User Guide

Manage Switches via the Omada Controller

About this Guide

Omada Controller offers centralized and efficient management for configuring enterprise networks comprised of gateways, switches, wireless access points (APs), optical line terminals (OLTs), and more. This guide provides information for centrally managing switches via the Omada Controller. Please read this guide carefully before operation.
For instructions about how to use the Omada Controller, refer to the Omada Controller User Guide. For instructions about how to manage other types of devices via the Omada Controller, refer to the relevant user guides.

Intended Readers

This guide is intended for network managers familiar with IT concepts and network terminologies.

Conventions

When using this guide, notice that:

- Features available in the Omada Controller may vary due to your region, controller type and version, and device model. All images, steps, and descriptions in this guide are only examples and may not reflect your actual experience.
- The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute the warranty of any kind, express or implied. Users must take full responsibility for their application of any products.
- This guide uses the specific formats to highlight special messages. The following table lists the notice icons that are used throughout this guide.

In this guide, the following conventions are used:

Controller	Stands for the Omada On-Premises Controller and the Omada Cloud-Based Controller.
On-Premises Controller	Includes the Omada Software Controller (also referred to as the Omada Network Application), Omada Hardware Controller, and Omada Integrated Gateway (Controller).
Cloud-Based Controller/ Omada Central	The Omada Cloud-Based Controller is now referred to as the Omada Network system on the Omada Central. Note that the Omada Central integrates the Omada Network system and Omada Guard system. The Omada Network system works as an Omada Controller to manage network devices (gateways, switches, access points, OLTs, and more), while the Omada Guard system works as a VMS system to manage surveillance devices (security cameras, NVRs, and more). This guide involves instructions about the Omada Network system. For instructions about the Omada Guard system, refer to the Omada Guard User Guide.
Switch	Stands for the Omada Switch.

Note:	The note contains the helpful information for a better use of the controller.
Configuration Guidelines:	Provide guidelines for the feature and its configurations.

More Resources

Main Site	https://www.omadanetworks.com/
Video Center	https://support.omadanetworks.com/video/
Documents	https://support.omadanetworks.com/document/
Product Support	https://support.omadanetworks.com/product/
Technical Support	https://support.omadanetworks.com/contact-support/

For technical support, the latest software, and management app, visit https://support.omadanetworks.com/.

CONTENTS

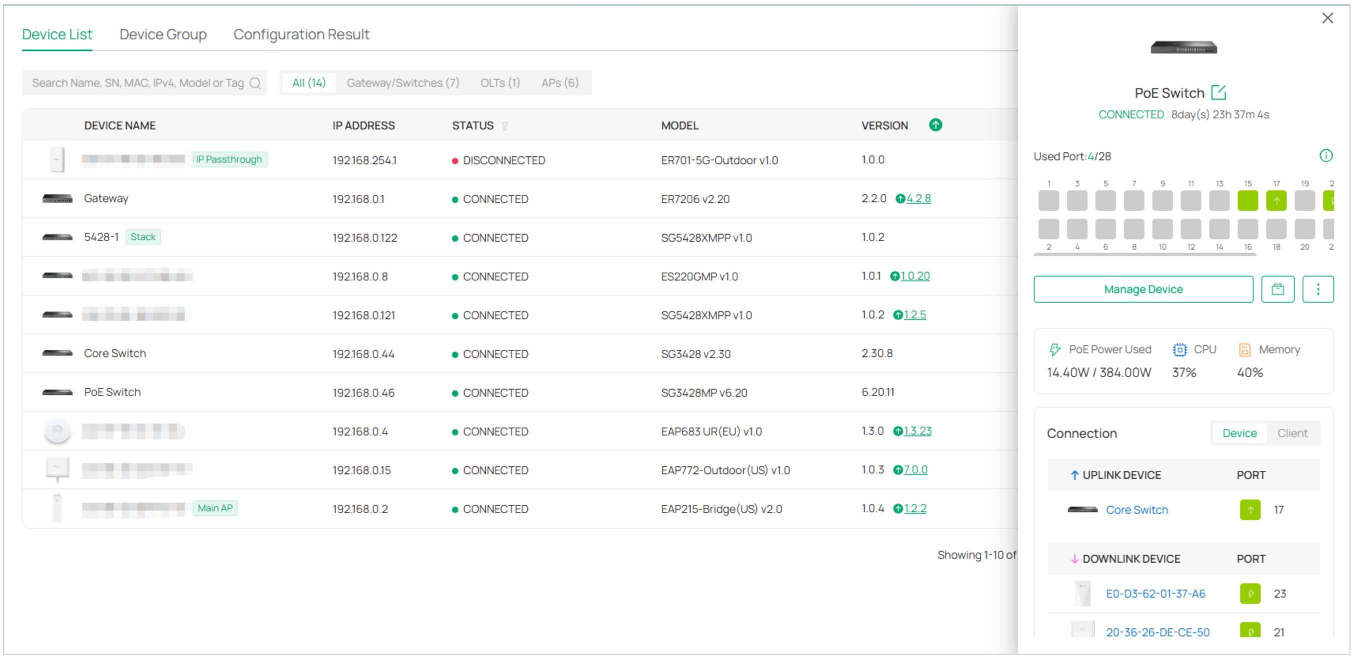
1 Manage the Switch

Launch the controller and access a site. Go to Devices > Device List. In the device list, click a switch, then you can monitor and manage it in the Properties window and Device Management window.

1.1 Properties Window

The Properties window displays the device status, port status, connection information, and other device information.

Note: The available functions in the window may vary by device model and status.



DEVICE NAME	IP ADDRESS	STATUS	MODEL	VERSION
[redacted] IP Passthrough	192.168.254.1	● DISCONNECTED	ER701-5G-Outdoor v1.0	1.0.0
Gateway	192.168.0.1	● CONNECTED	ER7206 v2.20	2.2.0 4.2.8
5428-1 Stack	192.168.0.122	● CONNECTED	SG5428XMPP v1.0	1.0.2
[redacted]	192.168.0.8	● CONNECTED	ES220GMP v1.0	1.0.1 1.0.20
[redacted]	192.168.0.121	● CONNECTED	SG5428XMPP v1.0	1.0.2 1.2.5
Core Switch	192.168.0.44	● CONNECTED	SG3428 v2.30	2.30.8
PoE Switch	192.168.0.46	● CONNECTED	SG3428MP v6.20	6.20.11
[redacted]	192.168.0.4	● CONNECTED	EAP683 UR(EU) v1.0	1.3.0 1.3.23
[redacted]	192.168.0.15	● CONNECTED	EAP772-Outdoor(US) v1.0	1.0.3 7.0.0
[redacted] Main AP	192.168.0.2	● CONNECTED	EAP215-Bridge(US) v2.0	1.0.4 1.2.2

Showing 1-10 of

PoE Switch

CONNECTED | 8day(s) 23h 37m 4s

Used Port: 4/28

PoE Power Used: 14.40W / 384.00W

CPU: 37%

Memory: 40%

Connection

UPLINK DEVICE	PORT
Core Switch	17

DOWNLINK DEVICE	PORT
E0-D3-62-01-37-A6	23
20-36-26-DE-CE-50	21

Quick Operations

Click the ⋮ icon and choose an operation to quickly operate the device.

Custom Upgrade	Click Browse and choose a file from your computer to upgrade the device. After upgraded, the device will reboot and be readopted by the controller.
Copy Configuration	Select another device at the current site to copy its configurations. **Note:** Only devices of the same model as the current device will be displayed.
Download Device Info	If the device has an abnormality, you can download the device information and provide it to our R&D personnel to analyze the problem. **Note:** Firmware updates are required for earlier devices to obtain complete information.
Move to Site	Select a site which the device will be moved to. After moving to another site, device configurations on the prior site will be replaced by that on the new site, and its traffic history will be cleared.

Force Provision	Click Force Provision to synchronize the configurations of the device with the controller. The device will lose connection temporarily, and be adopted to the controller again to get the configurations from the controller.
Forget This Device	Click Forget and then the device will be removed from the controller. Once forgotten, all configurations and history related to the device will be wiped out.

Network Tools

Click the 🧰 icon and choose a network tool to analyze the network.

Network Check	Test the device connectivity via ping or traceroute. Ping: Sends ICMP echo request packets to a destination to verify basic reachability and measure round-trip time. Traceroute: Maps the path data takes to a destination, identifying each “hop” and pinpointing where delays or packet loss occur in the route. DNS Lookup: Verifies that the switch can correctly resolve domain names to IP addresses, which is essential for cloud connectivity. ARP Table: Displays the Address Resolution Protocol table, showing the mapping between IP addresses and physical MAC addresses of devices directly connected to the switch.
Terminal	Open Terminal to execute CLI or Shell commands.
Cable Test	Perform cable test to check cable issues.

1.2 Device Management Window

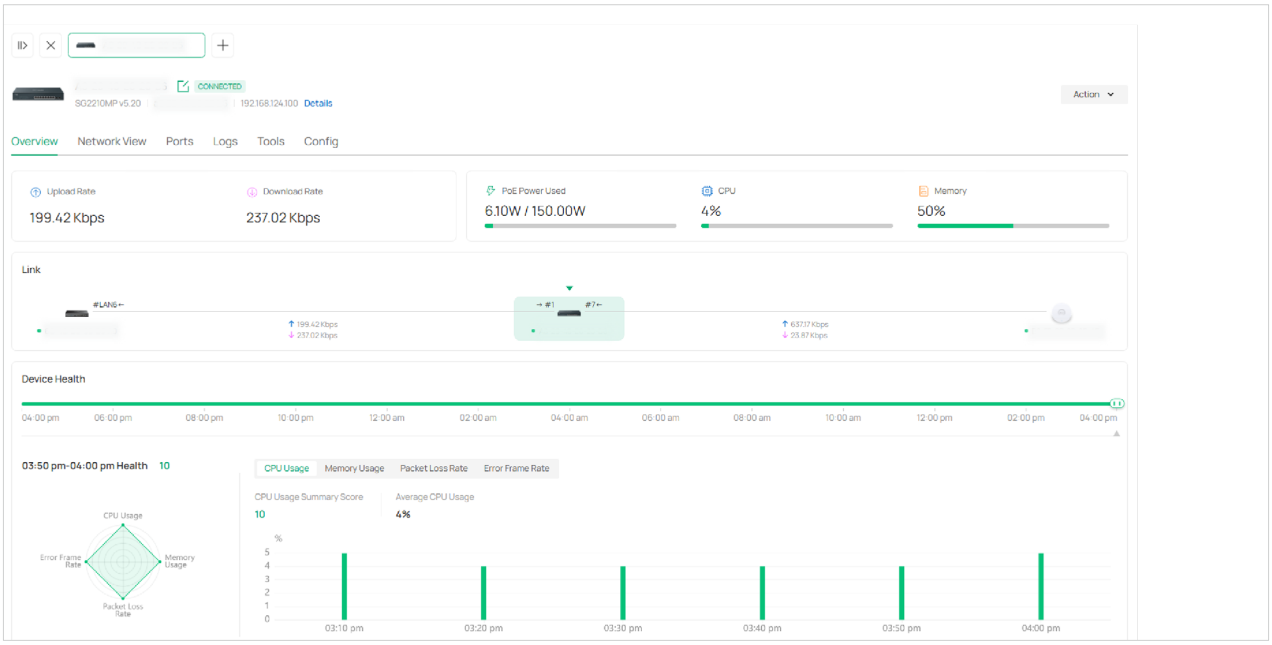
Click Manage Device to open the Device Management window to view more device details and change device settings.

In the management window, you can click + and select one or more devices to open new management windows, click the ⏵ icon in the top left to minimize the windows to the ⏴ icon in the right side, and click the ⏴ icon to reopen the minimized windows.

You can also click each tab to monitor and manage the device. The tabs available may vary by model.

Overview

In Overview, you can get an overview of the device, such as device status, link status, online time, current clients, and more.



Upload Rate: 199.42 Kbps

Download Rate: 237.02 Kbps

PoE Power Used: 6.10W / 150.00W

CPU: 4%

Memory: 50%

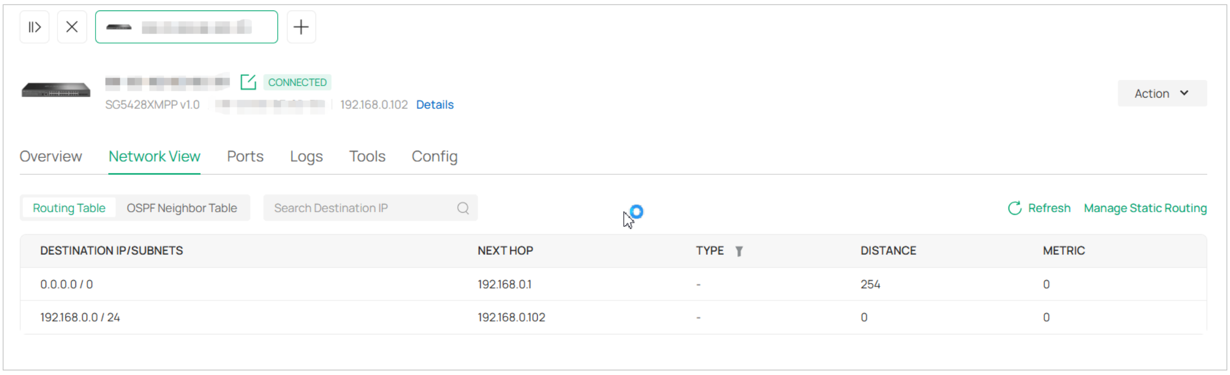
03:50 pm-04:00 pm Health 10

CPU Usage Summary Score: 10

Average CPU Usage: 4%

Network View

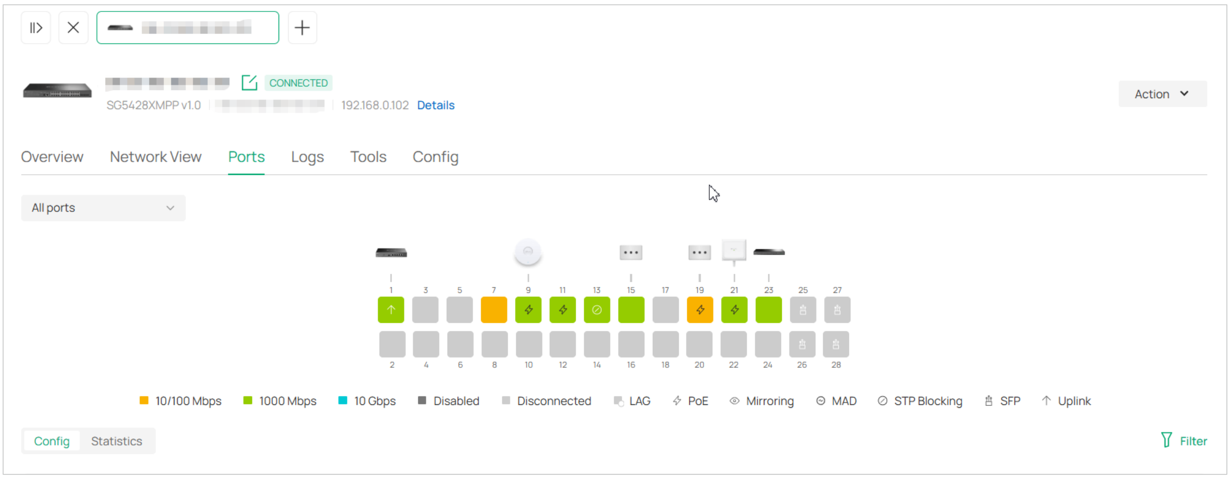
In Network View, you can check the network information of the device, such as routing table and OSPF neighbor table.



DESTINATION IP/SUBNETS	NEXT HOP	TYPE	DISTANCE	METRIC
0.0.0.0 / 0	192.168.0.1	-	254	0
192.168.0.0 / 24	192.168.0.102	-	0	0

Ports

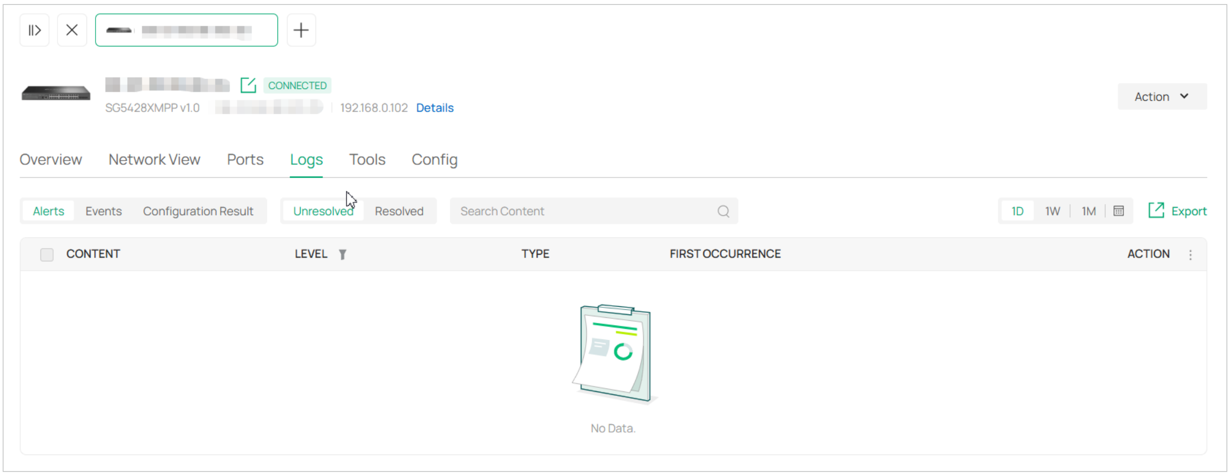
In Ports, you can view the port status and statistics and edit port settings.



To configure a port, click the edit icon in the Action column. Port settings may vary by port type. For configuration instructions, refer to Port Settings.

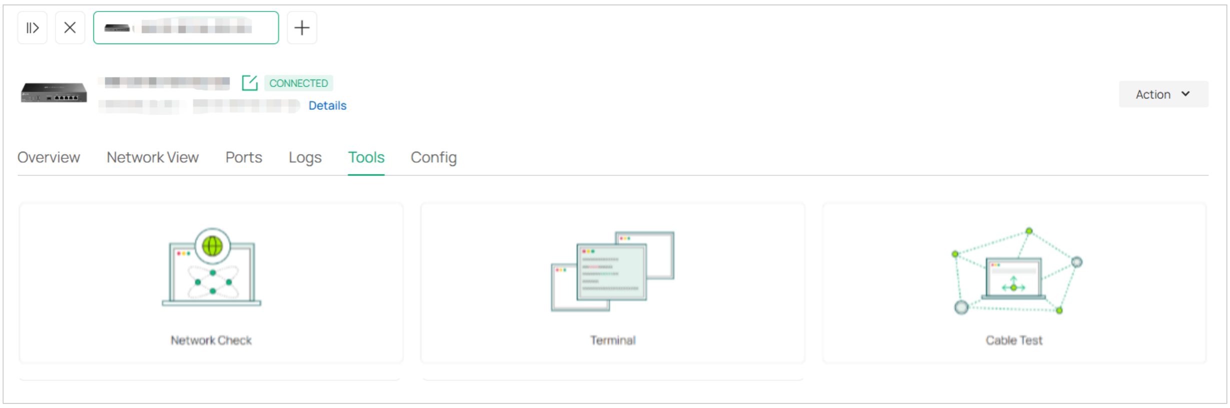
Logs

In Logs, you can check the logs of the device, such as alerts, events, and configuration result.



Tools

In Tools, you can use network tools to test the device connectivity, Open Terminal to execute CLI or Shell commands, and perform cable test to check cable issues.



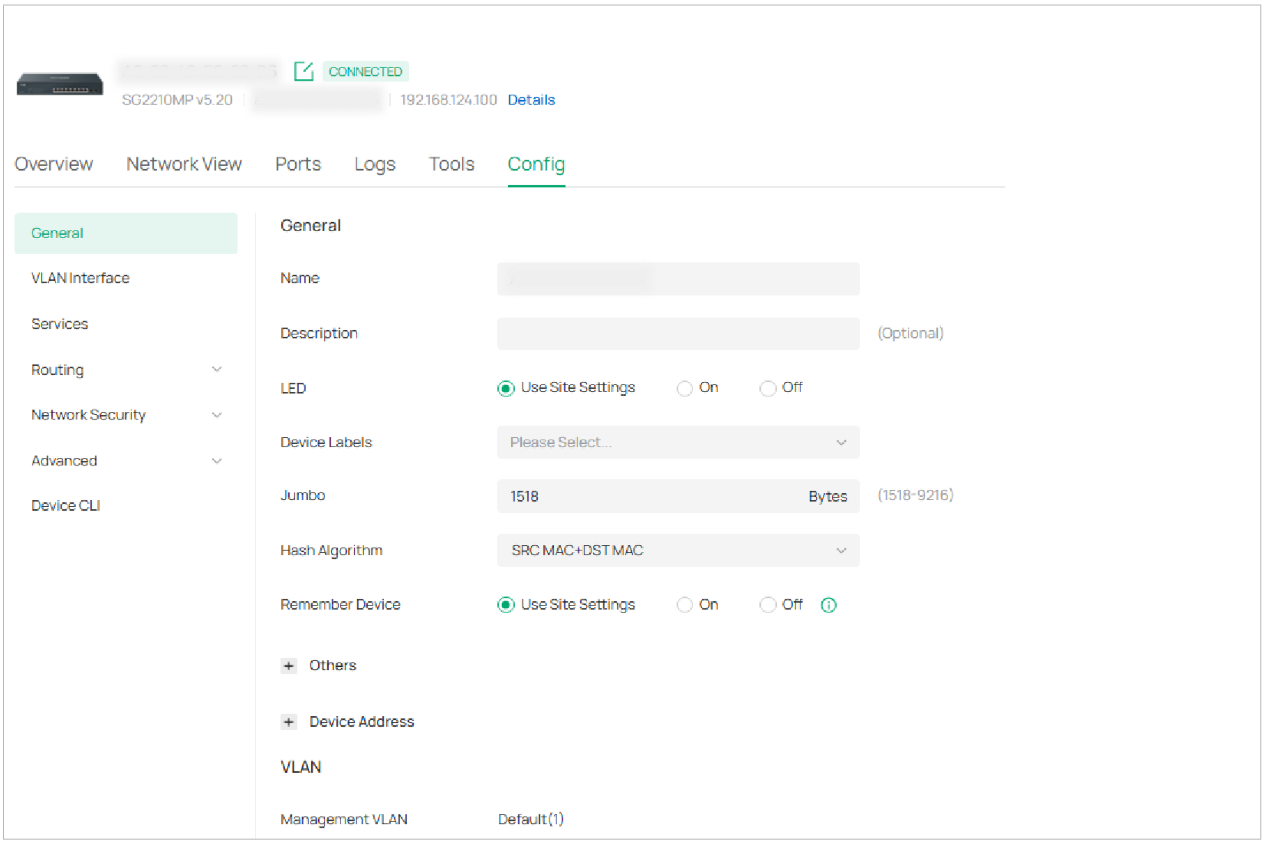
2 Configure General Settings

In General Settings, you can specify the device name, control the LED, configure the device address, and more.

To configure general settings of a switch, follow the steps below:

1. Launch the controller and access a site.
2. Go to Devices > Device List. In the device list, click a switch, click Manage Device and go to Config > General.

3. Configure the parameters.



[redacted] CONNECTED

SG2210MP v5.20 | [redacted] | 192.168.124.100 Details

General

Name: [redacted]

Description: (Optional)

LED: ● Use Site Settings ○ On ○ Off

Device Labels: Please Select...

Jumbo: 1518 Bytes (1518-9216)

Hash Algorithm: SRC MAC+DST MAC

Remember Device: ● Use Site Settings ○ On ○ Off

+ Others

+ Device Address

VLAN

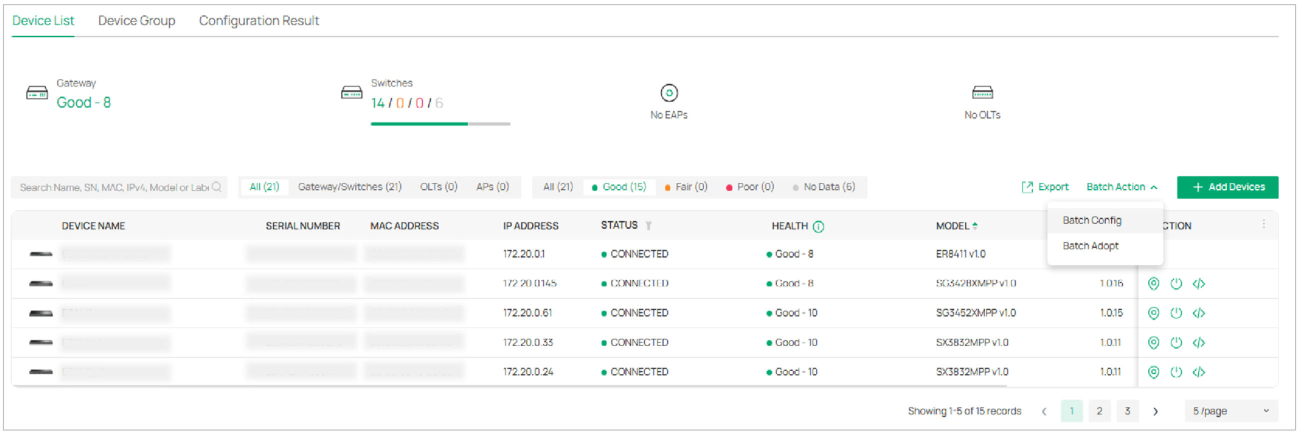
Management VLAN: Default(1)

Name	Specify a name of the device.
Description	(Optional) Enter a description for identification.
LED	Select the way that device's LEDs work. Use Site Settings: The device's LED will work following the settings of the site. On/Off: The device's LED will keep on/off.
Device Labels	Select a label from the drop-down list or create a new label to categorize the device.
Jumbo	Configure the size of jumbo frames. By default, it is 1518 bytes. Generally, the MTU (Maximum Transmission Unit) size of a normal frame is 1518 bytes. If you want the switch supports to transmit frames of which the MTU size is greater than 1518 bytes, you can configure the MTU size manually here.

Hash Algorithm	Select the Hash Algorithm, based on which the switch can choose the port to forward the received packets. In this way, different data flows are forwarded on different physical links to implement load balancing. SRC MAC: The computation is based on the source MAC addresses of the packets. DST MAC: The computation is based on the destination MAC addresses of the packets. SRC MAC+DST MAC: The computation is based on the source and destination MAC addresses of the packets. SRC IP: The computation is based on the source IP addresses of the packets. DST IP: The computation is based on the destination IP addresses of the packets. SRC IP+DST IP: The computation is based on the source and destination IP addresses of the packets.
Remember Device	With this function, the controller will remember this device. After device reset and power-on, the controller will automatically adopt the device if the controller can find it.
SNMP	Configure SNMP to write down the Location and Contact detail. You can also click Manage to jump to Network Config > General Settings > SNMP.
SDM Template	Modify the entry limit for the corresponding functions by adjusting the switch's SDM template.
Device Address	Configure the address, longitude, and latitude according to where the site is located. These fields are optional.
Management VLAN	Display the name of the current Management VLAN. To configure the Management VLAN, go to Config > VLAN Interface. Note that the controller will fail to manage your devices with wrong Management VLAN configurations. If you are not sure about your network conditions and the potential impact of any configurations, we recommend that you keep the default configurations. Refer to the Management VLAN Configuration Guide before you configure this feature.

To configure general settings in batches, follow the steps below:

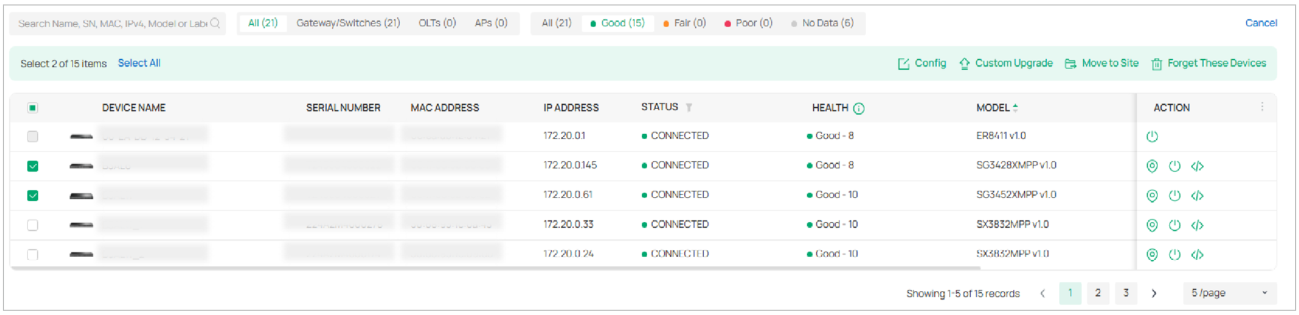
1. Launch the controller and access a site.
2. Go to Devices > Device List. In the device list, click Batch Action and then Batch Config.



DEVICE NAME	SERIAL NUMBER	MAC ADDRESS	IP ADDRESS	STATUS	HEALTH	MODEL		CTION
			172.20.0.1	● CONNECTED	● Good - 8	ER8411 v1.0		
			172.20.0.145	● CONNECTED	● Good - 8	SG3428XMPP v1.0	1.0.16	
			172.20.0.61	● CONNECTED	● Good - 10	SG3452XMPP v1.0	1.0.15	
			172.20.0.33	● CONNECTED	● Good - 10	SX3832MPP v1.0	1.0.11	
			172.20.0.24	● CONNECTED	● Good - 10	SX3832MPP v1.0	1.0.11	

Showing 1-5 of 15 records ‹ 1 2 3 › 5 /page

3. Select the switches for batch configuration and click Config.



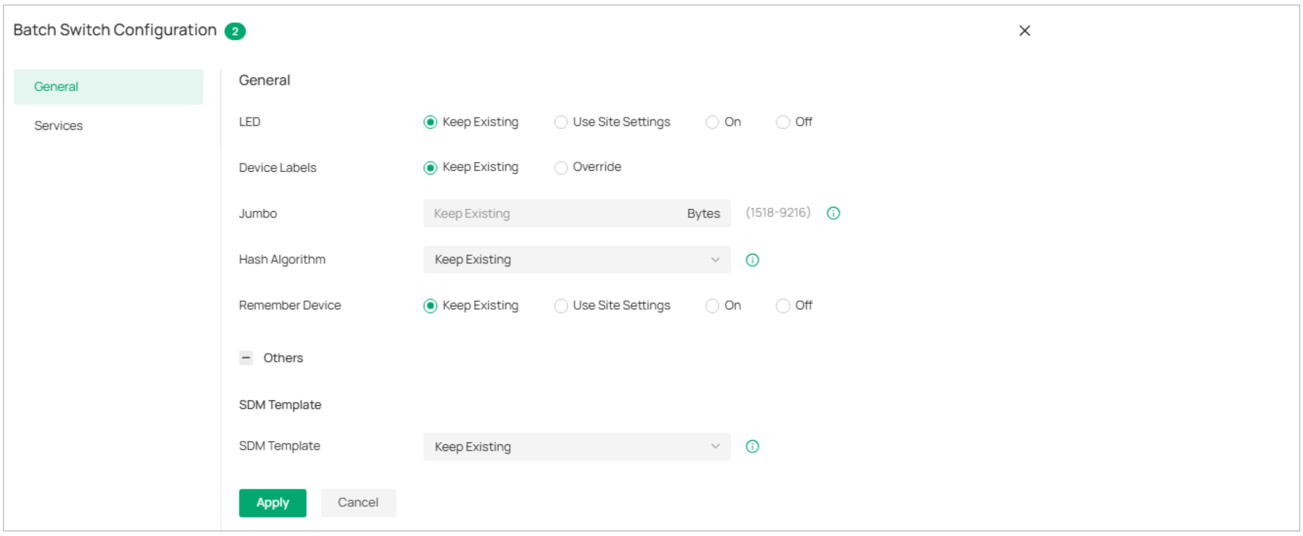
Search Name, SN, MAC, IPv4, Model or Labi | All (21) | Gateway/Switches (21) | OLTs (0) | APs (0) | All (21) | ● Good (15) | ● Fair (0) | ● Poor (0) | ● No Data (6) | Cancel

Select 2 of 15 items Select All | Config | Custom Upgrade | Move to Site | Forget These Devices

■	DEVICE NAME	SERIAL NUMBER	MAC ADDRESS	IP ADDRESS	STATUS	HEALTH	MODEL	ACTION
□	[redacted]	[redacted]	[redacted]	172.20.0.1	● CONNECTED	● Good - 8	ER8411 v1.0	
☑	[redacted]	[redacted]	[redacted]	172.20.0.145	● CONNECTED	● Good - 8	SG3428XMPP v1.0	
☑	[redacted]	[redacted]	[redacted]	172.20.0.61	● CONNECTED	● Good - 10	SG3452XMPP v1.0	
□	[redacted]	[redacted]	[redacted]	172.20.0.33	● CONNECTED	● Good - 10	SX3832MPP v1.0	
□	[redacted]	[redacted]	[redacted]	172.20.0.24	● CONNECTED	● Good - 10	SX3832MPP v1.0	

Showing 1-5 of 15 records ‹ 1 2 3 › 5 /page

4. Configure the parameters.



Batch Switch Configuration 2

General

LED: ● Keep Existing ○ Use Site Settings ○ On ○ Off

Device Labels: ● Keep Existing ○ Override

Jumbo: Keep Existing Bytes (1518-9216)

Hash Algorithm: Keep Existing

Remember Device: ● Keep Existing ○ Use Site Settings ○ On ○ Off

Others

SDM Template

SDM Template: Keep Existing

LED	Select the way that device's LEDs work. Use Site Settings: The device's LED will work following the settings of the site. On/Off: The device's LED will keep on/off.
Device Labels	Select a label from the drop-down list or create a new label to categorize the device.
Jumbo	Configure the size of jumbo frames. By default, it is 1518 bytes. Generally, the MTU (Maximum Transmission Unit) size of a normal frame is 1518 bytes. If you want the switch supports to transmit frames of which the MTU size is greater than 1518 bytes, you can configure the MTU size manually here.

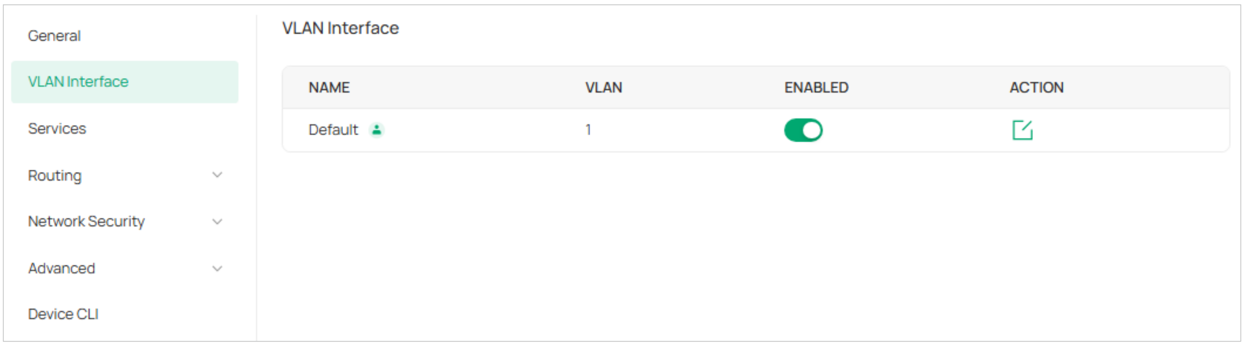
Hash Algorithm	Select the Hash Algorithm, based on which the switch can choose the port to forward the received packets. In this way, different data flows are forwarded on different physical links to implement load balancing. SRC MAC: The computation is based on the source MAC addresses of the packets. DST MAC: The computation is based on the destination MAC addresses of the packets. SRC MAC+DST MAC: The computation is based on the source and destination MAC addresses of the packets. SRC IP: The computation is based on the source IP addresses of the packets. DST IP: The computation is based on the destination IP addresses of the packets. SRC IP+DST IP: The computation is based on the source and destination IP addresses of the packets.
Remember Device	With this function, the controller will remember this device. After device reset and power-on, the controller will automatically adopt the device if the controller can find it.
SDM Template	Modify the entry limit for the corresponding functions by adjusting the switch's SDM template.

3 Configure VLAN Interface Settings

In VLAN Interface, you can enable and edit the VLAN interface.

To configure the VLAN interface of a switch, follow the steps below:

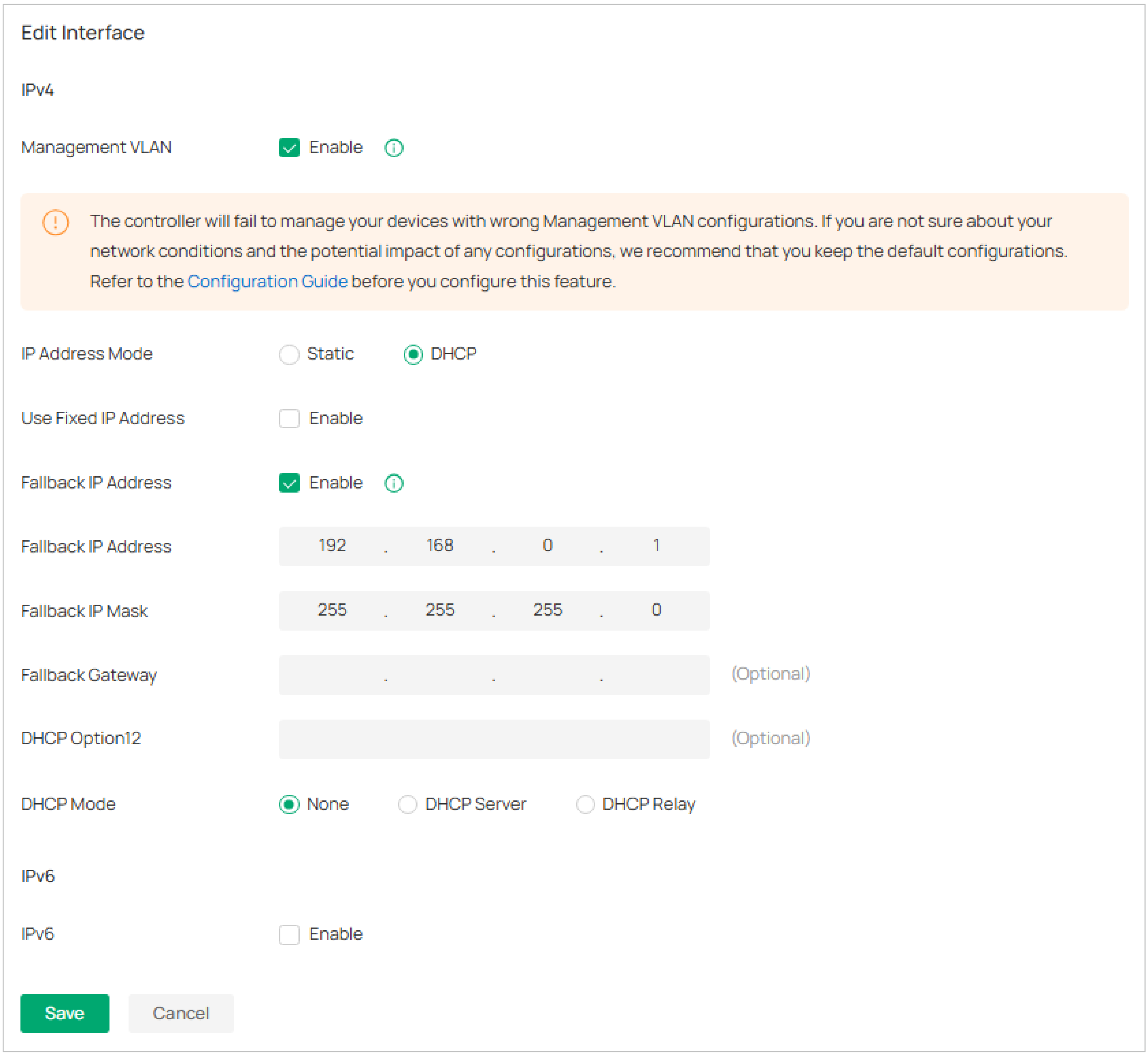
1. Launch the controller and access a site.
2. Go to Devices > Device List. In the device list, click a switch, click Manage Device and go to Config > VLAN Interface.



VLAN Interface

NAME	VLAN	ENABLED	ACTION
Default	1	●	✎

3. Click the Configure the parameters to edit the VLAN interface.



Edit Interface

IPv4

Management VLAN ☑ Enable

The controller will fail to manage your devices with wrong Management VLAN configurations. If you are not sure about your network conditions and the potential impact of any configurations, we recommend that you keep the default configurations. Refer to the Configuration Guide before you configure this feature.

IP Address Mode ○ Static ● DHCP

Use Fixed IP Address □ Enable

Fallback IP Address ☑ Enable

Fallback IP Address 192 . 168 . 0 . 1

Fallback IP Mask 255 . 255 . 255 . 0

Fallback Gateway . . . (Optional)

DHCP Option12 (Optional)

DHCP Mode ● None ○ DHCP Server ○ DHCP Relay

IPv6

IPv6 □ Enable

Management VLAN	Click the checkbox if you want to use the VLAN interface as Management VLAN. Note that the controller will fail to manage your devices with wrong Management VLAN configurations. If you are not sure about your network conditions and the potential impact of any configurations, we recommend that you keep the default configurations. Refer to the Management VLAN Configuration Guide before you configure this feature.

IP Address Mode (when Management VLAN enabled)	Select a mode for the interface to obtain its IP address, and the VLAN will communicate with other networks including VLANs with the IP address. Static: Assign an IP address to the interface manually, specify the IP Address and Subnet Mask for the interface. When the VLAN interface is set as the Management VLAN, it is optional for you to specify the Default Gateway and Primary/Secondary DNS for the interface. DHCP: Assign an IP address to the interface through a DHCP server. When you want to let device use a fixed IP address, enable Use Fixed IP Address and specify the Network and IP Address based on needs. When the VLAN interface is set as the Management VLAN, you can further enable Fallback IP Address, and specify the Fallback IP Address, Fallback IP Mask, and Fallback Gateway (optional). If the VLAN interface fails to get an IP address from the DHCP server, the fallback IP address will be used for the interface.
DHCP Option 12	When DHCP is selected as the IP Address Mode, you can specify the hostname of the DHCP client in the field. The DHCP client will use option 12 to tell the DHCP server their hostname.
DHCP Mode	Select a mode for the clients in the VLAN to obtain their IP address. None: Do not use DHCP to assign IP addresses. DHCP Server: Assign an IP address to the clients through a DHCP server. When DHCP Server is selected, you can specify the DHCP Range, and the IP addresses in the range can be assigned to the clients in the VLAN. Also, it is optional for you to specify the DHCP Option 138, Primary/Seconday DNS, Default Gateway, and Lease Time. DHCP Option 138 informs the DHCP client of the controller's IP address when the client sends a request to the DHCP server, and specify Option 138 as the controller's IP address here. Lease Time decides how long the client can use the assigned IP address. You can also click Custom Option and specify the DHCP Option code, type and value to add other DHCP Options. DHCP Relay: It allows clients in the VLAN to obtain IP addresses from a DHCP server ion different subnet. When DHCP Relay is selected, specify the IP address of the DHCP server in Server Address. Devices with the latest firmware support specifying multiple server IP addresses.
IPv6	Enable this option if you want to set up an IPv6 interface.
IPv6 Mode	Select the IPv6 mode. Dynamic IP (SLAAC/DHCPv6): In this mode, determine whether to Get Dynamic DNS or use the specified DNS addresses. Static: In this mode, set the IP address, prefix length, gateway, and DNS server for the static address.

DNS Address	Select whether to get the DNS address dynamically from your ISP or designate the DNS address manually. Get Dynamic DNS: The DNS address will be automatically assigned by the ISP. Use the Following DNS Addresses: Enter the DNS address provided by the ISP.

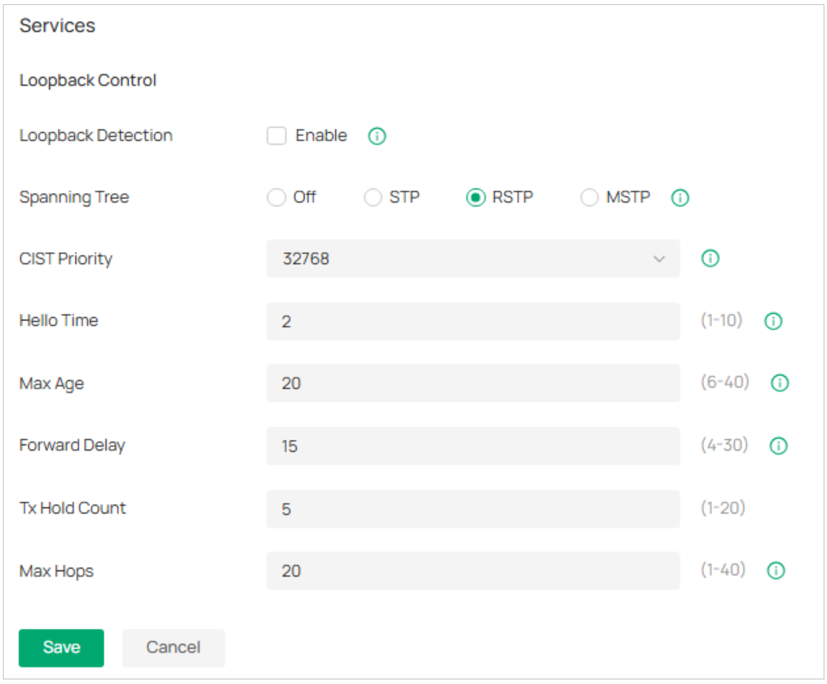
4 Configure Service Settings

4.1 Loopback Control

In Services, you can configure Loopback Control for the switch.

To configure the Loopback Control settings of a switch, follow the steps below:

1. Launch the controller and access a site.
2. Go to Devices > Device List. In the device list, click a switch, click Manage Device and go to Config > Services.
3. Configure the parameters.



Services

Loopback Control

Loopback Detection	□ Enable	
Spanning Tree	○ Off ○ STP ● RSTP ○ MSTP	
CIST Priority	32768	
Hello Time	2	(1-10)
Max Age	20	(6-40)
Forward Delay	15	(4-30)
Tx Hold Count	5	(1-20)
Max Hops	20	(1-40)

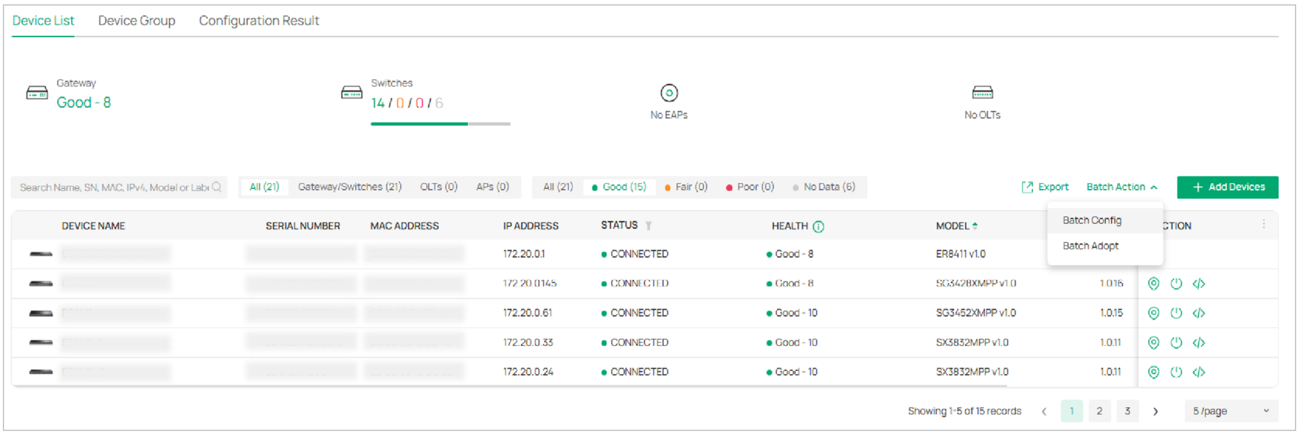
Loopback Detection	When enabled, the switch checks the network regularly to detect the loopback. Note that Lopback Detection and Spanning Tree are not available at the same time.

Spanning Tree	Select a mode for Spanning tree. This feature is available only when Loopback Detection is disabled. Off: Disable Spanning Tree on the switch. STP: Enable STP (Spanning Tree Protocal) to prevent loops in the network. STP helps to block specific ports of the switches to build a loop-free topology and detect topology changes and automatically generate a new loop-free topology. RSTP: Enable RSTP (Rapid Spanning Tree Protocal) to prevent loops in the network. RSTP provides the same features as STP with faster spanning tree convergence. MSTP: Enable MSTP (Multiple Spanning Tree Protocal) to prevent loops in the network. MSTP is the extension of STP and RSTP.
CIST Priority	Specify the CIST priority for the switch. It determines the root bridge election in the spanning tree. A smaller value indicates higher priority, and the switch with the highest priority will be elected as the root bridge.
Hello Time	Specify the interval for sending BPDUs to detect link failures. It works with Max Age to monitor link status and maintain the spanning tree.
Max Age	Specify the aging time of BPDU (Bridge Protocol Data Unit) packets, which refers to the maximum duration a switch will wait to regenerate a new spanning tree if no BPDUs are received.
Forward Delay	When a link failure triggers spanning tree recalculation, the new configuration messages generated from the recalculation cannot propagate throughout the network immediately. After a delay of twice the Forward Delay interval, this latency ensures that new configuration messages have fully propagated across the network, thus preventing the formation of temporary loops.
Tx Hold Count	Specify the maximum number of BPDU that can be sent in a second.
Max Hops	BPDUs are discarded when their hop count reaches zero. This value controls the scale of the spanning tree in an MST region. Switches decrement the hop count by 1 before forwarding BPDUs.
QoS	Select the QoS rules. DSCP 802.1p Mapping: Select the rule for DSCP 802.1p Mapping. The DSCP 802.1p Mapping function is used to match the DSCP priority in different packets, then map them to the 802.1p priority. This rule has a lower priority than the VLAN Priority Mapping rule. 802.1p Queue Mapping: Select the rule for 802.1p Queue Mapping. The 802.1p Queue Mapping function is used to classify the packets based on the value of 802.1p priority, then map them to different queues. Queue Scheduler Profile: Select the Queue Scheduler profile.The Queue Scheduler Profile function is used to set the scheduler rule for the corresponding 802.1p queue.

To configure the Loopback Control settings in batches, follow the steps below:

1. Launch the controller and access a site.

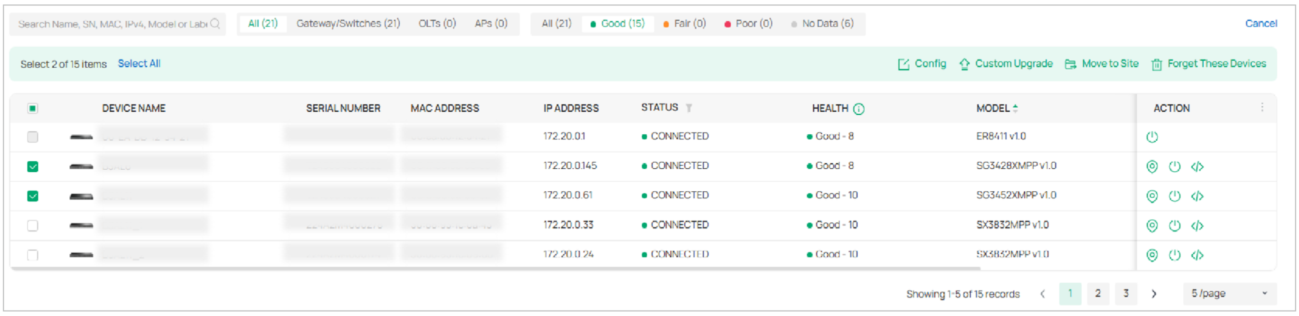
2. Go to Devices > Device List. In the device list, click Batch Action and then Batch Config.



DEVICE NAME	SERIAL NUMBER	MAC ADDRESS	IP ADDRESS	STATUS	HEALTH	MODEL		ACTION
[redacted]	[redacted]	[redacted]	172.20.0.1	● CONNECTED	● Good - 8	ER8411 v1.0		
[redacted]	[redacted]	[redacted]	172.20.0.145	● CONNECTED	● Good - 8	SG3428XMPP v1.0	1.0.16	
[redacted]	[redacted]	[redacted]	172.20.0.61	● CONNECTED	● Good - 10	SG3452XMPP v1.0	1.0.15	
[redacted]	[redacted]	[redacted]	172.20.0.33	● CONNECTED	● Good - 10	SX3832MPP v1.0	1.0.11	
[redacted]	[redacted]	[redacted]	172.20.0.24	● CONNECTED	● Good - 10	SX3832MPP v1.0	1.0.11	

Showing 1-5 of 15 records ‹ 1 2 3 › 5 /page

3. Select the switches for batch configuration and click Config.

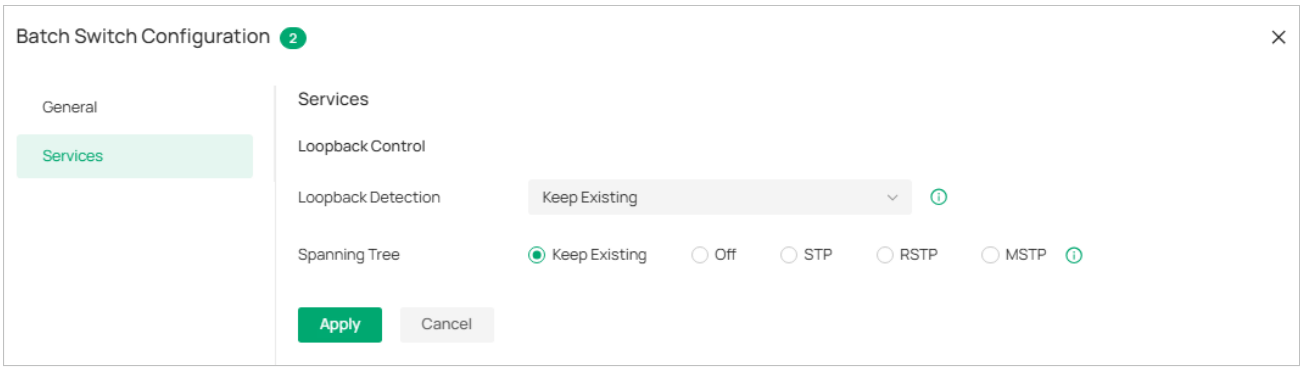


Select 2 of 15 items

■	DEVICE NAME	SERIAL NUMBER	MAC ADDRESS	IP ADDRESS	STATUS	HEALTH	MODEL	ACTION
□	[redacted]	[redacted]	[redacted]	172.20.0.1	● CONNECTED	● Good - 8	ER8411 v1.0	
☑	[redacted]	[redacted]	[redacted]	172.20.0.145	● CONNECTED	● Good - 8	SG3428XMPP v1.0	
☑	[redacted]	[redacted]	[redacted]	172.20.0.61	● CONNECTED	● Good - 10	SG3452XMPP v1.0	
□	[redacted]	[redacted]	[redacted]	172.20.0.33	● CONNECTED	● Good - 10	SX3832MPP v1.0	
□	[redacted]	[redacted]	[redacted]	172.20.0.24	● CONNECTED	● Good - 10	SX3832MPP v1.0	

Showing 1-5 of 15 records ‹ 1 2 3 › 5 /page

4. Configure the parameters.



Services

Loopback Control

Loopback Detection: Keep Existing

Spanning Tree: ● Keep Existing ○ Off ○ STP ○ RSTP ○ MSTP

Loopback Detection	When enabled, the switch checks the network regularly to detect the loopback. Note that Lopback Detection and Spanning Tree are not available at the same time.

Spanning Tree	Select a mode for Spanning tree. This feature is available only when Loopback Detection is disabled. Off: Disable Spanning Tree on the switch. STP: Enable STP (Spanning Tree Protocal) to prevent loops in the network. STP helps to block specific ports of the switches to build a loop-free topology and detect topology changes and automatically generate a new loop-free topology. RSTP: Enable RSTP (Rapid Spanning Tree Protocal) to prevent loops in the network. RSTP provides the same features as STP with faster spanning tree convergence. MSTP: Enable MSTP (Multiple Spanning Tree Protocal) to prevent loops in the network. MSTP is the extension of STP and RSTP.

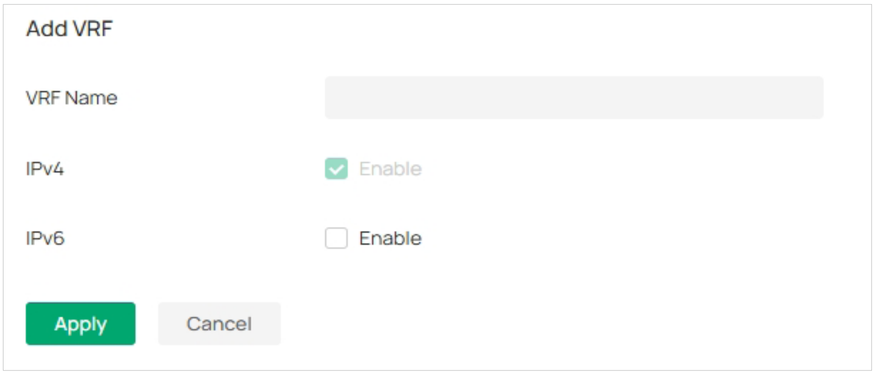
4.2 VRF (Only for certain models)

In Services, you can add VRF instances to enhance functionality by enabling the division of network paths without requiring multiple devices, effectively transforming one physical router into multiple virtual routers.

To add a VRF instance, click Add and configure the parameters.

To configure the VRF settings of a switch, follow the steps below:

1. Launch the controller and access a site.
2. Go to Devices > Device List. In the device list, click a switch, click Manage Device and go to Config > Advanced > VRF.
3. Click Add to add a VRF instance and configure the parameters.



Add VRF

VRF Name

IPv4 ☑ Enable

IPv6 □ Enable

VRF Name	Specify the VRF instance name.
IPv4	Check the box to enable IPv4 for the instance.
IPv6	Check the box to enable IPv6 for the instance.

5 Configure Routing Settings

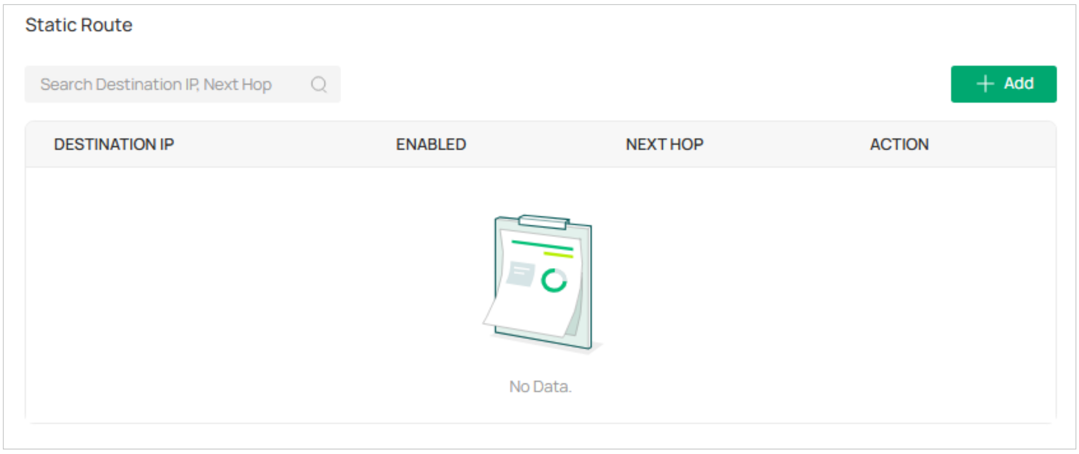
5.1 Static Route

In Routing, you can configure the Static Route of the switch.

Network traffic is oriented to a specific destination, and Static Route designates the next hop or interface where to forward the traffic.

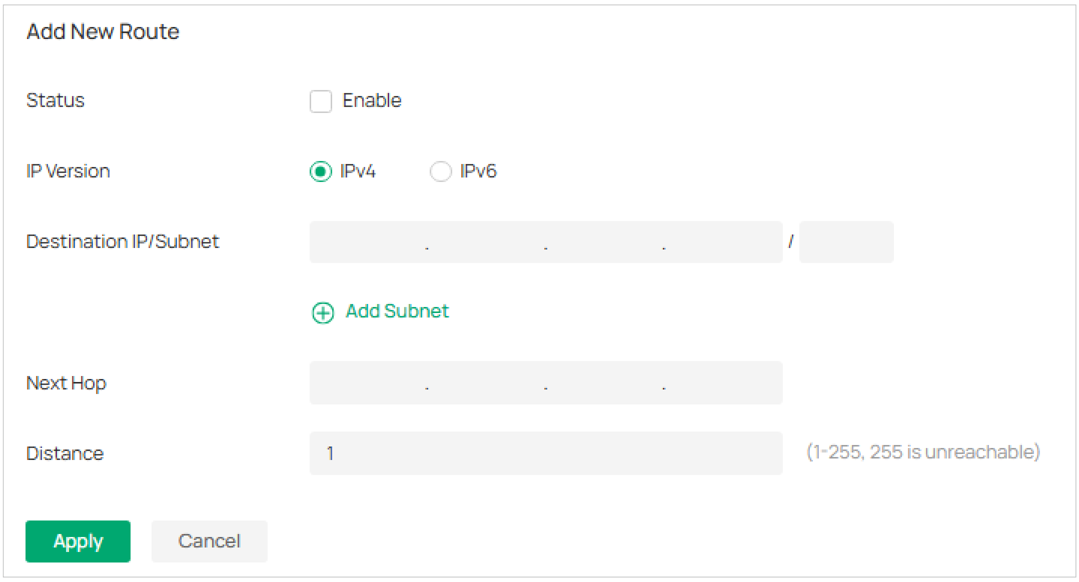
To configure the Static Route settings of a switch, follow the steps below:

1. Launch the controller and access a site.
2. Go to Devices > Device List. In the device list, click a switch, click Manage Device and go to Config > Routing > Static Route.



DESTINATION IP	ENABLED	NEXT HOP	ACTION

3. Click Add to add a new route and configure the parameters.



Status: □ Enable

IP Version: ● IPv4 ○ IPv6

Destination IP/Subnet: . . . /

Next Hop: . . .

Distance: 1

Status	Click the checkbox to enable the static route entry.

IP Version	Specify the IP version. With IPv4 selected, specify the Destination IP/Subnet of the network traffic. The traffic will be forwarded to the specified destination. With IPv6 selected, specify the Destination IP/Prefix Length of the network traffic. The traffic will be forwarded to the specified destination.
Next Hop	Specify the IP address as the next hop. The device will forward the corresponding network traffic to the specific IP address.
Distance	Specify the distance. It ranges from 1 to 255, and 255 is unreachable.

5.2 OSPF (Only for certain models)

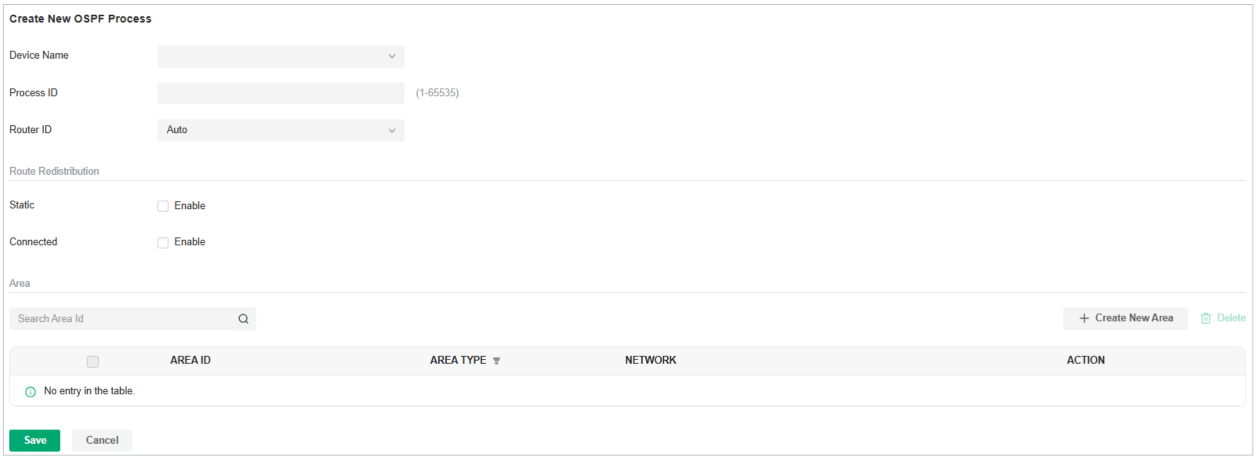
In Routing, you can configure the OSPF of the switch.

The OSPF protocol (Open Shortest Path First) is a link-state-based dynamic routing protocol that uses Dijkstra's SPF (shortest path first) algorithm to calculate routes within a single AS (autonomous system). OSPF establishes a link state database by advertising the state of network interfaces between routers, and generates shortest path trees. Other OSPF routers in the area use these shortest paths to construct routes.

To configure the OSPF settings of a switch, follow the steps below:

1. Launch the controller and access a site.
2. Go to Devices > Device List. In the device list, click a switch, click Manage Device and go to Config > Routing > OSPF.

   In OSPF Process, you can add an OSPF process and configure the following parameters:



Create New OSPF Process

Device Name

Process ID (1-65535)

Router ID: Auto

Route Redistribution

Static □ Enable

Connected □ Enable

Area

Search Area Id

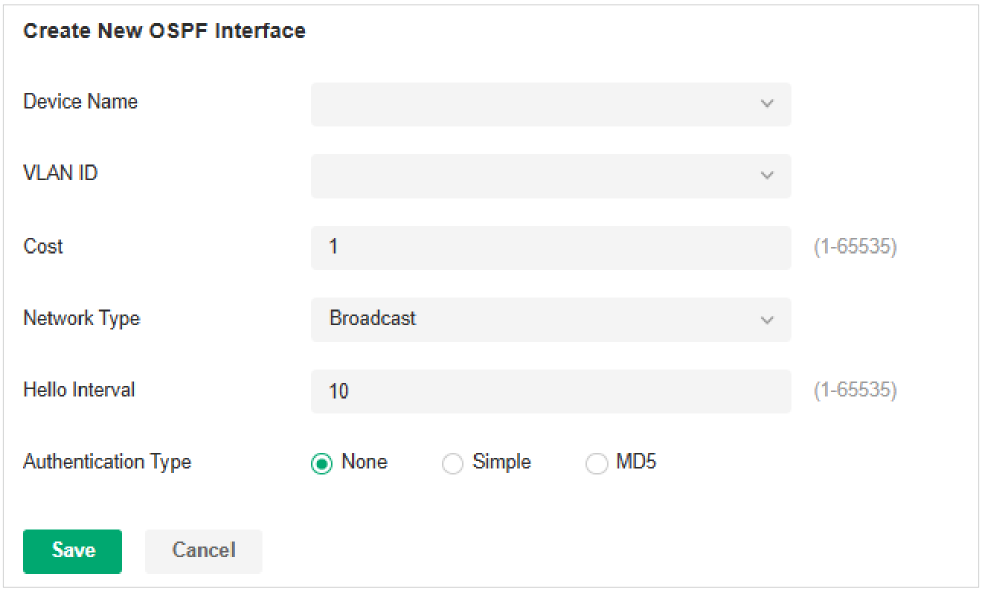
□	AREA ID	AREA TYPE	NETWORK	ACTION

No entry in the table.

Process ID	Enter a number between 1 and 65535 to identify the OSPF process locally on the router.
Router ID	Specify the identity of the router. The selection priority order is manually configured interface, loopback interface, then physical interface.

Static	Check the box to enable static route. With this option selected, configure the following parameters: Metric: Specify the path cost when importing external routes. Metric Type: Specify the cost calculation type. Type 1 calculates internal cost and external cost. Type 2 calculates external cost only. The default value is type 2.
Connected	Check the box to enable direct route.
Area	Configure the OSPF areas.

In OSPF Interface, you can add an OSPF interface and configure the following parameters:



Create New OSPF Interface

Device Name		
VLAN ID		
Cost	1	(1-65535)
Network Type	Broadcast	
Hello Interval	10	(1-65535)
Authentication Type	● None ○ Simple ○ MD5	

VLAN ID	Specify the ID of the VLAN.
Cost	Specify the interface overhead.
Network Type	Specify the network type of the OSPF interface.
Hello Interval	Specify the interval between Hello packets sent on the interface.
Dead Interval	Set the number of seconds after the last device hello packet was seen before its neighbors declare the OSPF router to be down.
Authentication Type	Specify the interface area verification method. None: No authentication. Simple: Simple authentication mode. The key is transmitted with clear texts. With this option selected, specify the Simple Key for authentication. MD5: MD5 authentication mode. The key and key ID are transmitted through MD5 encryption. With this option selected, specify the MD5 Key ID and MD5 Key for authentication.

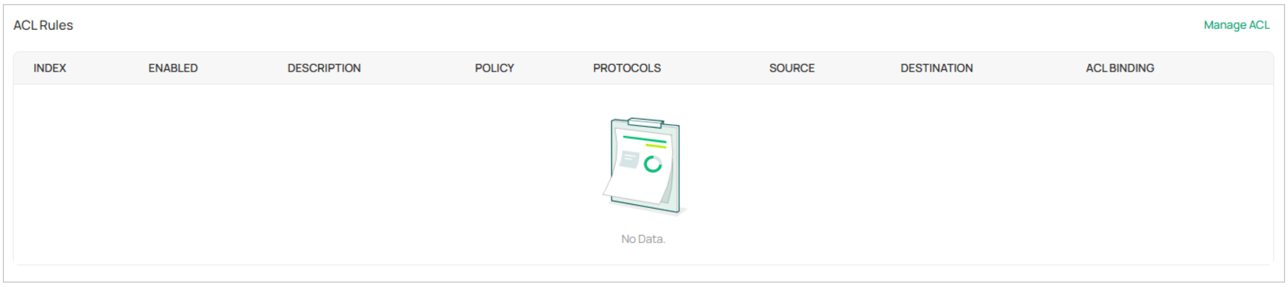
6 Configure Network Security Settings

In Network Security, you can view the ACL rules of the switch.

ACL (Access Control List) allows a network administrator to create rules to restrict access to network resources. ACL rules filter traffic based on specified criteria such as source IP addresses, destination IP addresses, and port numbers, and determine whether to forward the matched packets.

To configure the ACL rules of a switch, follow the steps below:

1. Launch the controller and access a site.
2. Go to Devices > Device List. In the device list, click a switch, click Manage Device and go to Config > Network Security > ACL.



ACL Rules

Manage ACL

INDEX	ENABLED	DESCRIPTION	POLICY	PROTOCOLS	SOURCE	DESTINATION	ACL BINDING

No Data.

3. Click Manage ACL to redirect to the Switch ACL page of the site to create and edit ACL rules. For detailed instructions about ACL, refer to the Omada Controller User Guide.

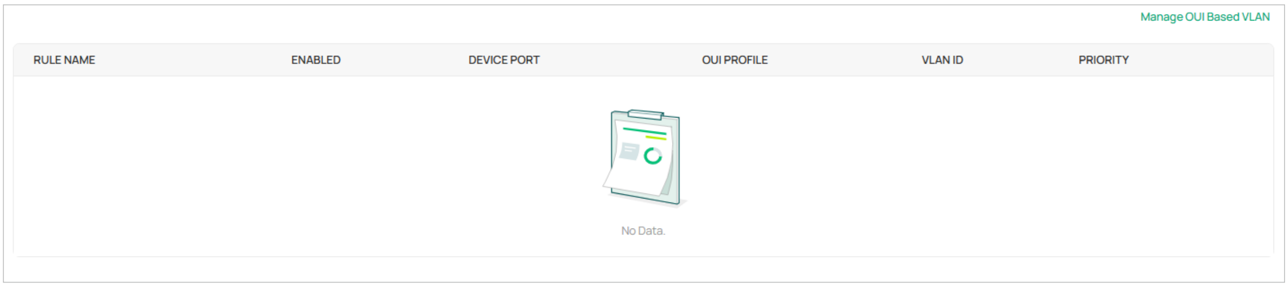
7 Configure Advanced Settings

In Advanced settings, you can view the OUI Based VLAN of the switch.

The OUI Based VLAN function can perform VLAN and priority division and processing on device data packets starting with specific MAC addresses based on OUIs.

To configure the OUI Based VLAN rules of a switch, follow the steps below:

1. Launch the controller and access a site.
2. Go to Devices > Device List. In the device list, click a switch, click Manage Device and go to Config > Advanced > OUI Based VLAN.



Manage OUI Based VLAN

RULE NAME	ENABLED	DEVICE PORT	OUI PROFILE	VLAN ID	PRIORITY

No Data.

3. Click Manage OUI Based VLAN to redirect to the OUI Based VLAN page of the site to create and edit switch rules. For detailed instructions about OUI Based VLAN, refer to the Omada Controller User Guide.

8 Configure Device CLI Settings

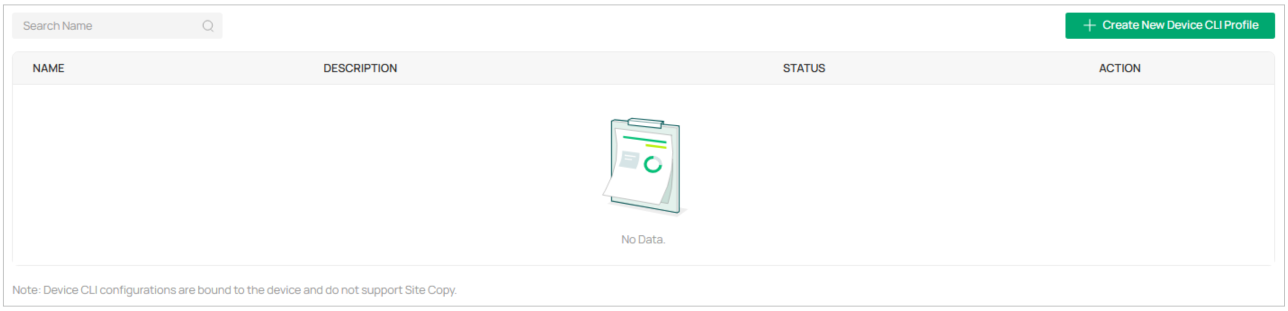
In Device CLI, you can configure the Device CLI settings of the switch.

Device CLI enables batch configuration of specific devices via command lines. Device CLI supports variables. You can use the %x% format to define a variable x, and then set different values for different switches. When the Controller applies the Device CLI configuration to switches, it will automatically modify the variable %x% to the values you set.

To configure the Device CLI settings of a switch, follow the steps below:

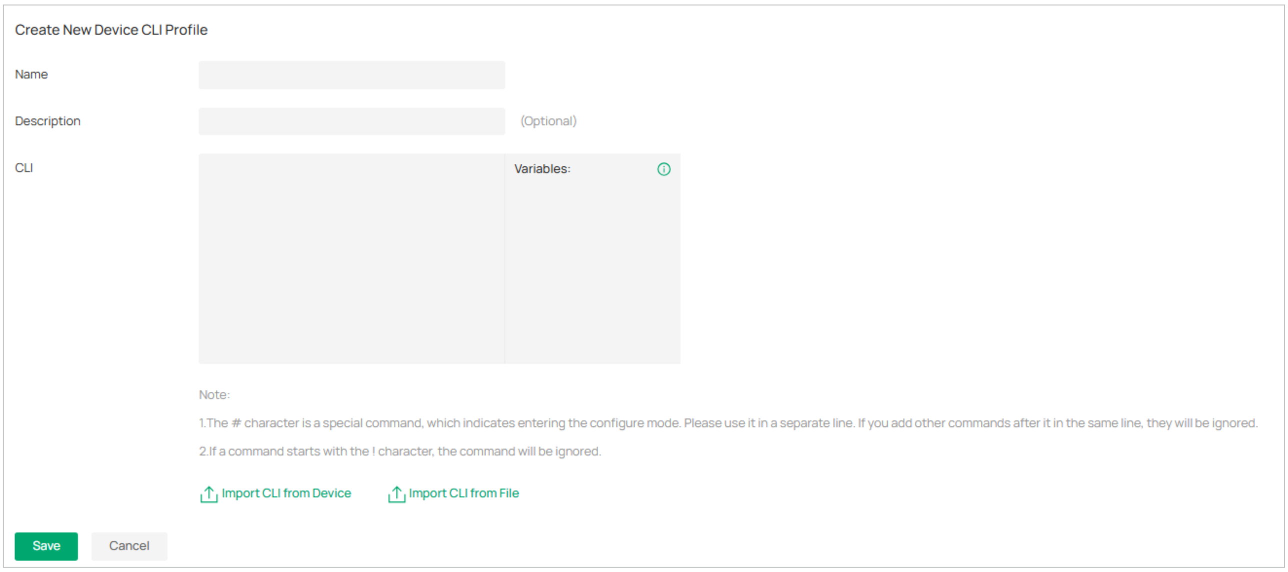
1. Launch the controller and access a site.
2. Go to Devices > Device List. In the device list, click a switch, click Manage Device and go to Config > Device CLI.

   Note: Device CLI configurations are bound to the device and do not support Site Copy.



Note: Device CLI configurations are bound to the device and do not support Site Copy.

3. Click Create New Device CLI Profile and create a CLI profile according to your needs. Click Save to create the profile. The new profile is in inactive state and will not be applied to the device.



Note:

1.The # character is a special command, which indicates entering the configure mode. Please use it in a separate line. If you add other commands after it in the same line, they will be ignored.

2.If a command starts with the ! character, the command will be ignored.

Note:

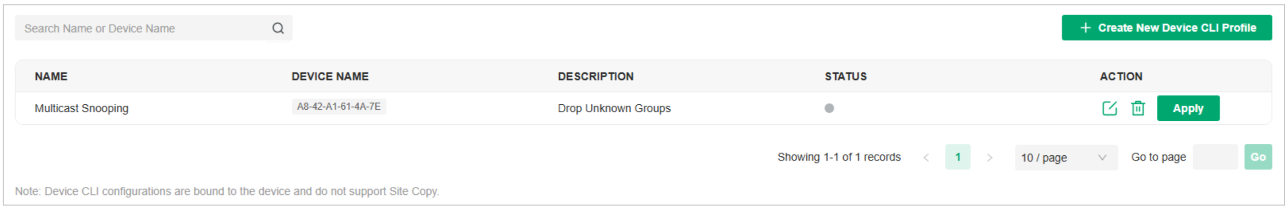
• The # character is a special command, which indicates entering the configure mode. Please use it in a separate line. If you add other commands after it in the same line, they will be ignored.

• If a command starts with the ! character, the command will be ignored.

Name	Specify the name of the CLI profile.
Description	(Optional) Enter a description for identification.

CLI	Enter the command lines manually. You can enter %xxx% in the CLI template to define variables.
Import CLI from Device	Click and select a device that supports CLI configuration to import its running config.
Import CLI from File	Click and select an existing command file to import command lines.

4. Click Apply to apply the CLI. The profile will change to active state and apply configurations to the device.



NAME	DEVICE NAME	DESCRIPTION	STATUS	ACTION
Multicast Snooping	A8-42-A1-61-4A-7E	Drop Unknown Groups	●	Apply

Showing 1-1 of 1 records   1   10 / page   Go to page

Note: Device CLI configurations are bound to the device and do not support Site Copy.

Note: Once the profile becomes active, you will be unable to edit it.

5. To check whether the profile is successfully applied to devices and takes effect, click View CLI Details to view the configuration results on the Devices > Application Result page.

Note: Deleting a CLI profile will not take effect on existing configurations on devices. To delete the configurations, use the "no" command.

9 Configure Switch Ports

9.1 Port Profile

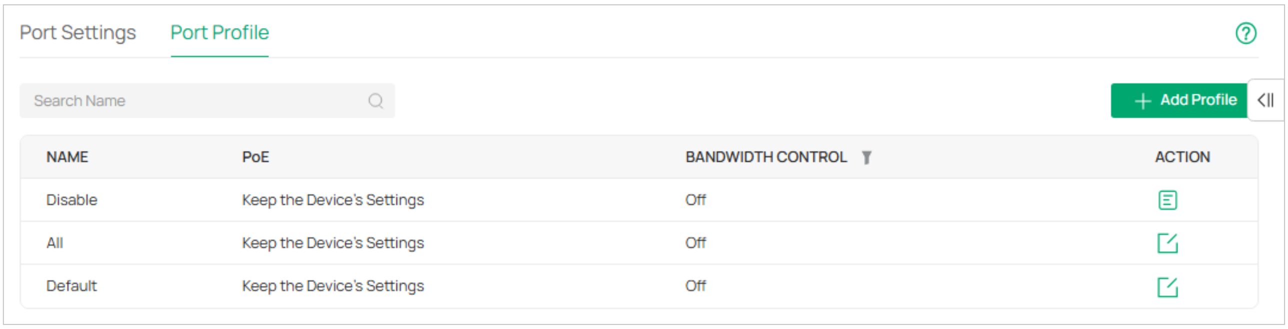
The Switch Port Profile allows you to create port configuration profiles for fast, bulk configuration of switch port parameters.

Note: The port network configurations previously included in the Switch Port Profile have been removed. To configure these settings, please go to Port Settings or switch's Properties Window > Manage Device > Ports.

To configure the Port Profile of a switch, follow the steps below:

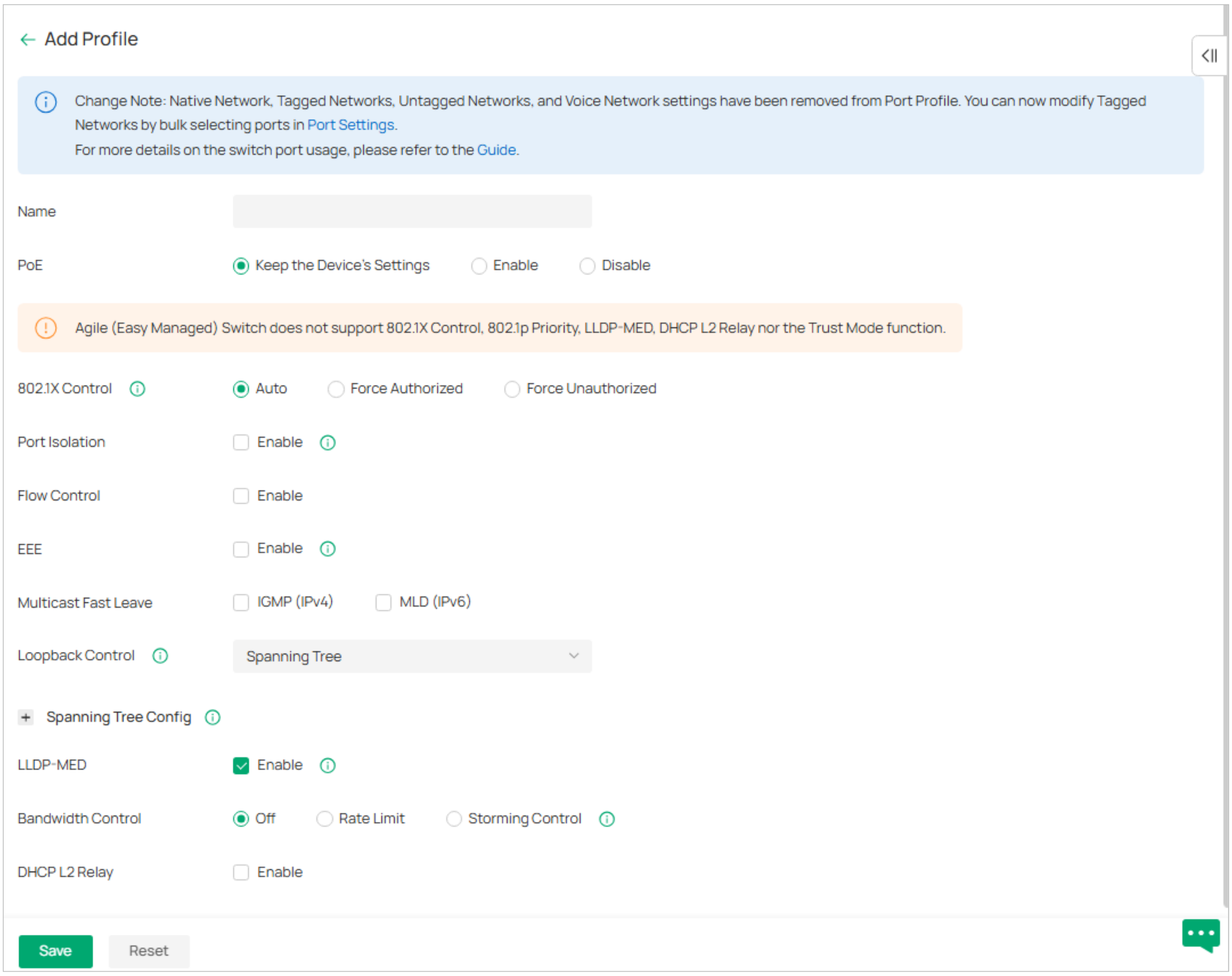
1. Launch the controller and access a site.
2. Go to Device Config > Switch > Switch Ports > Port Profile.

Three port profiles are preconfigured on the controller: Default, Disable, and All. You can click the view icon to check the Disable profile, or click the edit icon to view and edit the Default or All profile.



NAME	PoE	BANDWIDTH CONTROL	ACTION
Disable	Keep the Device's Settings	Off	
All	Keep the Device's Settings	Off	
Default	Keep the Device's Settings	Off	

3. If you want to create a profile, click Add Profile and configure the parameters.



← Add Profile

Change Note: Native Network, Tagged Networks, Untagged Networks, and Voice Network settings have been removed from Port Profile. You can now modify Tagged Networks by bulk selecting ports in Port Settings.
For more details on the switch port usage, please refer to the Guide.

Name

PoE ● Keep the Device's Settings ○ Enable ○ Disable

Agile (Easy Managed) Switch does not support 802.1X Control, 802.1p Priority, LLDP-MED, DHCP L2 Relay nor the Trust Mode function.

802.1X Control ● Auto ○ Force Authorized ○ Force Unauthorized

Port Isolation □ Enable

Flow Control □ Enable

EEE □ Enable

Multicast Fast Leave □ IGMP (IPv4) □ MLD (IPv6)

Loopback Control Spanning Tree

+ Spanning Tree Config

LLDP-MED ☑ Enable

Bandwidth Control ● Off ○ Rate Limit ○ Storming Control

DHCP L2 Relay □ Enable

Name	Enter a name to identify the port profile.
PoE	Select the PoE mode for the ports. Keep the Device's Settings: PoE keep enabled or disabled according to the switches' settings. By default, the switches enable PoE on all PoE ports. Enable: Enable PoE on PoE ports. Disable: Disable PoE on PoE ports.
802.1X Control	Select 802.1X Control mode for the ports. To configure the 802.1X authentication globally, enter the site view and go to Network Config > Authentication > 802.1X. Auto: The port is unauthorized until the client is authenticated by the authentication server successfully. Force Authorized: The port remains in the authorized state, sends and receives normal traffic without 802.1X authentication of the client. Force Unauthorized: The port remains in the unauthorized state, ignoring all attempts by the client to authenticate. The switch cannot provide authentication services to the client through the port.

Port Isolation	Click the checkbox to enable Port Isolation. An isolated port cannot communicate directly with any other isolated ports, while the isolated port can send and receive traffic to non-isolated ports.
Flow Control	With this option enabled, when a device gets overloaded it will send a PAUSE frame to notify the peer device to stop sending data for a specified period of time, thus avoiding the packet loss caused by congestion.
EEE	Click the checkbox to enable EEE (Energy Efficient Ethernet) to allow power reduction.
Multicast Fast Leave	After selecting the corresponding protocol, the multicast fast leave feature can be enabled for the port. This allows the switch to immediately stop forwarding multicast traffic to a port when detecting that the last multicast receiver has left the group, improving network bandwidth utilization.
Loopback Control	Loopback refers to the routing of data streams back to their source in the network. You can disable loopback control for the network or choose a method to prevent loopback happening in your network. Off: Disable loopback control on the port. Loopback Detection Port Based: Loopback Detection Port Based helps detect loops that occur on a specific port. When a loop is detected on a port, the port will be blocked. Loopback Detection VLAN Based: Loopback Detection VLAN Based helps detect loops that occur on a specific VLAN. When a loop is detected on a VLAN, the current port will be removed from the VLAN. Spanning Tree: Select STP (Spanning Tree Protocal) to prevent loops in the network. STP helps block specific ports of the switches to build a loop-free topology and detect topology changes and automatically generate a new loop-free topology.

Spanning Tree Config	If you set Loopback Control to Spanning Tree, configure the following parameters: Priority: Set the port priority. A smaller value indicates higher priority, reducing the likelihood of the port being blocked. Path Cost: Enter the value of the external path cost and internal path cost. External Path Cost determines the root port selection (lowest cost path to the root bridge). Internal Path Cost is used in MSTP to select the root port within an IST (Internal Spanning Tree). Edge Port: Select Enable to set the port as an edge port. Edge ports transition directly from blocking to forwarding during topology changes. Configure ports connected to end devices (e.g., PCs) as edge ports. P2P Link: Select the status of the P2P (Point-to-Point) link to which the ports are connected. During the regeneration of the spanning tree, if the port of P2P link is elected as the root port or the designated port, it can transit its state to forwarding directly. By default, it is Auto. • Auto: The switch automatically checks if the port is connected to a P2P link, then sets the status as Open or Closed. • Open(Force): A port is set as the one that is connected to a P2P link. You should check the link first. • Close(Force): A port is set as the one that is not connected to a P2P link. You should check the link first. STP Security: STP Security prevents the loops caused by wrong configurations or BPDU attacks. It contains the following options: • Loop Protect: Ports with Root/Alternate/Backup roles enter error-disabled blocking if no BPDUs are received. Automatically recovers when BPDUs resume. Enable this on Root/Alternate/Backup ports. • Root Protect: Ports enter error-disabled blocking upon receiving superior BPDUs. Automatically recovers when superior BPDUs stop. Enable on Designated ports; avoid enabling on Root/Alternate/Backup ports (may cause device unmanageability). • TC Guard: When enabled, ports do not flush MAC address tables upon receiving TC (Topology Change) notifications. • BPDU Protect: Manually configured edge ports enter error-disabled blocking upon receiving BPDUs. Requires manual recovery. Enable on Edge Ports. • BPDU Filter: When enabled, ports neither send nor process BPDUs, disabling loop prevention. Use only on network-edge ports with no loop risk. Enabling on Root/Alternate/Backup ports risks broadcast storms. • BPDU Forward: BPDU Forward will take effect only when the Spanning Tree is disabled for the entire device.
LLDP-MED	Click the checkbox to enable LLDP-MED (Link Layer Discovery Protocol-Media Endpoint Discovery) for device discovery and auto-configuration of VoIP devices.

Bandwidth Control	Select the type of Bandwidth Control functions to control the traffic rate and traffic threshold on each port to ensure network performance. Off: Disable Bandwidth Control for the port. Rate Limit: Select Rate limit to limit the ingress/egress traffic rate on each port. With this function, the network bandwidth can be reasonably distributed and utilized. Storming Control: With this feature enabled, Omada switches can control the traffic rate or the percentage of total bandwidth used on each port, and set traffic thresholds to ensure network performance (the Kbps value entered must be a multiple of 64).
Ingress Rate Limit	When Rate Limit selected, click the checkbox and specify the upper rate limit for receiving packets on the port.
Egress Rate Limitv	When Rate Limit selected, click the checkbox and specify the upper rate limit for sending packets on the port.
Rate Mode	Specifies the rate threshold measurement for storm control. Kbps: Sets an absolute rate threshold in kilobits per second. Ratio: Sets a relative threshold as a percentage of total bandwidth.
Broadcast Threshold	When Storming Control selected, click the checkbox and specify the upper rate limit for receiving broadcast frames. The broadcast traffic exceeding the limit will be processed according to the Action configurations.
Multicast Threshold	When Storming Control selected, click the checkbox and specify the upper rate limit for receiving multicast frames. The multicast traffic exceeding the limit will be processed according to the Action configurations.
Unknown Unicast Threshold	When Storming Control selected, click the checkbox and specify the upper rate limit for receiving unknown unicast frames. The traffic exceeding the limit will be processed according to the Action configurations.
Action	When Storming Control selected, select the action that the switch will take when the traffic exceeds its corresponding limit. Drop: The port will drop the subsequent frames when the traffic exceeds the limit. Shutdown: The port will be shutdown when the traffic exceeds the limit.
Recover Time	With Shutdown selected as the Action, specify the recover time, and the port will be opened after the specified time.
DHCP L2 Relay	Click the checkbox to enable DHCP L2 Relay for the network.
Format	Select the format of option 82 sub-option value field. Normal: The format of sub-option value field is TLV (type-length-value). Private: The format of sub-option value field is just value.

802.1p Priority	Specify the port-to-802.1p priority mapping for the desired port. The ingress packets are first mapped to 802.1p priority, then to TC queues according to the 802.1p queue mappings.
Trust Mode	Select the trusted priority mode for the desired port. The switch will process the ingress packets according to the trusted priority mode. Untrusted: In this mode, the packets will be processed according to the port priority configuration. Trust 802.1p: In this mode, the packets will be processed according to the 802.1p priority configuration. Trust DSCP: In this mode, the packets will be processed according to the DSCP priority configuration.

4. Click Save. The new port profile will be added to the profile list.

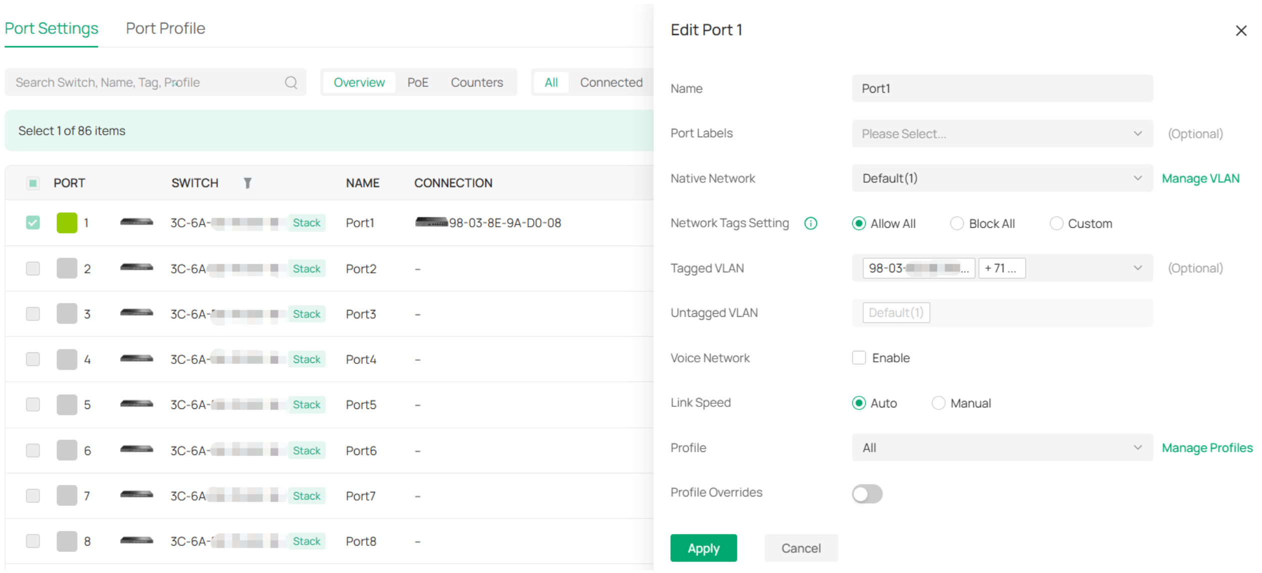
9.2 Port Settings

The Port Settings page allows you to monitor and manage the ports of all adopted switches in the Site.

To configure the Port Settings of a switch, follow the steps below:

1. Launch the controller and access a site.
2. Go to Device Config > Switch > Switch Ports > Port Settings.
3. Switch between Overview, PoE, and Counters to view the general, PoE-related, and traffic-related information of the ports.
4. To configure a single port, click the edit icon of the port entry. To configure ports in batches, click the checkboxes and then click Edit Selected.

Note: When configuring ports in batches, only common configuration items can be configured and all settings are Keep Existing by default.



Select 1 of 86 items

■	PORT	SWITCH	NAME	CONNECTION
☑	🟩 1	3C-6A-[redacted] Stack	Port1	98-03-8E-9A-D0-08
□	2	3C-6A[redacted] Stack	Port2	-
□	3	3C-6A-[redacted] Stack	Port3	-
□	4	3C-6A-[redacted] Stack	Port4	-
□	5	3C-6A-[redacted] Stack	Port5	-
□	6	3C-6A-[redacted] Stack	Port6	-
□	7	3C-6A[redacted] Stack	Port7	-
□	8	3C-6A-[redacted] Stack	Port8	-

Edit Port 1

Name: Port1

Port Labels: Please Select... (Optional)

Native Network: Default(1) Manage VLAN

Network Tags Setting: ● Allow All ○ Block All ○ Custom

Tagged VLAN: 98-03-[redacted]... + 71 ... (Optional)

Untagged VLAN: Default(1)

Voice Network: □ Enable

Link Speed: ● Auto ○ Manual

Profile: All Manage Profiles

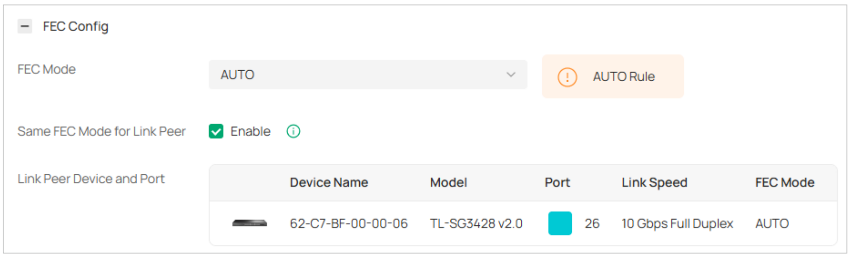
Profile Overrides

Name	Specify the name of the port.
Port Labels	Set a user-defined label for port identify.
Native Network	Select the native network from all networks. The native network determines the Port VLAN Identifier (PVID) for switch ports. When a port receives an untagged frame, the switch inserts a VLAN tag to the frame based on the PVID, and forwards the frame in the native network. Each physical switch port can have multiple networks attached, but only one of them can be native.
Network Tags Setting	Select a network communication mode for the port. Allow All: The port will be automatically tag the configured VLANS.Any tagged traffic with a non existent VLAN ID will be dropped. Block All: The port will be automatically block all VLAN traffic except for the Native Network(PVID).Any tagged traffic with a other VLAN ID will be dropped. Custom: VLAN Management can be customized to either tag specific VLANS only. If you select Custom, set the following parameters: Tagged VLAN: Select the Tagged Networks. Frames sent out of a Tagged Network are kept with VLAN tags. Usually networks that connect the switch to network devices like routers and other switches, or VoIP devices like IP phones should be configured as Tagged Networks. Untagged VLAN: Select the Untagged Networks. Frames that sent out of an Untagged Network are stripped of VLAN tags. Usually networks that connect the switch to endpoint devices like computers should be configured as Untagged Networks. Note that the native network is untagged.

Voice Network	Enable this option and select a network that connects VoIP devices like IP phones as the Voice Network. The Voice Network feature configures IP Phones via the LLDP-MED protocol to ensure their transmitted packets carry a specific VLAN tag, directing voice traffic through the designated VLAN. Enabling this feature will automatically activate LLDP-MED on the port.
Link Speed	Select the speed mode for the port. Auto: The port negotiates the speed and duplex automatically. Manual: Specify the speed and duplex from the drop-down list manually.
Profile	Set the switch port configuration file to quickly batch configure switch port parameters.
Profile Overrides	Click the checkbox to override the applied profile if needed. The parameters to be configured vary in Operation modes,

For switch ports supporting FEC (Forward Error Correction), FEC parameters will be displayed.

FEC is a technology used to enhance the reliability of data transmission by adding redundant information to the data being sent. This allows the receiver to detect and correct errors that may have occurred during transmission. FEC is commonly used in environments requiring high reliability, particularly in long-distance fiber optic transmissions or networks with high bit error rates. It helps ensure a stable network and high data transmission quality.



FEC Config

FEC Mode: AUTO

Same FEC Mode for Link Peer: ☑ Enable

Link Peer Device and Port

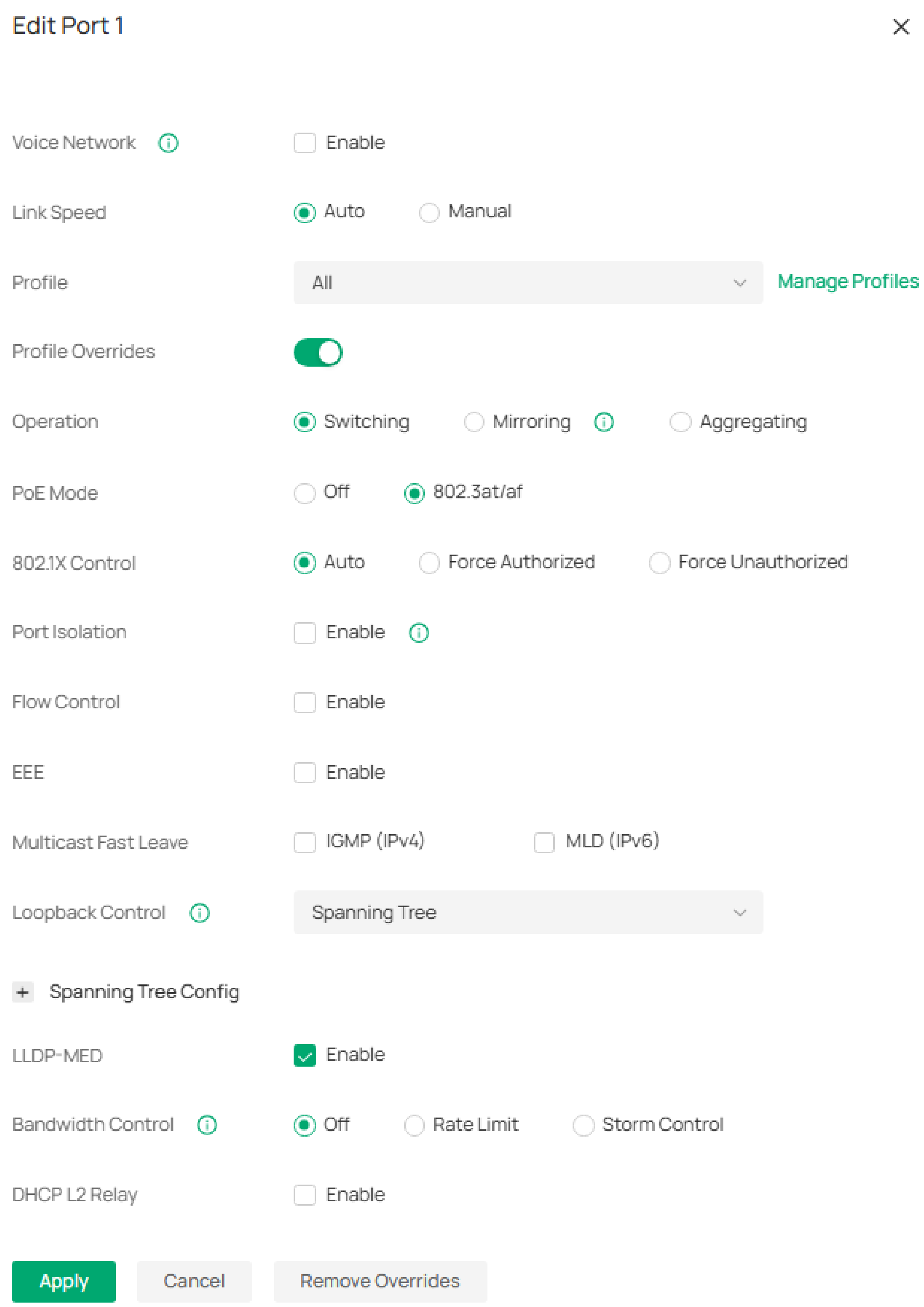
Device Name	Model	Port	Link Speed	FEC Mode
62-C7-BF-00-00-06	TL-SG3428 v2.0	26	10 Gbps Full Duplex	AUTO

FEC Mode	Select the FEC Mode. By default, the port supporting the FEC function would have FEC Mode as AUTO. **Note:** 1. The function requires both sides using the same FEC mode, otherwise the Link cannot be established. 2. Each Link Speed has a different list of configurable FEC modes, please try changing the link speed manually if can't find desired FEC mode. 3. Ports in the LAG group do not support configuring the FEC mode.
Same FEC Mode for Link Peer	If this option is enabled and the peer is also a managed Omada Switch with firmware supporting FEC report function, it would synchronize local Link speed & FEC configuration to the peer port, show the peer's FEC configuration, and the available options are limited to those supported by both ends for your convenience to adjust accordingly.

5. If you enable Profile Overrides, select an operation mode and configure the parameters.

- Override the Applied Profile

If you select Switching for Operation, configure the following parameters and click Apply to override the applied profile. To discard the modifications, click Remove Overrides and all profile configurations will become the same as the applied profile.



Edit Port 1 ×

Voice Network ⓘ □ Enable

Link Speed ● Auto ○ Manual

Profile: All ⌵ Manage Profiles

Profile Overrides: on

Operation ● Switching ○ Mirroring ⓘ ○ Aggregating

PoE Mode ○ Off ● 802.3at/af

802.1X Control ● Auto ○ Force Authorized ○ Force Unauthorized

Port Isolation □ Enable ⓘ

Flow Control □ Enable

EEE □ Enable

Multicast Fast Leave □ IGMP (IPv4) □ MLD (IPv6)

Loopback Control ⓘ Spanning Tree ⌵

+ Spanning Tree Config

LLDP-MED ☑ Enable

Bandwidth Control ⓘ ● Off ○ Rate Limit ○ Storm Control

DHCP L2 Relay □ Enable

Apply | Cancel | Remove Overrides

PoE Mode	(Only for PoE ports) Select the PoE (Power over Ethernet) mode for the port. Off: Disable PoE function on the PoE port. 802.3bt/at/af: Enable PoE function on the PoE port.

802.1X Control	Select 802.1X Control mode for the ports. To configure the 802.1X authentication globally, go to Network Config > Authentication > 802.1X. Auto: The port is unauthorized until the client is authenticated by the authentication server successfully. Force Authorized: The port remains in the authorized state, sends and receives normal traffic without 802.1X authentication of the client. Force Unauthorized: The port remains in the unauthorized state, and the client connected to the port cannot authenticate with any means. The switch cannot provide authentication services to the client through the port.
Port Isolation	Click the checkbox to enable Port Isolation. An isolated port cannot communicate directly with any other isolated ports, while the isolated port can send and receive traffic to non-isolated ports.
Flow Control	With this option enabled, when a device gets overloaded it will send a PAUSE frame to notify the peer device to stop sending data for a specified period of time, thus avoiding the packet loss caused by congestion.
EEE	Click the checkbox to enable EEE (Energy Efficient Ethernet) to allow power reduction.
Multicast Fast Leave	Select IGMP (IPv4) and/or MLD (IPv6) to allow the port to immediately stop forwarding multicast traffic to a client when it receives an IGMP and/or MLD Leave message, instead of waiting for the next group-specific query. This process improves network efficiency by saving bandwidth and resources, especially in networks with many hosts or frequent group departures.
Loopback Control	Loopback refers to the routing of data streams back to their source in the network. You can disable loopback control for the network or choose a method to prevent loopback happening in your network. Off: Disable loopback control on the port. Loopback Detection Port Based: Loopback Detection Port Based helps detect loops that occur on a specific port. When a loop is detected on a port, the port will be blocked. Loopback Detection VLAN Based: Loopback Detection VLAN Based helps detect loops that occur on a specific VLAN. When a loop is detected on a VLAN, the current port will be removed from the VLAN. Spanning Tree: Select STP (Spanning Tree Protocal) to prevent loops in the network. STP helps block specific ports of the switches to build a loop-free topology and detect topology changes and automatically generate a new loop-free topology. To make sure Spanning Tree takes effect on the port, go to the Config tab and enable Spanning Tree on the switch.

Spanning Tree Config	If you set Loopback Control to Spanning Tree, configure the following parameters: Priority: Set the port priority. A smaller value indicates higher priority, reducing the likelihood of the port being blocked. Path Cost: Enter the value of the external path cost and internal path cost. External Path Cost determines the root port selection (lowest cost path to the root bridge). Internal Path Cost is used in MSTP to select the root port within an IST (Internal Spanning Tree). Edge Port: Select Enable to set the port as an edge port. Edge ports transition directly from blocking to forwarding during topology changes. Configure ports connected to end devices (e.g., PCs) as edge ports. P2P Link: Select the status of the P2P (Point-to-Point) link to which the ports are connected. During the regeneration of the spanning tree, if the port of P2P link is elected as the root port or the designated port, it can transit its state to forwarding directly. By default, it is Auto. • Auto: The switch automatically checks if the port is connected to a P2P link, then sets the status as Open or Closed. • Open(Force): A port is set as the one that is connected to a P2P link. You should check the link first. • Close(Force): A port is set as the one that is not connected to a P2P link. You should check the link first. STP Security: STP Security prevents the loops caused by wrong configurations or BPDU attacks. It contains the following options: • Loop Protect: Ports with Root/Alternate/Backup roles enter error-disabled blocking if no BPDUs are received. Automatically recovers when BPDUs resume. Enable this on Root/Alternate/Backup ports. • Root Protect: Ports enter error-disabled blocking upon receiving superior BPDUs. Automatically recovers when superior BPDUs stop. Enable on Designated ports; avoid enabling on Root/Alternate/Backup ports (may cause device unmanageability). • TC Guard: When enabled, ports do not flush MAC address tables upon receiving TC (Topology Change) notifications. • BPDU Protect: Manually configured edge ports enter error-disabled blocking upon receiving BPDUs. Requires manual recovery. Enable on Edge Ports. • BPDU Filter: When enabled, ports neither send nor process BPDUs, disabling loop prevention. Use only on network-edge ports with no loop risk. Enabling on Root/Alternate/Backup ports risks broadcast storms. • BPDU Forward: BPDU Forward will take effect only when the Spanning Tree is disabled for the entire device.
LLDP-MED	Click the checkbox to enable LLDP-MED (Link Layer Discovery Protocol-Media Endpoint Discovery) for device discovery and auto-configuration of VoIP (Voice over Internet Protocol) devices.

Bandwidth Control	Select the type of Bandwidth Control functions to control the traffic rate and specify traffic threshold on each port to make good use of network bandwidth. Off: Disable Bandwidth Control for the port. Rate Limit: Select Rate limit to limit the ingress/egress traffic rate on each port. With this function, the network bandwidth can be reasonably distributed and utilized. Storming Control: With this feature enabled, Omada switches can control the traffic rate or the percentage of total bandwidth used on each port, and set traffic thresholds to ensure network performance (the Kbps value entered must be a multiple of 64).
Ingress Rate Limit	When Rate Limit selected, click the checkbox and specify the upper rate limit for receiving packets on the port.
Egress Rate Limit	When Rate Limit selected, click the checkbox and specify the upper rate limit for sending packets on the port.
Rate Mode	Specifies the rate threshold measurement for storm control. Kbps: Sets an absolute rate threshold in kilobits per second. Ratio: Sets a relative threshold as a percentage of total bandwidth.
Broadcast Threshold	When Storming Control selected, click the checkbox and specify the upper rate limit for receiving broadcast frames. The broadcast traffic exceeding the limit will be processed according to the Action configurations.
Multicast Threshold	When Storming Control selected, click the checkbox and specify the upper rate limit for receiving multicast frames. The multicast traffic exceeding the limit will be processed according to the Action configurations.
Unknown Unicast Threshold	When Storming Control selected, click the checkbox and specify the upper rate limit for receiving unknown unicast frames. The traffic exceeding the limit will be processed according to the Action configurations.
Action	When Storming Control selected, select the action that the switch will take when the traffic exceeds its corresponding limit. Drop: The port will drop the subsequent frames when the traffic exceeds the limit. Shutdown: The port will be shutdown when the traffic exceeds the limit.
Recover Time	With Shutdown selected as the Action, specify the recover time, and the port will be opened after the specified time.

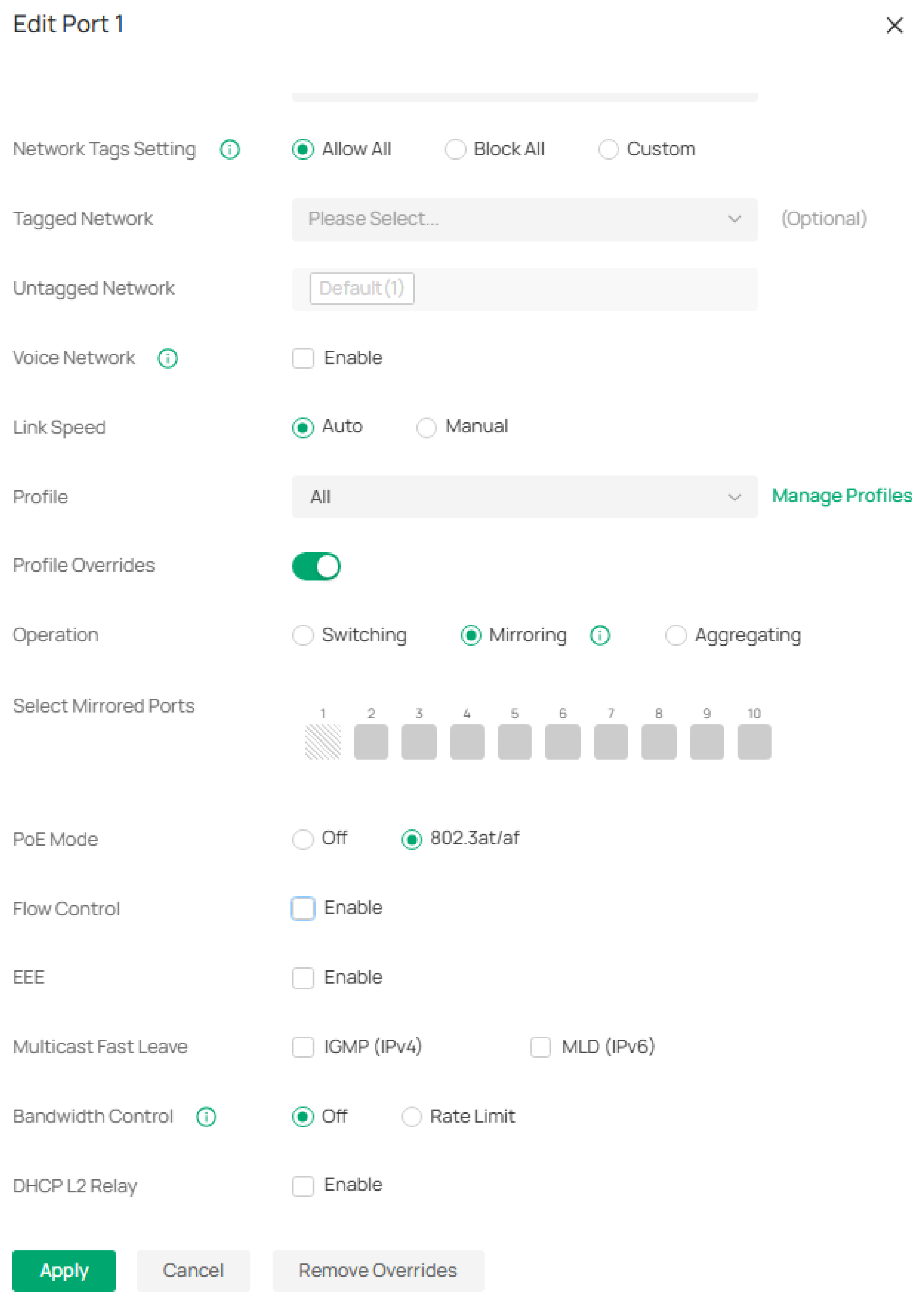
DHCP L2 Relay	Click the checkbox to enable DHCP L2 Relay for the network, which takes the Layer 2 DHCP communications (Discover, Request, etc.) and forwards them to a specified IP address (your DHCP server). Format: Select the format of option 82 sub-option value field. • Normal: The format of sub-option value field is TLV (type-length-value). • Private: The format of sub-option value field is just value. Circuit ID: Omada switches preset a default Circuit ID in TLV (Type, Length, and Value) format. You can also customize it if needed. Remote ID: Omada switches preset a default Remote ID in TLV (Type, Length, and Value) format. You can also customize them if needed.
802.1p Priority	Specify the port-to-802.1p priority mapping for the desired port. The ingress packets are first mapped to 802.1p priority, then to TC queues according to the 802.1p queue mappings.
Trust Mode	Select the trusted priority mode for the desired port. The switch will process the ingress packets according to the trusted priority mode. Untrusted: In this mode, the packets will be processed according to the port priority configuration. Trust 802.1p: In this mode, the packets will be processed according to the 802.1p priority configuration. Trust DSCP: In this mode, the packets will be processed according to the DSCP priority configuration.

- Configure a Mirroring Port

If you select Mirroring as Operation, the edited port can be configured as a mirroring port. Specify other ports as the mirrored port, and the switch sends a copy of traffics passing through the mirrored port to the mirroring port. You can use mirroring to analyze network traffic and troubleshoot network problems.

To configure Mirroring, select the mirrored port or LAG, specify the following parameters, and click Apply. To discard the modifications, click Remove Overrides and all profile configurations become the same as the applied profile.

Note: The mirroring ports and the member ports of LAG cannot be selected as mirrored ports.



Edit Port 1

Network Tags Setting: ● Allow All ○ Block All ○ Custom

Tagged Network: Please Select... (Optional)

Untagged Network: Default (1)

Voice Network: ☐ Enable

Link Speed: ● Auto ○ Manual

Profile: All

Profile Overrides: On

Operation: ○ Switching ● Mirroring ○ Aggregating

Select Mirrored Ports: 1 2 3 4 5 6 7 8 9 10

PoE Mode: ○ Off ● 802.3at/af

Flow Control: ☐ Enable

EEE: ☐ Enable

Multicast Fast Leave: ☐ IGMP (IPv4) ☐ MLD (IPv6)

Bandwidth Control: ● Off ○ Rate Limit

DHCP L2 Relay: ☐ Enable

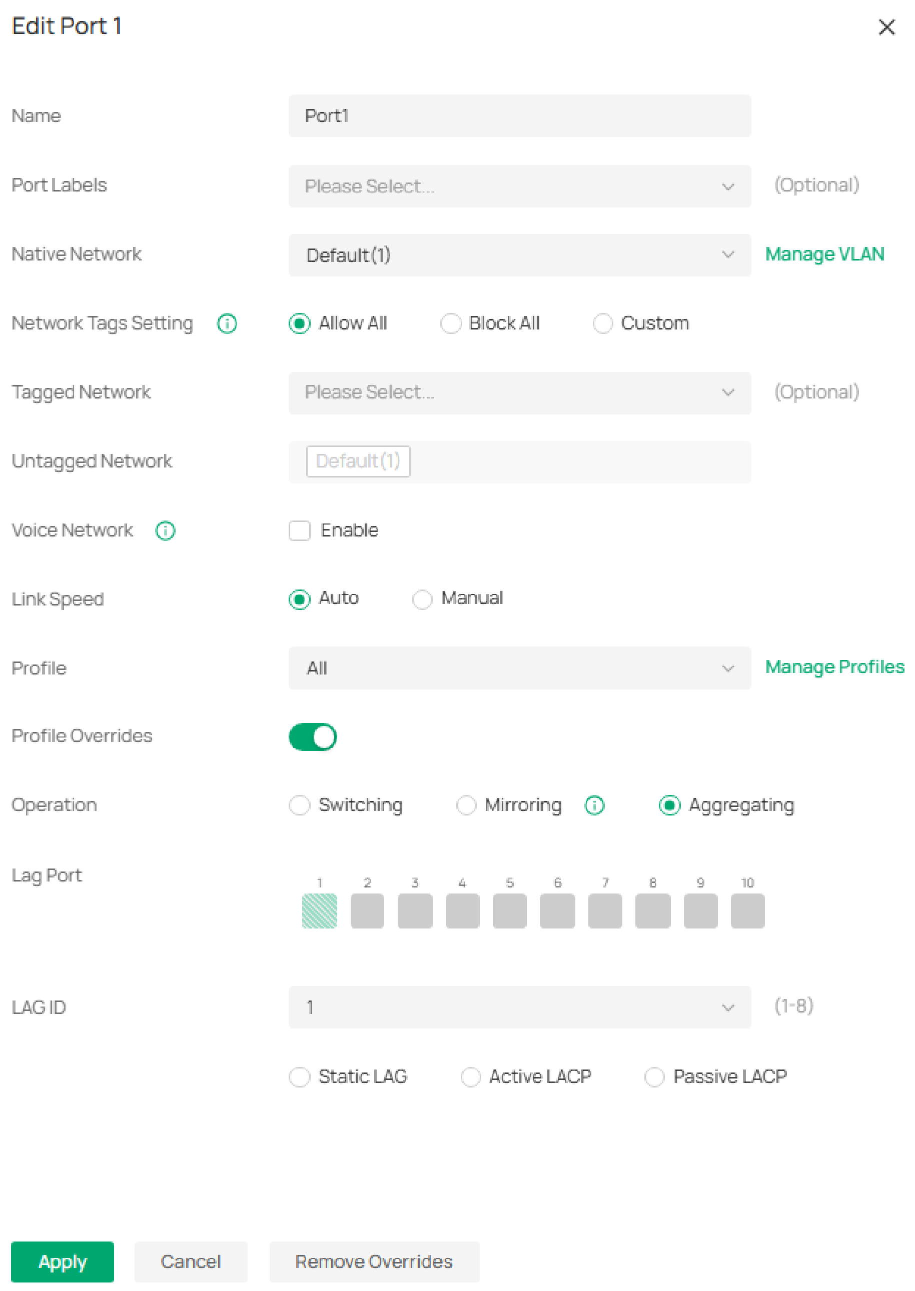
PoE Mode	(Only for PoE ports) Select the PoE mode for the port. Off: Disable PoE on the PoE port. 802.3bt/at/af: Enable PoE on the PoE port.

Flow Control	With this option enabled, when a device gets overloaded it will send a PAUSE frame to notify the peer device to stop sending data for a specified period of time, thus avoiding the packet loss caused by congestion.
EEE	Click the checkbox to enable EEE (Energy Efficient Ethernet) to allow power reduction.
Multicast Fast Leave	Select IGMP (IPv4) and/or MLD (IPv6) to allow the port to immediately stop forwarding multicast traffic to a client when it receives an IGMP and/or MLD Leave message, instead of waiting for the next group-specific query. This process improves network efficiency by saving bandwidth and resources, especially in networks with many hosts or frequent group departures.
Bandwidth Control	Bandwidth control optimizes network performance by limiting the bandwidth of specific sources. Off: Disable bandwidth control on the port. Rate Limit: Enable bandwidth control on the port, and you need to specify the ingress and/or egress rate limit.
Ingress Rate Limit	With Rate Limit selected, click the checkbox and specify the upper rate limit for receiving packets on the port. With this function, the network bandwidth can be reasonably distributed and utilized.
Egress Rate Limit	With Rate Limit selected, click the checkbox and specify the upper rate limit for sending packets on the port. With this function, the network bandwidth can be reasonably distributed and utilized.
DHCP L2 Relay	Click the checkbox to enable DHCP L2 Relay for the network, which takes the Layer 2 DHCP communications (Discover, Request, etc.) and forwards them to a specified IP address (your DHCP server). Format: Select the format of option 82 sub-option value field. • Normal: The format of sub-option value field is TLV (type-length-value). • Private: The format of sub-option value field is just value. Circuit ID: Omada switches preset a default Circuit ID in TLV (Type, Length, and Value) format. You can also customize it if needed. Remote ID: Omada switches preset a default Remote ID in TLV (Type, Length, and Value) format. You can also customize them if needed.
802.1p Priority	Specify the port-to-802.1p priority mapping for the desired port. The ingress packets are first mapped to 802.1p priority, then to TC queues according to the 802.1p queue mappings.

Trust Mode	Select the trusted priority mode for the desired port. The switch will process the ingress packets according to the trusted priority mode. Untrusted: In this mode, the packets will be processed according to the port priority configuration. Trust 802.1p: In this mode, the packets will be processed according to the 802.1p priority configuration. Trust DSCP: In this mode, the packets will be processed according to the DSCP priority configuration.

- Configure a LAG

If you select Aggregating as Operation, you can aggregate multiple physical ports into a logical interface, which can increase link bandwidth and enhance the connection reliability.



Edit Port 1

Name: Port1

Port Labels: Please Select... (Optional)

Native Network: Default(1) Manage VLAN

Network Tags Setting: ● Allow All ○ Block All ○ Custom

Tagged Network: Please Select... (Optional)

Untagged Network: Default(1)

Voice Network: □ Enable

Link Speed: ● Auto ○ Manual

Profile: All Manage Profiles

Profile Overrides: On

Operation: ○ Switching ○ Mirroring ● Aggregating

Lag Port: 1 2 3 4 5 6 7 8 9 10

LAG ID: 1 (1-8)

○ Static LAG ○ Active LACP ○ Passive LACP

Configuration Guidelines:

- Ensure that both ends of the aggregation link work in the same LAG mode. For example, if the local end works in LACP mode, the peer end should also be set as LACP mode.
- Ensure that devices on both ends of the aggregation link use the same number of physical ports with the same speed, duplex, jumbo and flow control mode.
- A port cannot be added to more than one LAG at the same time.
- LACP does not support half-duplex links.
- One static LAG supports up to eight member ports. All the member ports share the bandwidth evenly. If an active link fails, the other active links share the bandwidth evenly.
- One LACP LAG supports multiple member ports, but at most eight of them can work simultaneously, and the other member ports are backups. Using LACP protocol, the switches negotiate parameters and determine the working ports. When a working port fails, the backup port with the highest priority will replace the faulty port and start to forward data.
- The member port of an LAG follows the configuration of the LAG but not its own. Once removed, the LAG member will be configured as the default All profile and Switching operation.
- The port enabled with Port Security, Port Mirror, MAC Address Filtering or 802.1X cannot be added to an LAG, and the member port of an LAG cannot be enabled with these functions.

To configure a new LAG, select other ports to be added to the LAG, specify the LAG ID, and choose a LAG type. Click Apply. To discard the modifications, click Remove Overrides and all profile configurations become the same as the applied profile. For other parameters, configure them under the LAG tab.

LAG ID	Specify the LAG ID of the LAG. Note that the LAG ID should be unique. The valid value of the LAG ID is determined by the maximum number of LAGs supported by your switch. For example, if your switch supports up to 14 LAGs, the valid value ranges from 1 to 14.
Static LAG	In Static LAG mode, the member ports are added to the LAG manually.
Active LACP / Passive LACP	LACP extends the flexibility of the LAG configurations. In LACP, the switch uses LACPDU (Link Aggregation Control Protocol Data Unit) to negotiate the parameters with the peer end. In this way, the two ends select active ports and form the aggregation link. Active LACP: In this mode, the port will take the initiative to send LACPDU. Passive LACP: In this mode, the port will not send LACPDU before receiving the LACPDU from the peer end.

10 Configure VRRP

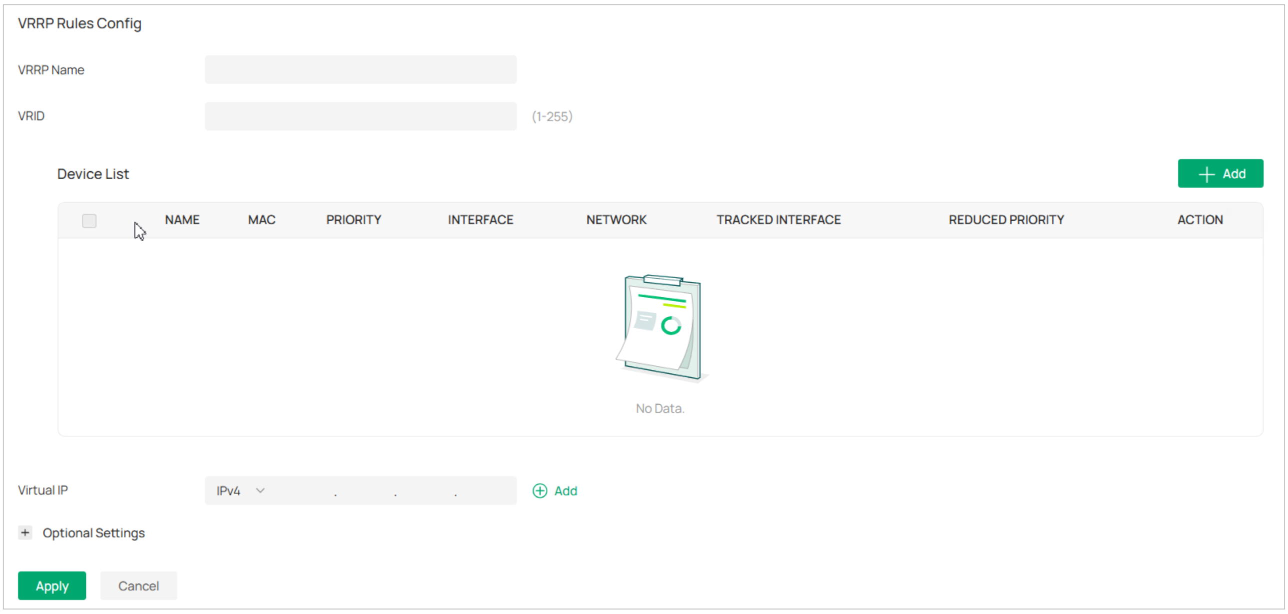
VRRP or Virtual Routing Redundancy Protocol is a function on the switch that dynamically assigns responsibility for a virtual router to one of the VRRP routers on a LAN. The VRRP router that controls the IP address associated with a virtual router is called the Master and will forward packets sent to this IP address. This will allow any Virtual Router IP address on the LAN to be used as the default first hop router by end hosts.

To configure the VRRP of a switch, follow the steps below:

1. Launch the controller and access a site.

2. Go to Device Config > Switch > VRRP.

3. Click Create VRRP Rules. Configure the parameters.



VRRP Rules Config

VRRP Name:

VRID: (1-255)

Device List

□	NAME	MAC	PRIORITY	INTERFACE	NETWORK	TRACKED INTERFACE	REDUCED PRIORITY	ACTION

No Data.

Virtual IP: IPv4

VRRP Name	Enter a name to identify the rule.
VRID	Enter the VRID to create a new VRRP. The VRID ranges from 1 to 255.
Device List	Click Add to select a switch and configure device VRRP. The switch you add will display in the Device List. Device Name: Name of the device. MAC: MAC address of the device. Priority: Priority associated with the VRRP. It ranges from 1 to 254. Interface: Interface ID associated with the VRRP. Network: Intersection of device network (IP/mask). Tracked Interface: Interface to be tracked. Reduced Priority: Priority to reduce if the associated interface is down.
Virtual IP	Add virtual IP addresses associated with the VRRP.

4. Expand and configure Optional Settings if needed.

Advertise Timer	Enter the advertise timer associated with the VRRP. It ranges from 1 to 255.
Preempt Mode	Select Enable or disable the preempt Mode from the pull-down list. If you select Enable, a backup router will preempt the master router if it has a priority greater than the master virtual router's priority. The Preempt Mode is enabled by default.
Delay Time	Enter the delay time associated with the VRRP. It ranges from 0 to 255.

Authentication	Select the type of Authentication for the Virtual Router from the pull-down list. The default is None. None: No authentication will be performed. Simple: Authentication will be performed using a text password. If you select this mode, enter the Key. MD5: Authentication of MD5 will be performed using a text password. If you select this mode, enter the Key.

5. Apply the settings.