(Możesz wprowadzić od 8 do 63 znaków ASCII lub 64 znaków szesnastkowych.)

Szyfrowanie WPA: AES

Szyfrowanie WEP: Wylączone

Zapisz/Zastosuj

Rysunek 4-82

- **Wstępne uwierzytelnianie WPA2:** Wybierz Włączone z listy. Podłączone urządzenia będą przeprowadzać uwierzytelnienie podczas skanowania sieci.
- **Interwał ponownego uwierzytelniania:** Wprowadź czas (w sekundach), po upływie którego router będzie wymagał ponownego uwierzytelniania. Pozostaw pole puste lub wprowadź wartość „0”, aby wyłączyć ponowne uwierzytelnienie.

5. WPA2-Personal

Aby skonfigurować ustawienia WPA2-Personal, wybierz WPA2-Personal z listy. Uwierzytelnianie WPA2-Personal wymaga wprowadzenia klucza sieciowego i nie używa dodatkowego serwera uwierzytelniającego. Klucz sieciowy może być w formacie ASCII lub szesnastkowym. Konfiguracja przebiega w taki sam sposób, jak w przypadku konfiguracji WPA2-Personal.

Ręczna konfiguracja

Aby zabezpieczyć sieć przed niepowołanymi użytkownikami zalecane jest wybranie jednego z dostępnych typów zabezpieczeń. Poniżej możesz skonfigurować typ uwierzytelniania, szyfrowanie, określić klucz wymagany do połączenia z siecią oraz ustalić siłę szyfrowania. **Uwaga: nie zalecamy używania szyfrowania WEP jeżeli router pracuje w trybie 11n. Maksymalna prędkość transmisji przy użyciu szyfrowania WEP spada do 54Mb/s.** Wskazówka: Tryb Tylko 11n nie jest obsługiwany kiedy szyfrowanie WEP jest "Włączone" lub kiedy typ szyfrowania WPA to "TKIP". Wskazówki: "Szyfrowanie WPA" nie może być ustawione w tryb "TKIP" jeżeli urządzenie działa w trybie 11n. Po zakończeniu naciśnij przycisk "Zapisz/Zastosuj".

Typ uwierzytelniania: WPA2-Personal (najlepsze/zalecane)

Hasło: (nazywane też kluczem sieciowym)
[Kliknij aby wyświetlić](#)
(Możesz wprowadzić od 8 do 63 znaków ASCII lub 64 znaków szesnastkowych.)

Interwał aktualizacji klucza WPA grupy: 0 (opcjonalnie)

Szyfrowanie WPA: AES

Szyfrowanie WEP: Wylączone

Zapisz/Zastosuj

Rysunek 4-83

6. Mieszane WPA2/WPA-Enterprise

Aby skonfigurować ustawienia Mieszane WPA2/WPA-Enterprise, wybierz Mieszane WPA2/WPA-Enterprise z listy. Konfiguracja przebiega w taki sam sposób, jak w przypadku konfiguracji WPA2-Enterprise.

Ręczna konfiguracja

Aby zabezpieczyć sieć przed niepożądanymi użytkownikami zalecane jest wybranie jednego z dostępnych typów zabezpieczeń.

Poniżej możesz skonfigurować typ uwierzytelniania, szyfrowanie, określić klucz wymagany do połączenia z siecią oraz ustalić siłę szyfrowania.

Uwaga: nie zalecamy używania szyfrowania WEP jeżeli router pracuje w trybie 11n. Maksymalna prędkość transmisji przy użyciu szyfrowania WEP spada do 54Mb/s.

Wskazówka: Tryb Tylko 11n nie jest obsługiwany kiedy szyfrowanie WEP jest "Włączone" lub kiedy typ szyfrowania WPA to "TKIP".

Wskazówki: "Szyfrowanie WPA" nie może być ustawione w tryb "TKIP" jeżeli urządzenie działa w trybie 11n.

Po zakończeniu naciśnij przycisk "Zapisz/Zastosuj".

Typ uwierzytelniania:	Mieszany WPA2/WPA Enterprise	▼
Wstępne uwierzytelnianie WPA2:	Wyłączone	▼
Interwał ponownego uwierzytelniania:	36000	(opcjonalnie)
Interwał aktualizacji klucza WPA grupy:	0	(opcjonalnie)
Adres IP serwera RADIUS:	0.0.0.0	
Port RADIUS:	1812	(1-65535)
Hasło RADIUS:		(opcjonalnie)
	(Możesz wprowadzić od 8 do 63 znaków ASCII lub 64 znaków szesnastkowych.)	
Szyfrowanie WPA:	AES	▼
Szyfrowanie WEP:	Wyłączone	▼

Rysunek 4-84

7. Mieszane WPA2/WPA-Personal

Aby skonfigurować ustawienia Mieszane WPA2/WPA-Personal, wybierz Mieszane WPA2/WPA-Personal z listy. Konfiguracja przebiega w taki sam sposób, jak w przypadku konfiguracji WPA2-Personal.

Ręczna konfiguracja		
Aby zabezpieczyć sieć przed niepożądanymi użytkownikami zalecane jest wybranie jednego z dostępnych typów zabezpieczeń.		
Poniżej możesz skonfigurować typ uwierzytelniania, szyfrowanie, określić klucz wymagany do połączenia z siecią oraz ustalić siłę szyfrowania.		
Uwaga: nie zalecamy używania szyfrowania WEP jeżeli router pracuje w trybie 11n. Maksymalna prędkość transmisji przy użyciu szyfrowania WEP spada do 54Mb/s.		
Wskazówka: Tryb Tylko 11n nie jest obsługiwany kiedy szyfrowanie WEP jest "Włączone" lub kiedy typ szyfrowania WPA to "TKIP".		
Wskazówki: "Szyfrowanie WPA" nie może być ustawione w tryb "TKIP" jeżeli urządzenie działa w trybie 11n.		
Po zakończeniu naciśnij przycisk "Zapisz/Zastosuj".		
Typ uwierzytelniania:	Mieszany WPA2/WPA-PSK Personal	▼
Hasło:		(nazywane też kluczem sieciowym)
	Kliknij aby wyświetlić	
	(Możesz wprowadzić od 8 do 63 znaków ASCII lub 64 znaków szesnastkowych.)	
Interwał aktualizacji klucza WPA grupy:	0	(opcjonalnie)
Szyfrowanie WPA:	AES	▼
Szyfrowanie WEP:	Wyłączone	▼

Rysunek 4-85

4.5.3 Harmonogram

Po wybraniu opcji „Sieć bezprzewodowa” → „Harmonogram” pojawi się ekran konfiguracji harmonogramu sieci bezprzewodowej.

Sieć bezprzewodowa -- Harmonogram

Na tej stronie możesz skonfigurować harmonogram sieci bezprzewodowej.

Kliknij na tablicy harmonogramu lub użyj przycisku 'Dodaj' aby określić czas w którym sieć bezprzewodowa zostanie automatycznie wyłączona!

Harmonogram nie będzie działał jeżeli czas systemowy nie został ustawiony. Kliknij [tutaj](#) aby ustawić czas systemowy.

Harmonogram sieci bezprzewodowej: Włącz Wyłącz

Zastosuj do:

Każdego dnia ▼

Czas początkowy:

00:00 ▼

Czas końcowy:

24:00 ▼

Czas	0:00	1:00	2:00	3:00	4:00	5:00	6:00	7:00	8:00	9:00	10:00	11:00	12:00	13:00	14:00
Nie.															
Pon.															
Wto.															
Śro.															
Czw.															
Pią.															
Sob.															

Rysunek 4-86

☞ Uwaga:

Sieć bezprzewodowa nie będzie dostępna w wybranych terminach.

Funkcja Harmonogram nie działa bez ustawionego czasu systemowego ([4.8.5 Pobieranie czasu](#)).

- **Zastosuj do:** Wybierz dni, dla których reguła będzie aktywna.
- **Czas początkowy, Czas końcowy:** Wybierz czas początkowy oraz czas końcowy, dla którego reguła będzie aktywna.
- **Dodaj:** Po naciśnięciu przycisku „Dodaj”, wybrany przedział czasu zostanie wprowadzony do tabeli.

Naciśnij przycisk „**Wyczyść harmonogram**”, aby usunąć wszystkie wpisy z tabeli.

Naciśnij przycisk „**Zapisz/Zastosuj**”, aby zapisać ustawienia.

4.5.4 Filtrowanie MAC

Po wybraniu opcji „Sieć bezprzewodowa” → „Filtrowanie MAC” pojawi się ekran konfiguracji filtrów MAC dla sieci bezprzewodowej.

Sieć bezprzewodowa -- Filtr MAC

Można skonfigurować maksymalnie 64 wpisy.

Tryb filtrowania adresów MAC: Wyłączone Zezwalaj Blokuj Uwaga: Jeżeli wybrana zostanie opcja 'zezwalałaj' i żaden adres nie zostanie dodany funkcja WPS nie będzie działać

Adres MAC	Usuń
-----------	------

Rysunek 4-87

Dostęp do sieci bezprzewodowej może być filtrowany, bazując na adresach MAC urządzeń. Aby włączyć filtrowanie wybierz opcję **Zezwalaj** lub **Blokuj**. Jeżeli nie chcesz korzystać z tej funkcji, wybierz **Wyłączone**.

- **Wyłączone:** Wybierz tą opcję, aby wyłączyć filtrowanie MAC.
- **Zezwalaj:** Wybierz tą opcję, aby pozwolić urządzeniom z listy na dostęp do sieci bezprzewodowej.
- **Blokuj:** Wybierz tą opcję, aby nie pozwolić urządzeniom z listy na dostęp do sieci bezprzewodowej.
- **Dodaj:** Naciśnij ten przycisk, aby dodać wpis w tabeli filtrowania MAC
- **Usuń:** Naciśnij ten przycisk, aby usunąć wpis z tabeli filtrowania MAC

Po naciśnięciu przycisku „**Dodaj**”, pojawi się ekran dodawania nowego filtra (Rysunek 4-88). W polu **Adres MAC** wprowadź adres MAC urządzenia, a następnie naciśnij przycisk „**Zapisz/Zastosuj**”.

Uwaga:

Adres MAC musi być w formacie „**xx:xx:xx:xx:xx:xx**”, np. „**00:11:22:33:44:DD**”.

Sieć bezprzewodowa -- Filtr MAC

Wprowadź adres MAC i naciśnij przycisk "Zapisz/Zastosuj" aby dodać adres do listy filtrowania adresów MAC.

Adres MAC:

Rysunek 4-88

4.5.5 Połączenie Bridge

Po wybraniu opcji „Sieć bezprzewodowa” → „Połączenie Bridge” pojawi się ekran konfiguracji trybu bridge dla sieci bezprzewodowej.

Sieć bezprzewodowa -- połączenia Bridge

Ta strona umożliwia skonfigurowanie ustawień związanych z połączeniami bridge. Jeżeli w menu Tryb AP wybierzesz tryb Bridge zwykle urządzenia bezprzewodowe (laptopy, telefony itp.) nie będą miały dostępu do sieci bezprzewodowej. Połączenie będzie dostępne jedynie dla określonych wcześniej urządzeń działających w trybie bridge. Aby laptopy i inne urządzenia mogły łączyć się do sieci bezprzewodowej wybierz Tryb Punkt Dostępowy. Funkcja ograniczenie połączeń bridge służy do umożliwienia nawiązania połączeń typu bridge jedynie określonym urządzeniom. Po jej włączeniu należy wpisać adresy MAC urządzeń (ustawienie Włączone) lub wybrać adresy MAC urządzeń z listy (ustawienie Włączone(Skan)).
 Naciśnij przycisk "Odśwież" aby zaktualizować listę zdalnych urządzeń. Poczekaj kilka sekund na aktualizację.
 Naciśnij przycisk "Zapisz/Zastosuj" aby zapisać konfigurację.

Wskazówka1: Połączenia typu bridge obsługiwane są jedynie przy uwierzytelnianiu ustawionym w tryb "Otwarte" lub "Współdzielone".
Aby połączyć inne urządzenia bezprzewodowe z routerem należy najpierw ustawić uwierzytelnianie w tryb "Otwarte" lub "Współdzielone"!
Wskazówka2: Inne punkty dostępowe mogą nawiązać połączenie z routerem jedynie z użyciem tego samego kanału transmisji bezprzewodowej.

Tryb AP:

Ograniczenie połączeń bridge:

Rysunek 4-89

- **Tryb AP:** Wybierz tryb AP z listy. Dostępne opcje to: Punkt dostępowy i Bridge.
 - **Punkt dostępowy:** Wybierz tę opcję, aby umożliwić innym urządzeniom łączenie się sieci bezprzewodowej.
 - **Bridge:** Opcja ta (zwana również WDS) pozwala na połączenie bezprzewodowe pomiędzy sieciami lokalnymi.
- **Ograniczenie połączeń bridge:**
 - **Wyłączone:** Wybierz tę opcję, aby umożliwić nieograniczone łączenie się do sieci bezprzewodowej innym urządzeniom.
 - **Włączone:** Wybierz tę opcję (Rysunek 4-90), aby umożliwić łączenie się do sieci bezprzewodowej tylko urządzeniom o podanych poniżej adresach MAC.

Tryb AP:

Ograniczenie połączeń bridge:

Adres MAC zdalnego urządzenia:

Rysunek 4-90

- **Włączone(Skan):** Wybierz tę opcję, aby wyświetlić listę dostępnych połączeń bezprzewodowych. Tylko zaznaczone urządzenia będą mogły łączyć się z siecią bezprzewodową.
- **Odśwież:** Naciśnij ten przycisk, aby ponownie przeprowadzić skan

Tryb AP:	Punkt dostępowy ▾		
Ograniczenie połączeń bridge:	Włączone(Skan) ▾		
Adres MAC zdalnego urządzenia:			
	SSID	BSSID	kanal
<input type="checkbox"/>	TP-LINK_2.4GHz_0000	E8:94:F6:FA:08:D7	1
<input type="checkbox"/>	TP-LINK_514C	90:0A:EB:11:51:4C	1
<input type="checkbox"/>	TP-LINK_pon123	00:0A:EB:13:09:69	1
<input type="checkbox"/>	TP-LINK_11FF13	02:01:00:11:FF:13	1
<input type="checkbox"/>	TP-LINK_9E99	14:CC:20:3A:9E:99	1

Rysunek 4-91

Uwaga:

Połączenia typu bridge obsługiwane są jedynie przy uwierzytelnianiu ustawionym w tryb „**Otwarte**” lub „**Współdzielone**”. Tryb zabezpieczeń można zmienić w zakładce „**Sieć bezprzewodowa**” → „**Zabezpieczenia**”.

Naciśnij przycisk „**Zapisz/Zastosuj**”, aby zapisać ustawienia.

4.5.6 Zaawansowane

Po wybraniu opcji „**Sieć bezprzewodowa**” → „**Zaawansowane**” pojawi się ekran konfiguracji ustawień zaawansowanych sieci bezprzewodowej.

Sieć bezprzewodowa -- Zaawansowane

Na tej stronie możesz skonfigurować zaawansowane ustawienia sieci bezprzewodowej. Możesz wybrać kanał transmisji bezprzewodowej, ustawić próg fragmentacji, próg RTS, skonfigurować interwał wybudzania Klientów połączonych w trybie oszczędzania energii oraz interwał wysyłania pakietów Beacon.
Porada: Jeżeli ustawisz tryb działania sieci na „Tylko 11n”, nie będziesz mógł ustawić typu szyfrowania na „WEP” ani „TKIP”.
Naciśnij przycisk „Zapisz/Zastosuj” aby zapisać ustawienia.

Kanał:	Auto ▾
Tryb:	11bgn ▾
Szerokość kanału:	20/40MHz ▾
Kanał dodatkowy:	Górny ▾
Próg fragmentacji:	2346
Próg RTS:	2347
Interwał DTIM:	1
Interwał pakietów Beacon:	100
Moc transmisji:	100% ▾
WMM(Wi-Fi Multimedia):	Włączone ▾

Rysunek 4-92

- **Kanał:** Wybierz z listy kanał, z którego chcesz korzystać. Wybrany kanał ma wpływ na częstotliwość, na której nadawana będzie sieć bezprzewodowa. Nie ma konieczności zmiany kanału, dopóki nie pojawią się zakłócenia spowodowane innymi punktami dostępowymi na tej samej częstotliwości.
- **Tryb:** Dostępne są opcje: „11b”, „11bg”, „11bgn” oraz „Tylko 11n”. Tryb „11bgn” pozwala na podłączanie się do sieci bezprzewodowej urządzeniom pracującym w standardach 802.11b, 802.11g oraz 802.11n.

- **Szerokość kanału:** Wybierz szerokość kanału z listy. Jeżeli wybrany zostanie szerszy kanał, urządzenia będą mogły przysyłać dane z wyższą prędkością.
- **Kanał dodatkowy:** Jeżeli wybrany zostanie szeroki kanał (20/40 MHz), opcja ta pozwala na wybranie kanału dodatkowego.
- **Próg fragmentacji:** Opcja ta pozwala na zmianę maksymalnego rozmiaru pakietu danych, po przekroczeniu którego pakiet będzie dzielony na kilka mniejszych. Jeżeli występuje problem z dużą ilością błędnych pakietów, można lekko zwiększyć Próg fragmentacji. Ustawienie zbyt niskiej wartości może powodować gorsze funkcjonowanie sieci. Zalecane są tylko drobne zmiany wartości. Jednakże w większości przypadków, powinny one pozostać bez zmian.
- **Próg RTS:** W wypadku wystąpienia problemu ze stabilnością połączenia, można spróbować obniżyć tę wartość. Jeżeli pakiet sieciowy jest mniejszy niż ustawiona wartość progu RTS, mechanizm RTS/CTS nie zostanie uruchomiony. Router wysyła ramkę RTS do odbiorcy, w celu negocjacji przesyłu ramki danych. Odbiorca po odebraniu RTS wysyła ramkę CTS do routera, zgłaszając tym samym gotowość do odbioru danych. Odpowiednie ustawienie wartości Progu RTS pozwala na zablokowanie przesyłu danych pomiędzy urządzeniami. W większości wypadków nie zaleca się zmiany wartości domyślnej.
- **Interwał DTIM:** Wartość pomiędzy 1 a 255. Interwał DTIM informuje klientów o konieczności włączenia nasłuchu na pakiety broadcast i multicast. Wartość ta mierzona jest ilością otrzymanych pakietów beacon. Kiedy router ma zakolejkowany pakiet broadcast lub multicast dla konkretnych klientów, wysyła im DTIM oraz wartość Interwału DTIM. Klient odbiera pakiet beacon, włącza tryb nasłuchu na pakiety broadcast i multicast, a następnie otrzymuje je od routera. Domyślna wartość to 1.
- **Interwał pakietów Beacon:** Wprowadź wartość pomiędzy 20 a 1000 (milisekund). Interwał pakietów Beacon to czas, po upływie którego wysyłane będą pakiety beacon, mające na celu synchronizację sieci bezprzewodowej. Domyślna wartość to 100.
- **Moc transmisji:** Opcja ta pozwala skonfigurować moc transmisji bezprzewodowej. Wysoka wartość zwiększa zasięg sieci i poprawia widoczność sygnału. Niska wartość zmniejsza zasięg sieci, dzięki czemu zakłócenia spowodowane przez inne nadajniki są mniejsze.
- **WMM(Wi-Fi Multimedia):** Funkcja ta nadaje pierwszeństwo pakietom o wysokim priorytecie. Zalecane jest włączenie tej opcji.

4.5.7 Podłączone urządzenia

Po wybraniu opcji „Sieć bezprzewodowa” → „Podłączone urządzenia” pojawi się lista urządzeń podłączonych do sieci bezprzewodowej.

Sieć bezprzewodowa -- Połączone urządzenia			
Na tej stronie pokazane są uwierzytelnione urządzenia bezprzewodowe oraz ich status.			
MAC	Powiązane	Uwierzytelnione	SSID
<input type="button" value="Odśwież"/>			

Rysunek 4-93

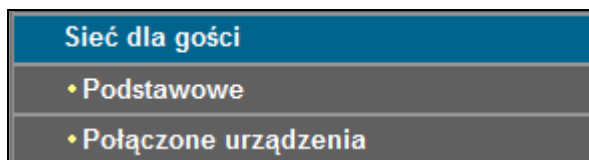
Lista pokazuje połączone urządzenia i ich stan.

- **MAC:** Adres MAC urządzenia.
- **Powiązane:** Informacja o powiązaniu połączonego urządzenia z punktem dostępowym.

- **Uwierzytelnione:** Informacja o uwierzytelnieniu połączonego urządzenia.
- **SSID:** Nazwa sieci bezprzewodowej, do której podłączone jest urządzenie.

Nie można zmienić żadnych wartości na tej stronie. Aby odświeżyć listę, naciśnij przycisk „Odśwież”.

4.6 Sieć dla gości



Zakładka „Sieć bezprzewodowa” zawiera dwie opcje: **Podstawowe** oraz **Podłączone urządzenia**. Opis każdej z opcji znajduje się poniżej.

4.6.1 Podstawowe

Po wybraniu opcji „Sieć dla gości” → „Podstawowe” pojawi się ekran konfiguracji sieci dla gości (Rysunek 4-94).

Sieć bezprzewodowa -- Sieć dla gości

Na tej stronie można skonfigurować sieć bezprzewodową dla gości.

Sieć dla gości: Włącz Wyłącz

Nazwa sieci dla gości:

Typ uwierzytelniania:

Szyfrowanie:

Hasło: (Wprowadź od 8 do 63 znaków ASCII lub od 8 do 64 znaków szesnastkowych.)
[Kliknij tutaj aby wyświetlić](#)

Częstotliwość aktualizacji klucza grupowego: (sekund, minimalna wartość to 30, 0 oznacza brak aktualizacji.)

Zezwalaj gościom na dostęp do sieci lokalnej:

Izolacja klientów sieci dla gości:

Kontrola przepustowości sieci dla gości:

	Minimalna prędkość(Kb/s)	Maksymalna prędkość(Kb/s)
Wysyłanie:	<input type="text" value="500"/>	<input type="text" value="1000"/>
Pobieranie:	<input type="text" value="500"/>	<input type="text" value="1000"/>

Rysunek 4-94

Możesz włączyć lub wyłączyć Sieć dla gości. Po jej włączeniu pojawią się poniższe pola:

- **Nazwa sieci dla gości:** Wprowadź nazwę sieci dla gości. Zaleca się użycie nazwy, która pozwoli na jej łatwe odróżnienie od głównej sieci bezprzewodowej.
- **Typ uwierzytelniania:** Wybierz z listy typ uwierzytelniania.
- **Szyfrowanie:** Wybierz szyfrowanie z listy. Dostępne są opcje: **AES** oraz **AES+TKIP**.
- **Hasło:** Wprowadź hasło do sieci dla gości. Możesz wprowadzić od 8 do 63 znaków ASCII lub od 8 do 64 znaków szesnastkowych. Po naciśnięciu „Kliknij tutaj aby wyświetlić”, pojawi się okno z wprowadzonym hasłem.

- **Częstotliwość aktualizacji klucza grupowego:** Wprowadź czas w sekundach. Minimalna wartość to 30, 0 oznacza brak aktualizacji.
- **Zezwalaj gościom na dostęp do sieci lokalnej:** Po włączeniu tej opcji goście będą mieli dostęp do sieci lokalnej, ale nadal nie będą mogli zalogować się na stronę konfiguracyjną routera.
- **Izolacja klientów sieci dla gości:** Po włączeniu tej opcji, urządzenia podłączone do sieci dla gości nie będą mogły komunikować się między sobą. Domyślnie opcja ta jest wyłączona.
- **Kontrola przepustowości sieci dla gości:** Po włączeniu tej opcji można skonfigurować kontrolę przepustowości dla urządzeń podłączonych do sieci dla gości.

Naciśnij przycisk „**Zapisz/Zastosuj**”, aby zapisać ustawienia.

4.6.2 Podłączone urządzenia

Po wybraniu opcji „**Sieć dla gości**”→„**Podłączone urządzenia**”, pojawi się lista urządzeń podłączonych do sieci dla gości.

Sieć bezprzewodowa -- Połączone urządzenia			
Na tej stronie pokazane są uwierzytelnione urządzenia bezprzewodowe oraz ich status.			
MAC	Powiązane	Uwierzytelnione	SSID
<input type="button" value="Odśwież"/>			

Rysunek 4-95

Lista pokazuje połączone urządzenia i ich stan.

- **MAC:** Adres MAC urządzenia.
- **Powiązane:** Informacja o powiązaniu połączonego urządzenia z punktem dostępowym.
- **Uwierzytelnione:** Informacja o uwierzytelnieniu połączonego urządzenia.
- **SSID:** Nazwa sieci bezprzewodowej, z którą połączone jest urządzenie.

Nie można zmienić żadnych wartości na tej stronie. Aby odświeżyć listę, naciśnij przycisk „**Odśwież**”.

4.7 Diagnostyka

Po wybraniu opcji „**Diagnostyka**” pojawi się ekran przedstawiający stan połączeń ENET(Ethernet), sieci bezprzewodowej oraz łącza ADSL. Po naciśnięciu przycisku „**Pomoc**”, wyświetlą się szczegółowe informacje dotyczące każdego z testów.

br_0_0_35 Diagnostyka

Możesz za pomocą routera przeprowadzić test diagnostyczny swojego połączenia. Jeżeli wystąpi błąd naciśnij przycisk "Uruchom ponownie Testy" u dołu strony aby upewnić się, że błąd występuje za każdym razem. Jeżeli błąd wystąpi ponownie, naciśnij przycisk "Pomoc" i postępuj zgodnie ze wskazówkami.

Test połączenia z siecią lokalną

Test połączenia portu LAN1	UDANY	Pomoc
Test połączenia portu LAN2	NIEUDANY	Pomoc
Test połączenia portu LAN3	NIEUDANY	Pomoc
Test połączenia portu LAN4/WAN	NIEUDANY	Pomoc
Test połączenia bezprzewodowego:	UDANY	Pomoc

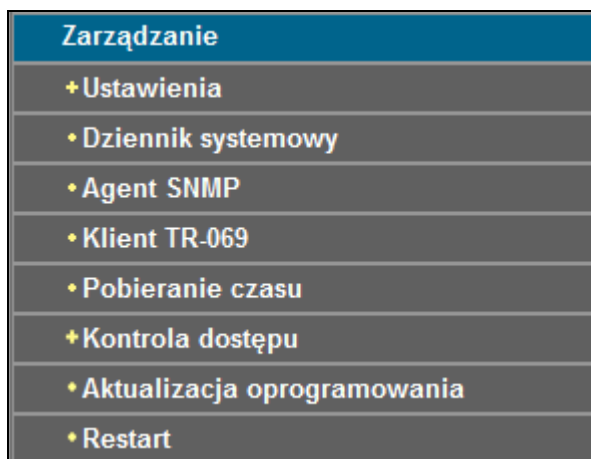
Test połączenia z siecią dostawcy Internetu

Test synchronizacji xDSL:	NIEUDANY	Pomoc
Test ping do segmentu F5 ATM OAM:	WYŁĄCZONY	Pomoc
Test ping poprzez segment F5 ATM OAM:	WYŁĄCZONY	Pomoc

Rysunek 4-96

4.8 Zarządzanie

Zakładka „**Zarządzanie**” zawiera opcje: **Ustawienia**, **Dziennik systemowy**, **Agent SNMP**, **Klient TR-069**, **Pobieranie czasu**, **Kontrola dostępu**, **Aktualizacja oprogramowania** oraz **Restart**. Opis każdej z opcji znajduje się poniżej.



4.8.1 Ustawienia

Zakładka **Ustawienia** posiada trzy istotne przy zarządzaniu routerem opcje: **Zapisz**, **Wczytaj** oraz **Przywróć domyślne**. Ich opis znajduje się poniżej.

Ustawienia - Zapisz

Zapis konfiguracji routera ADSL. Możesz zapisać konfigurację w pliku na swoim komputerze PC.

Zapisz konfigurację

Rysunek 4-97

4.8.1.1 Zapisz

Po wybraniu opcji „**Zarządzanie**”→„**Ustawienia**”→„**Zapisz**”, pojawi się ekran pozwalający na zapisanie obecnych ustawień routera w pliku na komputerze (Rysunek 4-98).

Ustawienia - Zapisz

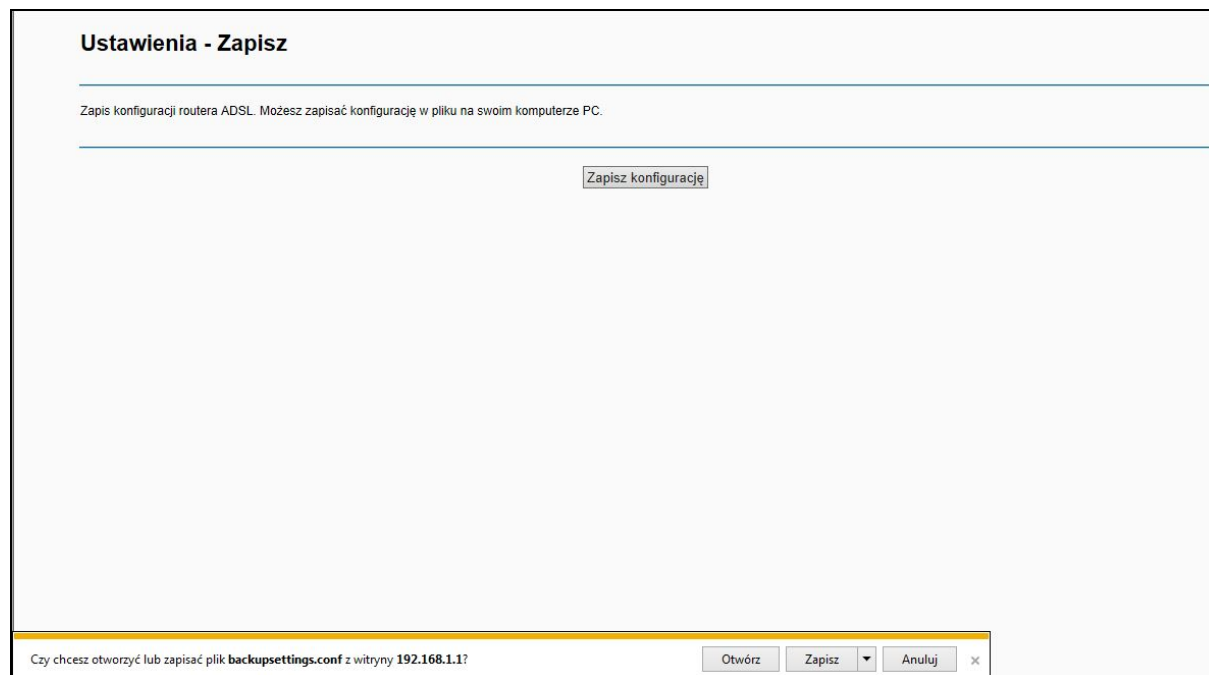
Zapis konfiguracji routera ADSL. Możesz zapisać konfigurację w pliku na swoim komputerze PC.

Zapisz konfigurację

Rysunek 4-98

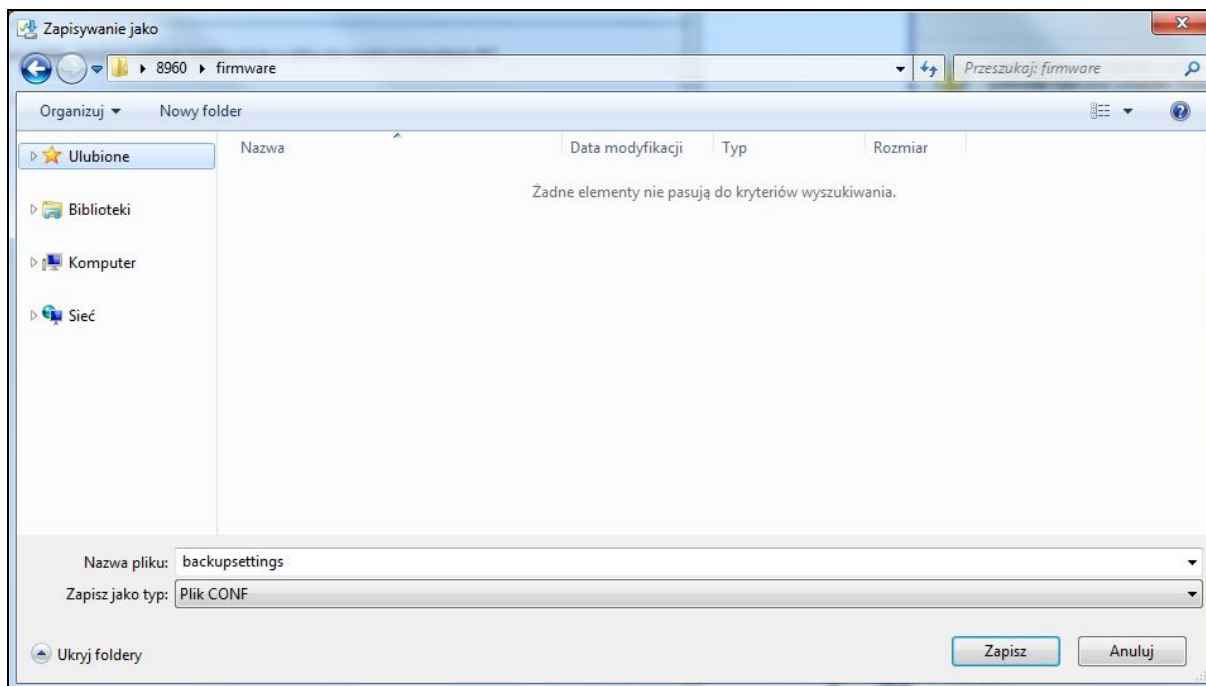
Aby zapisać obecne ustawienia routera:

1. Naciśnij przycisk „**Zapisz konfigurację**”. Pojawi się poniższe okienko (Rysunek 4-99).



Rysunek 4-99

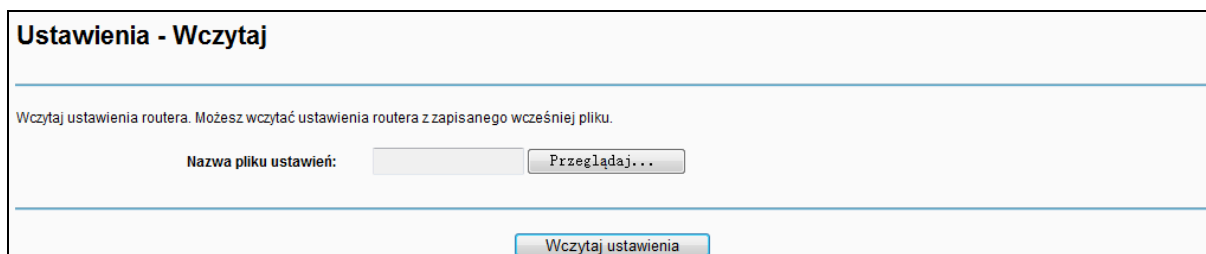
- Naciśnij przycisk „**Zapisz**”, aby zapisać ustawienia w wybranym przez siebie miejscu na dysku (Rysunek 4-100).



Rysunek 4-100

4.8.1.2 Wczytaj

Po wybraniu opcji „**Zarządzanie**” → „**Ustawienia**” → „**Wczytaj**” pojawi się ekran pozwalający na wczytanie ustawień routera z zapisanego wcześniej pliku (Rysunek 4-101).



Rysunek 4-101

Aby wczytać ustawienia routera:

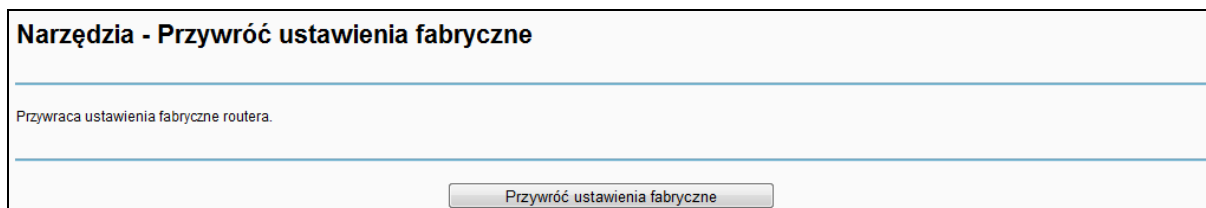
- Naciśnij przycisk „**Wybierz plik**”, a następnie wskaż plik z zapisaną konfiguracją.
- Po wybraniu właściwego pliku naciśnij przycisk „**Wczytaj ustawienia**”.

Uwaga:

Po wczytaniu ustawień, router się zrestartuje. Nie wyłączaj routera ani nie naciskaj przycisku **Reset** z tyłu urządzenia w trakcie restartowania.

4.8.1.3 Przywróć domyślne

Po wybraniu opcji „Zarządzanie”→„Ustawienia”→„Przywróć domyślne”, pojawi się ekran pozwalający na przywrócenie ustawień fabrycznych routera (Rysunek 4-102).

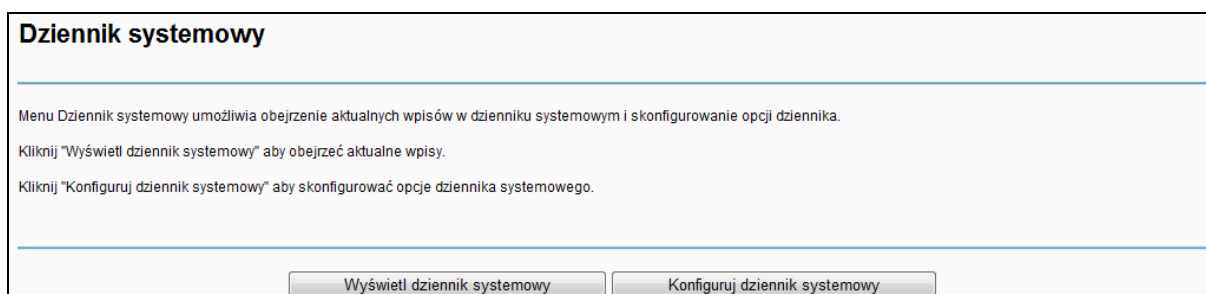


Rysunek 4-102

- **Przywróć ustawienia fabryczne:** Naciśnij ten przycisk, a następnie postępuj zgodnie z instrukcjami, aby przywrócić router do ustawień fabrycznych.
- **Nazwa użytkownika i Hasło:** Domyślna nazwa użytkownika i hasło to „admin”.
- **Domyślny Adres IP:** 192.168.1.1.
- **Domyślna Maska podsieci:** 255.255.255.0.

4.8.2 Dziennik systemowy

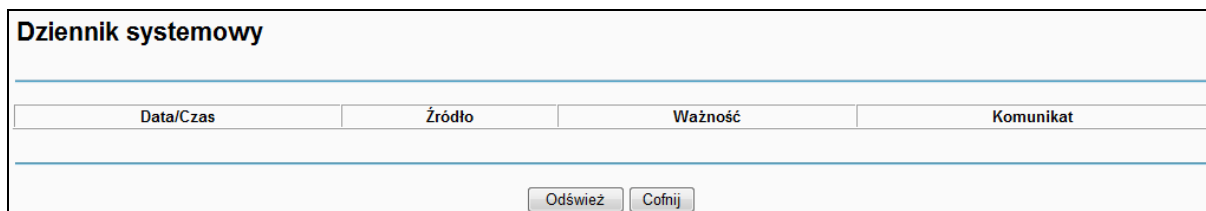
Po wybraniu opcji „Zarządzanie”→„Dziennik systemowy” pojawi się ekran pozwalający na wyświetlenie oraz skonfigurowanie dziennika systemowego (Rysunek 4-103).



Rysunek 4-103

Aby wyświetlić dziennik systemowy:

Naciśnij przycisk „Wyświetl dziennik systemowy”. Pojawi się lista najnowszych wpisów (Rysunek 4-104).



Rysunek 4-104

- **Odśwież:** Naciśnij ten przycisk, aby zaktualizować wpisy w tabeli.
- **Cofnij:** Naciśnij ten przycisk, aby wrócić do poprzedniej strony.

Aby skonfigurować dziennik systemowy:

Naciśnij przycisk „**Konfiguruj dziennik systemowy**”. Pojawi się ekran konfiguracji dziennika (Rysunek 4-105).

Dziennik systemowy -- Konfiguracja

Jeżeli tryb zapisywania jest aktywny, system będzie zapisywał informacje o wybranych zdarzeniach. Wszystkie zdarzenia o wybranym lub wyższym od wybranego poziomie zapisu będą zapisywane. Wszystkie zdarzenia o wybranym lub wyższym od wybranego poziomie wyświetlania będą wyświetlane. Jeżeli wybrana zostanie opcja 'Zdalnie' lub 'Oba' wybrane zdarzenia będą również wysyłane na określony adres IP/port UDP zdalnego serwera logowania. Jeżeli wybrana zostanie opcja 'Lokalnie' lub 'Oba,' zdarzenia będą zapisywane lokalnie w pamięci urządzenia.

Wybierz odpowiednie wartości i naciśnij przycisk 'Zapisz/Zastosuj' aby skonfigurować opcje dziennika systemowego.

Dziennik: Wyłącz Włącz

Poziom zapisywania:

Poziom wyświetlania:

Tryb:

Rysunek 4-105

- **Wyłącz/Włącz:** Wybierz **Włącz**, aby zapisywać informacje o wybranych zdarzeniach. W innym przypadku, wybierz **Wyłącz**.
- **Poziom zapisywania:** Wszystkie zdarzenia o wybranym poziomie zapisu lub wyższym od wybranego będą zapisywane/będą wyświetlane.
- **Poziom wyświetlania:** Wszystkie zdarzenia o wybranym poziomie zapisu lub wyższym od wybranego będą zapisywane/będą wyświetlane.
- **Tryb:** Jeżeli wybrana zostanie opcja „**Zdalnie**”, wybrane zdarzenia będą wysyłane na określony adres IP/port UDP zdalnego serwera logowania. Jeżeli wybrana zostanie opcja „**Lokalnie**”, zdarzenia będą zapisywane lokalnie w pamięci urządzenia. Jeżeli wybrana została opcja „**Oba**”, zdarzenia zapisywane będą lokalnie oraz na zdalnym serwerze logowania.

4.8.3 Agent SNMP

Po wybraniu opcji „**Zarządzanie**” → „**Agent SNMP**”, pojawi się ekran konfiguracji SNMP (Rysunek 4-106).

Protokół **SNMP** (Simple Network Management Protocol) jest obecnie szeroko stosowany w sieciach komputerowych i pozwala na zarządzanie urządzeniami przez sieć IP. Za jego pomocą administrator sieci może w łatwy sposób sprawdzić i zmienić konfigurację urządzeń oraz wykryć błędy w ich funkcjonowaniu.

Agent SNMP to aplikacja na routerze, która odbiera, przetwarza i wysyła odpowiedzi na komunikaty SNMP oraz wysyła komunikaty Trap. Router, który posiada Agenta SNMP może być monitorowany i zarządzany za pomocą Managera SNMP.

Manager SNMP to aplikacja przetwarzająca i generująca komunikaty SNMP. Pozwala ona na odbiór komunikatów Trap oraz odczytywanie i zmianę konfiguracji urządzeń, na których uruchomiony jest Agent SNMP.

SNMP - Konfiguracja

Protokół SNMP (Simple Network Management Protocol) umożliwia aplikacjom zarządzającym pobieranie statystyk i informacji z agenta SNMP w routerze.

Wybierz żądane wartości i naciśnij przycisk „Zapisz/Zastosuj” aby skonfigurować opcje SNMP.

Agent SNMP:	<input checked="" type="radio"/> Wyłącz <input type="radio"/> Włącz
Read Community:	public
Set Community:	private
Nazwa systemu:	TP-LINK
Lokacja systemu:	nieznany
Kontakt systemu:	nieznany
Adres IP menadżera komunikatów:	0.0.0.0

Zapisz/Zastosuj

Rysunek 4-106

- **Agent SNMP:** Zaznacz odpowiednią opcję, aby włączyć lub wyłączyć tę funkcję.

Uwaga:

Ciąg znaków **SNMP Community** służy jako hasło uwierzytelniające pomiędzy Agentem SNMP routera a Menadżerem SNMP sieci.

- **Read Community:** Wprowadź ciąg znaków Read Community. Pozwala on na uzyskanie dostępu do ustawień routera na poziomie odczytu. Domyślna wartość to „public”.
- **Set Community:** Wprowadź ciąg znaków Set Community. Pozwala on na uzyskanie dostępu do ustawień routera na poziomie odczytu i zapisu. Domyślna wartość to „private”.
- **Nazwa systemu:** Wprowadź nazwę systemu. Agent SNMP routera będzie wyświetlał dane konfiguracyjne pod wprowadzoną nazwą.
- **Lokacja systemu:** Lokalizacja osoby wprowadzonej jako **Kontakt systemu**.
- **Kontakt systemu:** Osoba, z którą należy się kontaktować w razie wystąpienia problemów.
- **Adres IP menadżera komunikatów:** Wprowadź adres IP Menadżera SNMP, na który router będzie wysyłał komunikaty Trap.

Naciśnij przycisk „**Zapisz/Zastosuj**”, aby zapisać ustawienia.

4.8.4 Klient TR-069

Po wybraniu opcji „Zarządzanie” → „Klient TR-069” pojawi się ekran konfiguracji klienta TR-069 (Rysunek 4-107).

Protokół zarządzania WAN (TR-069) umożliwia serwerowi automatycznej konfiguracji (ACS) automatyczne konfigurowanie, zbieranie danych oraz diagnostykę tego urządzenia.

Klient usługi TR-069 - Konfiguracja

Protokół zarządzania WAN (TR-069) umożliwia serwerowi automatycznej konfiguracji (ACS) automatyczne konfigurowanie, zbieranie danych oraz diagnostykę tego urządzenia.

Wprowadź określone wartości i naciśnij przycisk "Zapisz/Zastosuj" aby skonfigurować opcje klienta usługi TR-069.

Inform Wyłącz Włącz

Interwał komunikatów Inform:

Adres URL ACS:

Nazwa użytkownika ACS:

Hasło ACS:

Interfejs WAN używany przez klienta usługi TR-069:

Wyświetlaj komunikaty SOAP na konsoli szeregowej Wyłącz Włącz

Uwierzytelnianie żądania połączenia

Nazwa użytkownika żądania połączenia:

Hasło żądania połączenia:

Adres URL żądania połączenia:

Rysunek 4-107

- **Inform:** Zaznacz **Włącz**, aby włączyć **Interwał komunikatów Inform**.
- **Interwał komunikatów Inform:** Wprowadź okres czasu, po upływie którego router będzie komunikował się z ACS.
- **Adres URL ACS:** Wprowadź otrzymany od dostawcy adres serwera ACS.
- **Nazwa użytkownika ACS:** Wprowadź otrzymaną od dostawcy nazwę użytkownika ACS.
- **Hasło ACS:** Wprowadź otrzymane od dostawcy hasło ACS.

Uwaga:

Jeżeli chcesz zalogować się na **ACS**, musisz posiadać własną nazwę użytkownika i hasło.

- **Interfejs WAN używany przez klienta usługi TR-069:** Wybierz interfejs z listy.
- **Nazwa użytkownika żądania połączenia:** Wprowadź nazwę użytkownika, z której ACL będzie korzystał przy logowaniu do routera..
- **Hasło żądania połączenia:** Wprowadź hasło, z którego ACL będzie korzystał przy logowaniu do routera.

Naciśnij przycisk „Zapisz/Zastosuj”, aby zapisać ustawienia.

4.8.5 Pobieranie czasu

Po wybraniu opcji „Zarządzanie” → „Pobieranie czasu” pojawi się ekran konfiguracji czasu routera (Rysunek 4-108).

Ustawienia czasu

Ta strona umożliwia konfigurację ustawień czasu w routerze.

Data/Czas : Czw Sty 1 01:33:39 1970
Data/Czas w twoim komputerze : Śro Lip 15 16:25:39 2015

Konfiguracja daty/czasu routera

Data (R/M/D) : 1970/01/01
Czas (G:M:S) : 01:33:39

Włącz zmianę czasu

Początek: 1970 Sty 1 Czw 00:00
Koniec: 1971 Sty 1 Czw 00:00

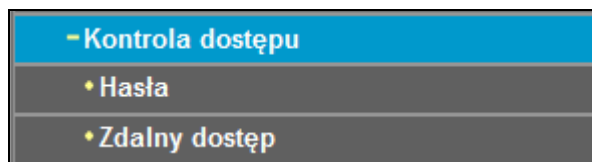
Automatycznie synchronizuj z serwerami czasu w Internecie

Pierwszy serwer czasu - NTP: time.nist.gov
Drugi serwer czasu - NTP: ntp1.tummy.com
Trzeci serwer czasu - NTP: Brak
Czwarty serwer czasu - NTP: Brak
Piąty serwer czasu - NTP: Brak
Przesunięcie strefy czasowej: (GMT+01:00) Warszaw

Rysunek 4-108

- **Włącz zmianę czasu:** Zaznacz tę opcję, aby włączyć zmianę czasu z zimowego na letni.

4.8.6 Kontrola dostępu



Zakładka „Kontrola dostępu” zawiera dwie opcje: **Hasła** oraz **Zdalny dostęp**. Opis każdej z opcji znajduje się poniżej.

4.8.6.1 Hasła

Po wybraniu opcji „Zarządzanie” → „Kontrola dostępu” → „Hasła” pojawi się ekran konfiguracji haseł dostępu do routera (Rysunek 4-109). Domyślne dane logowania dla trzech kont to odpowiednio admin/admin oraz user/user.

Kontrola dostępu -- Hasła

Dostęp do menu routera kontrolowany jest przez trzy następujące konta użytkownika: admin oraz user.

Użytkownik "admin" ma nieograniczony dostęp do zmiany oraz wyświetlania konfiguracji routera.

Użytkownik "user" może wyświetlić konfigurację i statystyki routera oraz zaktualizować jego oprogramowanie.

Wprowadź do 16 znaków w poniższe pola i naciśnij przycisk "Zapisz/Zastosuj" aby zmienić lub utworzyć hasła. Uwaga: hasła nie mogą zawierać spacji.

Nazwa użytkownika:

Stare hasło:

Nowe hasło:

Potwierdź hasło:

Rysunek 4-109

Aby zmienić hasło:

1. Wybierz nazwę użytkownika, dla której hasło chcesz zmienić.
2. Wprowadź **Stare hasło**.
3. Wprowadź **Nowe hasło** i **Potwierdź hasło**. Wartości wprowadzone w obydwu polach muszą być identyczne.
4. Naciśnij przycisk „**Zapisz/Zastosuj**”, aby zapisać ustawienia.

👉 Uwaga:

- 1) Dostęp do menu routera kontrolowany jest przez trzy następujące konta użytkownika: admin oraz user. Użytkownik „admin” ma nieograniczony dostęp do dokonywania zmian oraz wyświetlania konfiguracji routera. Użytkownik „user” może wyświetlić konfigurację i statystyki routera oraz zaktualizować jego oprogramowanie.
- 2) Zdalny dostęp możliwy jest dla kont „admin”. Ze względów bezpieczeństwa zalecana jest zmiana domyślnych haseł dla tych kont, jeżeli włączona jest funkcja zdalnego dostępu.
- 3) Hasło nie może zawierać spacji. Jego maksymalna długość to 16 znaków.

4.8.6.2 Zdalny dostęp

Po wybraniu opcji „**Zarządzanie**”→„**Kontrola dostępu**”→„**Zdalny dostęp**” pojawi się ekran konfiguracji zdalnego dostępu (Rysunek 4-110).

Kontrola dostępu -- Dostęp zdalny

Dostęp do routera od strony WAN z użyciem konta użytkownika (admin).

Wybrany interfejs WAN:

Web:

Telnet:

ICMP(ping):

Rysunek 4-110

- **Web:** Zaznacz tę opcję, aby włączyć zdalny dostęp do routera, przez interfejs w przeglądarce.
- **Telnet:** Zaznacz tę opcję, aby włączyć zdalny dostęp do routera przez linię komend.

- **ICMP(ping):** Zaznacz tę opcję, aby pozwolić routerowi na odpowiedź na pakiety PING.

Naciśnij przycisk „**Zapisz/Zastosuj**”, aby zapisać ustawienia.

4.8.7 Aktualizacja oprogramowania

Po wybraniu opcji „**Zarządzanie**” → „**Aktualizacja oprogramowania**” pojawi się ekran aktualizacji oprogramowania routera (Rysunek 4-111).

Narzędzia -- Aktualizacja Firmware

Krok 1: Pobierz aktualny plik firmware z naszej strony (www.tp-link.com).

Krok 2: Wprowadź ścieżkę do rozpakowanego pliku firmware w poniższe pole lub naciśnij przycisk "Przełóżaj" aby wskazać plik firmware.

Krok 3: Naciśnij przycisk "Aktualizuj Firmware" aby wczytać nowy plik firmware.

UWAGA: Proces aktualizacji trwa około 2 minut. Podczas aktualizacji router zostanie zrestartowany.

Nazwa pliku firmware:

Rysunek 4-111

- **Przełóżaj:** Naciśnij ten przycisk, aby wskazać lokalizację oprogramowania.
- **Aktualizuj Firmware:** Naciśnij ten przycisk, aby wczytać wskazany plik firmware.

Aby zaktualizować oprogramowanie routera:

1. Pobierz aktualny plik firmware z naszej strony (www.tp-link.com.pl).
2. Naciśnij przycisk „**Przełóżaj**”, aby wskazać plik firmware.
3. Naciśnij przycisk „**Aktualizuj Firmware**”.

Uwaga:

- 1) Nie ma konieczności aktualizacji oprogramowania, jeżeli nowa wersja nie wprowadza funkcji, z których chcesz skorzystać. Jeżeli występują problemy z działaniem routera, można spróbować zaktualizować oprogramowanie.
- 2) Przed aktualizacją oprogramowania zalecane jest zapisanie ustawień routera, aby zabezpieczyć się przed ewentualną utratą konfiguracji.
- 3) Nie wyłączaj routera ani nie wciskaj przycisku **RESET** z tyłu urządzenia podczas aktualizacji oprogramowania.
- 4) Po zainstalowaniu aktualizacji router samoczynnie się zrestartuje.

4.8.8 Restart

Po wybraniu opcji „**Zarządzanie**” → „**Restart**” pojawi się ekran restartu routera (Rysunek 4-112).

Restart routera

Naciśnij na przycisk poniżej aby zrestartować router.

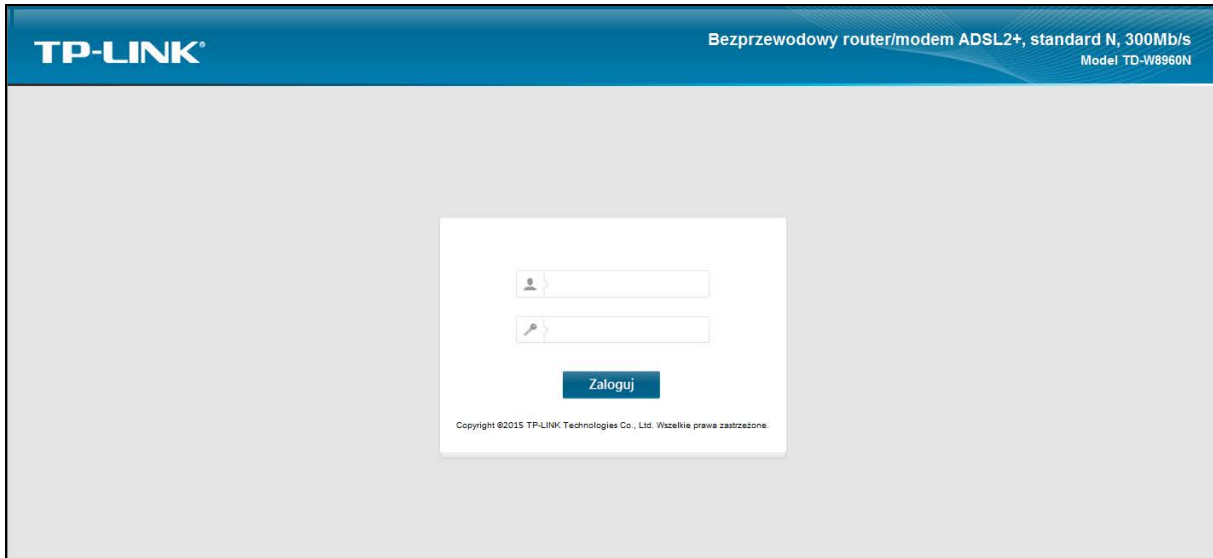
Rysunek 4-112

Uwaga:

- 1) Po naciśnięciu przycisku **Reset**, odczekaj chwilę przed ponownym otwarciem przeglądarki.
- 2) Nie wyłączaj routera ani nie wciskaj przycisku **RESET** z tyłu urządzenia podczas resetowania routera.
- 3) W razie potrzeby przeprowadź ponowną konfigurację adresu IP komputera.

4.9 Wyloguj

Po wybraniu opcji „**Wyloguj**”, powrócisz do ekranu logowania routera (Rysunek 4-113).



Rysunek 4-113

Dodatek A: Specyfikacja

Ogólne	
Standardy	ANSI T1.413, ITU G.992.1, ITU G.992.2, ITU G.992.3, ITU G.992.5, IEEE 802.3, IEEE 802.3u, IEEE 802.11b , IEEE 802.11g , 802.11n
Protokoły	TCP/IP, IPoA , PPPoA , PPPoE, SNTP, HTTP, DHCP, ICMP, NAT
Porty	Porty LAN: Cztery porty RJ45, 10/100M Auto-negocjacja (Auto MDI/MDIX)
	Jeden port RJ11
Typy kabli	10BASE-T: kable UTP kategorii 3, 4, 5 (maks. 100m) kable STP EIA/TIA-568 100Ω (maks. 100m)
	100BASE-TX: kable UTP kategorii 5, 5e (maks. 100m) kable STP EIA/TIA-568 100Ω (maks. 100m)
Diody	Power, ADSL, Internet, WLAN, WPS, 1,2,3,4(LAN)
Normy bezpieczeństwa	FCC, CE

Sieć bezprzewodowa	
Częstotliwość	2.4~2.4835GHz
Prędkość transmisji bezprzewodowej	11n: do 300Mbps (Automatycznie) 11g: 54/48/36/24/18/12/9/6Mbps (Automatycznie) 11b: 11/5.5/2/1Mbps (Automatycznie)
Rozpraszanie częstotliwości	DSSS(Direct Sequence Spread Spectrum)
Modulacja	DBPSK, DQPSK, CCK, OFDM, 16-QAM, 64-QAM
Zabezpieczenia	WEP/WPA/WPA2/WPA2-PSK/WPA-PSK
Czułość @PER	270M: -62dBm@10% PER 130M: -64dBm@10% PER 54M: -68dBm@10% PER 11M: -85dBm@8% PER 6M: -88dBm@10% PER 1M: -90dBm@8% PER

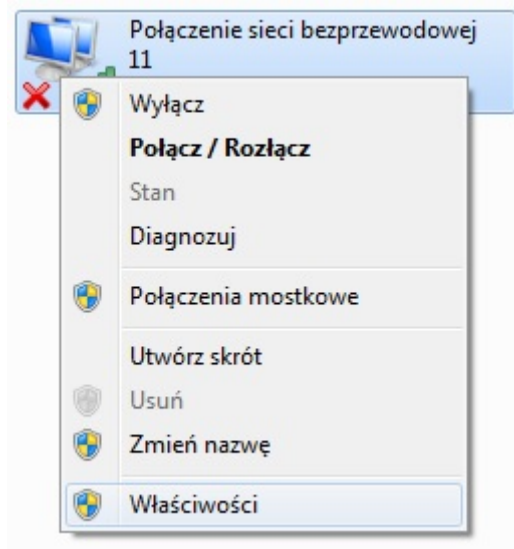
Wymagania środowiskowe	
Temperatura	Pracy: 0°C~40°C (32°F~104°F)
	Przechowywania: -40°C~70°C (-40°F~158°F)
Wilgotność	Pracy: 10% ~ 90% RH, Niekondensująca
	Przechowywania: 5% ~ 90% RH, Niekondensująca

Dodatek B: Konfiguracja komputerów

W tej sekcji opisany jest sposób prawidłowego konfigurowania parametrów TCP/IP w systemie Windows XP. Najpierw należy upewnić się, że karta Ethernet działa. W razie konieczności prosimy o skorzystanie z instrukcji obsługi karty.

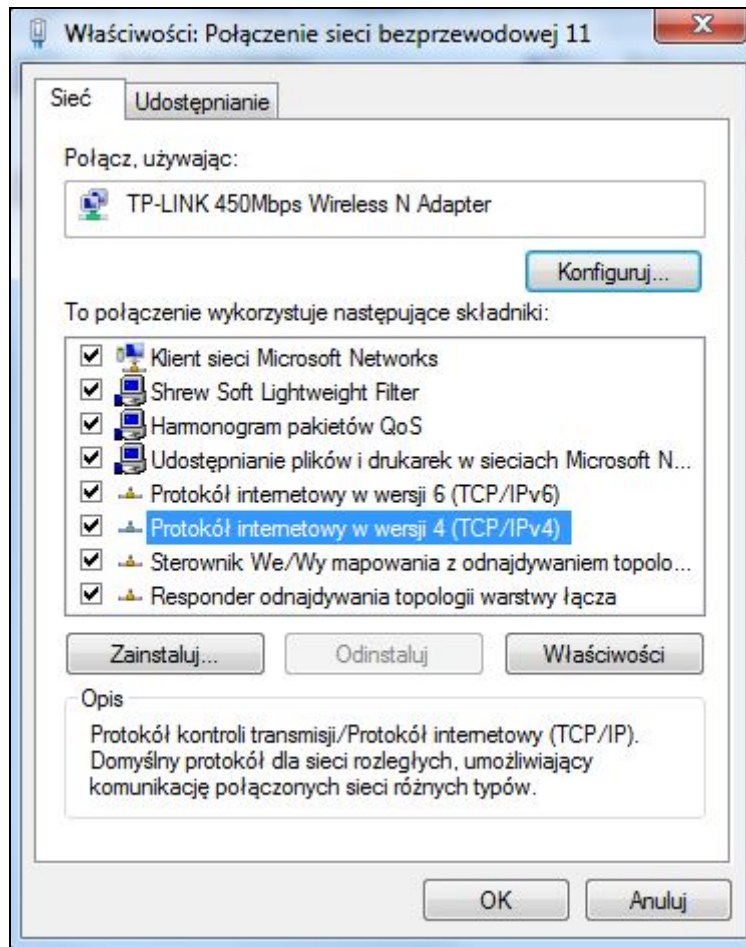
1. Konfiguracja protokołu TCP/IP

- 1) Naciśnij przycisk **Start**, wybierz **Ustawienia**, a następnie **Panel sterowania**.
- 2) Wybierz ikonę **Połączenia sieciowe i internetowe**, a następnie **Połączenia sieciowe**.
- 3) Kliknij prawym przyciskiem myszy ikonę **Połączenie lokalne** i wybierz opcję **Właściwości**.



Rysunek B-1

- 4) W oknie pokazanym poniżej kliknij dwukrotnie na **Protokół internetowy (TCP/IP)**.



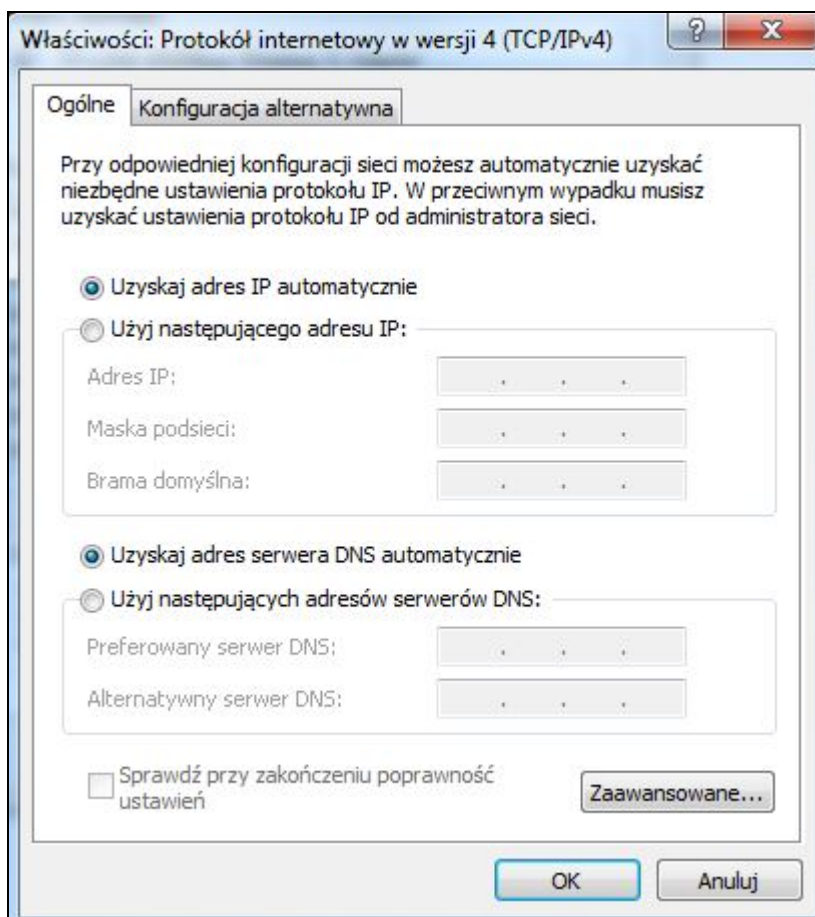
Rysunek B-2

5) Pojawi się okno **Właściwości TCP/IP**, z domyślnie otwartą zakładką **Adres IP**.

Są dwie możliwości skonfigurowania protokołu **TCP/IP**:

➤ **Uzyskiwanie adresu IP automatycznie**

Zaznacz opcje **Uzyskaj adres IP automatycznie** oraz **Uzyskaj adres serwera DNS automatycznie**, tak ja pokazano na rysunku poniżej.



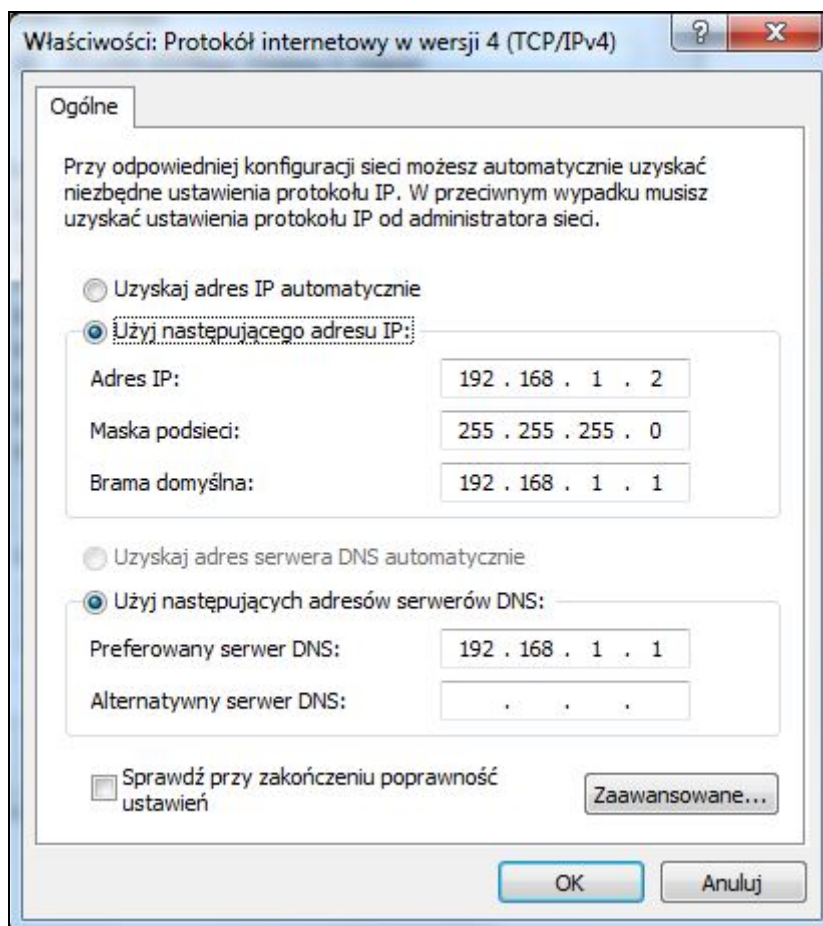
Rysunek B-3

 **Uwaga:**

W przypadku Windowsa 98 lub wersji wcześniejszych, komputer należy zrestartować.

➤ **Uzyskiwanie adresu IP ręcznie**

- 1 Zaznacz opcję **Użyj następującego adresu IP**.
- 2 Jeżeli adres LAN routera to 192.168.1.1, w polu **Adres IP** wprowadź 192.168.1.x (gdzie x to wartość z przedziału od 2 do 254), a w polu **Maska podsieci** wprowadź wartość 255.255.255.0.
- 3 W polu **Brama domyślna** wprowadź adres LAN routera (domyślny adres to 192.168.1.1).
- 4 Zaznacz opcję **Użyj następujących adresów serwerów DNS**. W polu **Preferowany serwer DNS** wprowadź taką samą wartość jak w polu **Brama domyślna** lub adres IP znanego serwera DNS.



Rysunek B-4

Naciśnij przycisk „**OK**”, aby zapisać ustawienia.

Dodatek C: Rozwiązywanie problemów

T1. Co mogę zrobić jeżeli nie znam hasła?

- 1) Domyślne hasło do sieci bezprzewodowej: Domyślne hasło do sieci bezprzewodowej znajduje się na naklejce u spodu routera.
- 2) Hasło do strony konfiguracyjnej: Przywróć router do ustawień fabrycznych. Domyślna nazwa użytkownika i hasło to: admin/admin.

T2. Jak przywrócić ustawienia fabryczne routera?

Przy włączonym zasilaniu należy przez 10 sekund przytrzymać przycisk RESET umieszczony z tyłu urządzenia.

 **Uwaga:**

Po przywróceniu ustawień fabrycznych, należy ponownie skonfigurować router – wszystkie ustawienia zostaną utracone.

T3. Co mogę zrobić jeżeli nie mogę wejść na stronę konfiguracyjną routera?

Skonfiguruj adres IP komputera:

Dla systemu Mac OS X

- Naciśnij ikonkę Apple w lewym górnym rogu ekranu.
- Wybierz „**Preferencje systemowe**”, a następnie „**Sieć**”.
- Wybierz **Airport** z menu po lewej stronie, a następnie kliknij **Zaawansowane** jeżeli łączysz się z routerem bezprzewodowo. Jeżeli masz połączenie kablowe, wybierz **Ethernet**.
- W **Konfiguracja IPv4** wybierz **Używając DHCP**.
- Naciśnij przycisk „**Zastosuj**”.



Dla systemu Windows 7

- Wybierz „**Start -> Panel sterowania -> Sieć i Internet-> Wyświetl stan sieci i zadania-> Zmień ustawienia karty sieciowej**”.
- Kliknij prawym przyciskiem myszy na **Połączenie lokalne** (lub **Połączenie sieci bezprzewodowej**), a następnie kliknij **Właściwości**.
- Zaznacz **Protokół internetowy w wersji 4 (TCP/IPv4)**, a następnie naciśnij przycisk „**Właściwości**”.
- Zaznacz opcje **Uzyskaj adres IP automatycznie** oraz **Uzyskaj adres serwera DNS automatycznie**, a następnie naciśnij przycisk „**OK**”.

Dla systemu Windows XP

- Wybierz „**Start -> Panel sterowania -> Połączenia sieciowe i internetowe-> Połączenia sieciowe**”.
- Kliknij prawym przyciskiem myszy na **Połączenie lokalne** (lub **Połączenie sieci bezprzewodowej**), a następnie kliknij **Właściwości**.
- Zaznacz **Protokół internetowy (TCP/IP)**, a następnie naciśnij przycisk „**Właściwości**”.
- Zaznacz opcje **Uzyskaj adres IP automatycznie** oraz **Uzyskaj adres serwera DNS automatycznie**, a następnie naciśnij przycisk „**OK**”.

Dla systemu Windows 8

- Przesuń myszkę w lewy dolny róg ekranu. Pojawi się ikonka **Wyszukiwanie** . Przejdź do  -> **Aplikacje**. Wpisz „**Panel sterowania**” w pasku wyszukiwania i naciśnij klawisz **Enter** na klawiaturze.
- Wybierz „**Wyświetl stan sieci i zadania**” -> „**Zmień ustawienia karty sieciowej**”.
- Kliknij prawym przyciskiem myszy na **Połączenie Ethernet** i wybierz **Właściwości**.
- Kliknij dwukrotnie na **Protokół internetowy w wersji 4 (TCP/IPv4)**. Wybierz **Uzyskaj adres IP automatycznie** oraz **Uzyskaj adres serwera DNS automatycznie**, a następnie naciśnij przycisk „**OK**”,

Następnie spróbuj zalogować się do strony konfiguracyjnej routera. Jeżeli nadal nie możesz zalogować się do routera, spróbuj przywrócić ustawienia fabryczne i skonfigurować router ponownie. W razie niepowodzenia skontaktuj się z naszą pomocą techniczną.

T4. Co mogę zrobić przy braku połączenia z Internetem?

- 1) Sprawdź czy wszystkie kable podłączone są prawidłowo.
- 2) Spróbuj zalogować się do strony konfiguracyjnej routera. Jeżeli uda się zalogować, postępuj zgodnie z poniższymi krokami. W przeciwnym wypadku skorzystaj z sekcji **T3**.
- 3) Skontaktuj się z dostawcą Internetu i upewnij się czy wszystkie wprowadzone w routerze parametry połączenia (w tym VPI/VCI, typ połączenia, nazwa użytkownika i hasło) są poprawne. W razie potrzeby popraw wprowadzone ustawienia i spróbuj ponownie.
- 4) Jeżeli nadal nie masz dostępu do Internetu, spróbuj przywrócić ustawienia fabryczne routera i skonfigurować router ponownie.
- 5) Jeżeli problem się utrzymuje, skontaktuj się z naszym wsparciem technicznym.

Uwaga:

Więcej informacji na temat rozwiązywania problemów znajduje się na naszej stronie, pod adresem <http://www.tp-link.com.pl/support>.

Dodatek D: Wsparcie techniczne

Wsparcie techniczne

- Więcej zagadnień dotyczących pomocy w rozwiązywaniu problemów znajduje się na stronie:
<http://www.tp-link.com.pl/support/faq>
- Najnowsze oprogramowanie, sterowniki i instrukcje obsługi można pobrać ze strony:
<http://www.tp-link.com.pl/support/download>
- Wsparcie techniczne można uzyskać pod następującymi adresami:

Centrala

Tel: +86 755 2650 4400

E-mail: support@tp-link.com

Czas obsługi: całodobowo, 7 dni w tygodniu

Polska

Tel: +48 (0) 801 080 618

+48 22 360 63 63 (z telefonów komórkowych)

E-mail: support.pl@tp-link.com

Czas obsługi: od poniedziałku do piątku w godz. 9:00 – 17:00