

# MX-NOS V5

## User Manual

**Version 1.0**

November 2024



# Table of Contents

<b>Overview .....</b>	<b>12</b>
<b>Introduction .....</b>	<b>13</b>
<b>About MX-NOS .....</b>	<b>14</b>
<b>What's in This Document .....</b>	<b>15</b>
<b>Supported Series and Firmware Versions .....</b>	<b>16</b>
<b>Product Series Feature Comparison Table .....</b>	<b>17</b>
Options Menu.....	17
System .....	17
Port .....	18
Layer 2 Switching .....	19
Network Interface.....	20
Redundancy.....	20
Network Service .....	20
Routing .....	21
Security .....	21
Diagnostics.....	22
Industrial Application .....	23
<b>Icons Used in the Web Interface .....</b>	<b>25</b>
<b>Quick Start .....</b>	<b>28</b>
<b>Using a Web Browser to Configure the Industrial Ethernet Switch .....</b>	<b>29</b>
<b>Using a RS-232 Console to Configure the Device .....</b>	<b>31</b>
<b>Using Telnet to Configure the Device.....</b>	<b>35</b>
<b>UI Reference .....</b>	<b>37</b>
<b>UI Reference Overview.....</b>	<b>38</b>
<b>The MX-NOS User Interface .....</b>	<b>39</b>

<b>Options Menu .....</b>	<b>41</b>
Options Menu - User Privileges .....	41
Change Language .....	42
Change Mode .....	42
Disable/Enable Auto Save .....	42
Locator .....	43
Reboot .....	43
Reset to Default Settings .....	44
Log Out .....	44
<b>Device Summary .....</b>	<b>45</b>
System Information .....	45
Panel Status .....	46
<i>Panel View .....</i>	<i>47</i>
Event Summary (Last 3 days) .....	48
CPU Usage History (%) .....	48
<b>System .....</b>	<b>49</b>
System - User Privileges .....	49
System Management .....	50
Account Management .....	71
Management Interface .....	79
<i>Configuring Simple Network Management Protocol .....</i>	<i>83</i>
Time .....	92
<i>About System Time .....</i>	<i>92</i>
<i>About NTP Servers .....</i>	<i>98</i>
<i>About Time Synchronization .....</i>	<i>99</i>
<i>Configuring NTP Server .....</i>	<i>111</i>
<b>Port .....</b>	<b>113</b>

PoE - User Privileges .....	113
Port Interface.....	113
<i>About Port Settings</i> .....	114
<i>About Linkup Delay</i> .....	118
About Link Aggregation .....	120
<i>Link Aggregation Settings</i> .....	121
PoE.....	127
<i>PoE Settings</i> .....	127
<b>Layer 2 Switching .....</b>	<b>142</b>
Layer 2 Switching - User Privileges .....	142
About VLAN .....	143
<i>Assigning VLANs to Ports</i> .....	143
<i>Creating VLANs</i> .....	144
<i>VLANs in Depth</i> .....	145
<i>VLAN Settings</i> .....	147
GARP .....	153
<i>GARP Settings</i> .....	153
MAC.....	155
<i>About Static Unicast</i> .....	155
<i>About MAC Address Tables</i> .....	157
About QoS .....	159
<i>QoS In Depth</i> .....	159
<i>QoS</i> .....	160
Multicast .....	193
<i>Multicast In Depth</i> .....	193
<i>Multicast</i> .....	195
<b>Network Interface .....</b>	<b>211</b>



Network Interface - User Privileges.....	211
Network Interface - Settings.....	211
<i>Loopback Interface Table</i> .....	212
<i>Create Loopback Interface Settings</i> .....	212
<i>VLAN Interface Table</i> .....	214
<i>Create VLAN Interface Settings</i> .....	214
Network Interface - Status .....	215
<i>Loopback Interface List</i> .....	216
<i>VLAN Interface List</i> .....	216
<b>Redundancy .....</b>	<b>218</b>
Redundancy - User Privileges .....	218
Layer 2 Redundancy .....	219
<i>About Spanning Tree</i> .....	219
<i>About Turbo Ring v2</i> .....	245
<i>About Turbo Chain</i> .....	261
<i>About MRP (Media Redundancy Protocol)</i> .....	267
<i>About Multiple Dual Homing</i> .....	274
<i>About Multiple Network Coupling</i> .....	283
Layer 3 Redundancy .....	295
<i>Layer 3 Redundancy</i> .....	295
<i>About VRRP</i> .....	295
Tracking .....	306
<i>Tracking In Depth</i> .....	306
<i>Controlling a Virtual Router With an Interface Tracking Entry</i> .....	308
<i>Controlling a Port Through Ping and Logical Tracking Entries</i> .....	310
<i>Controlling a Static Route Through an Interface Tracking Entry</i> .....	312
<i>Tracking</i> .....	314

<b>Network Service .....</b>	<b>331</b>
Network Service - User Privileges .....	331
Configuring DHCP Server Functions .....	331
<i>Introduction to DHCP.....</i>	<i>331</i>
<i>Overview of DHCP Server Configuration.....</i>	<i>332</i>
<i>Configuring Dynamic IP Address Assignment (DHCP Server Pool).....</i>	<i>332</i>
<i>Reserving IP Addresses for Specific Devices (MAC-based IP Assignment) ..</i>	<i>334</i>
<i>Configuring Port-based IP Assignment.....</i>	<i>336</i>
<i>DHCP Server .....</i>	<i>339</i>
Configuring DHCP Relay Agent .....	346
<i>About DHCP Relay Agents .....</i>	<i>346</i>
<i>Configuring DHCP Relay Agent (RKS-G4000 Series) .....</i>	<i>347</i>
<i>Configuring Option 82.....</i>	<i>348</i>
<i>DHCP Relay Agent.....</i>	<i>349</i>
About DNS.....	354
<i>DNS Settings.....</i>	<i>354</i>
<b>Routing.....</b>	<b>356</b>
Routing - User Privileges .....	356
About Unicast Routes .....	357
<i>Unicast Route .....</i>	<i>358</i>
Multicast Route .....	385
<i>PIM-DM .....</i>	<i>385</i>
<i>About PIM-SM .....</i>	<i>389</i>
<i>Multicast Local Route.....</i>	<i>407</i>
<b>Security .....</b>	<b>419</b>
Security - User Privileges.....	419
Device Security .....	420

<i>About Login Policy</i> .....	420
<i>About Trusted Access</i> .....	422
<i>About SSH &amp; SSL</i> .....	425
Network Security.....	428
<i>About IEEE 802.1X</i> .....	429
<i>About MAC Authentication Bypass</i> .....	442
<i>About Traffic Storm Control</i> .....	460
<i>About Access Control Lists</i> .....	463
<i>About Network Loop Protection</i> .....	475
<i>About Binding Databases</i> .....	478
<i>About DHCP Snooping</i> .....	484
<i>About IP Source Guard</i> .....	487
<i>About Dynamic ARP Inspection</i> .....	490
<i>About MAC Security</i> .....	494
Authentication.....	501
<i>About Login Authentication</i> .....	501
RADIUS .....	504
TACACS+.....	506
<b>Diagnostics</b> .....	<b>509</b>
Diagnostics - User Privileges .....	509
System Status .....	510
<i>About Resource Utilization</i> .....	510
<i>About Fiber Check</i> .....	513
Network Status .....	519
<i>About Network Statistics</i> .....	519
<i>About LLDP</i> .....	523
<i>About ARP Tables</i> .....	533

Tools.....	534
<i>About Port Mirroring</i> .....	534
<i>Ping</i> .....	544
Event Logs and Notifications .....	545
<i>About Event Logs</i> .....	546
<i>About Event Notifications</i> .....	552
<i>Syslog</i> .....	557
<i>About SNMP Trap/Inform</i> .....	561
<i>About Email Settings</i> .....	567
<b>Industrial Application .....</b>	<b>570</b>
Industrial Application - User Privileges .....	570
IEC 61850 .....	570
<i>MMS</i> .....	571
<i>About GOOSE Check</i> .....	579
About Modbus TCP.....	584
<i>Modbus In Depth</i> .....	584
<i>Modbus TCP</i> .....	585
About EtherNet/IP .....	586
<i>EtherNet/IP</i> .....	586
About PROFINET.....	586
<i>PROFINET In Depth</i> .....	587
<i>PROFINET</i> .....	596
<b>Appendix .....</b>	<b>598</b>
<b>CIP EtherNet/IP Objects .....</b>	<b>599</b>
Identity Object.....	599
<i>Class Attribute List</i> .....	600
<i>Instance Attribute List</i> .....	600
<i>Common Service List</i> .....	601

Message Router Object.....	602
<i>Class Attribute List</i> .....	602
<i>Instance Attribute List</i> .....	602
<i>Common Service List</i> .....	603
Assembly Object .....	603
<i>Class Attribute List</i> .....	603
<i>Instance Attribute List</i> .....	603
<i>Common Service List</i> .....	604
<i>I/O Assembly Data Attribute Formats</i> .....	604
Mapping I/O Assembly Data Attribute Components .....	605
Connection Manager Object .....	605
<i>Class Attribute List</i> .....	605
<i>Instance Attribute List</i> .....	606
<i>Common Service List</i> .....	606
QoS Object.....	606
<i>Class Attribute</i> .....	607
<i>Instance Attribute</i> .....	607
<i>Common Service</i> .....	608
Base Switch Object.....	608
<i>Class Attribute List</i> .....	608
<i>Instance Attribute List</i> .....	608
<i>Common Service List</i> .....	610
Port Object .....	610
<i>Class Attribute List</i> .....	610
<i>Instance Attribute List</i> .....	611
<i>Common Service List</i> .....	612
TCP/IP Interface Object.....	612

<i>Class Attribute List</i> .....	612
<i>Instance Attribute List</i> .....	613
<i>Common Service List</i> .....	614
Ethernet Link Object .....	615
<i>Class Attribute List</i> .....	615
<i>Instance Attribute List</i> .....	616
<i>Interface Flags</i> .....	624
<i>Common Service List</i> .....	625
LLDP Management Object .....	626
<i>Class Attribute List</i> .....	626
<i>Instance Attribute List</i> .....	626
<i>Common Service List</i> .....	627
LLDP Data Table Object .....	627
<i>Common Attribute List</i> .....	628
<i>Instance Attribute</i> .....	628
<i>Common Service</i> .....	633
Moxa Networking Object (Vendor Specific) .....	634
<i>Class Attribute List</i> .....	634
<i>Instance Attribute List</i> .....	634
<i>Common Service List</i> .....	644
<b>Configuration Types</b> .....	<b>645</b>
<b>Event Log Descriptions</b> .....	<b>646</b>
<b>Modbus Data Map and Information</b> .....	<b>652</b>
System Information .....	652
Port Information .....	657
Packet Information .....	658
Redundancy Information .....	660

<b>Product Codes Used in Industrial Protocols .....</b>	<b>665</b>
<b>Security Guidelines .....</b>	<b>669</b>
Physical Installation .....	669
Account Management.....	669
Vulnerable Network Ports.....	670
Operation .....	670
Maintenance .....	674
Decommissioning .....	675
<b>Severity Level List .....</b>	<b>676</b>
<b>SNMP MIB Files.....</b>	<b>677</b>
Structure of the Moxa MIB group package .....	677
Standard MIB Installation Order .....	680
MIB Tree .....	681
<b>User Role Privileges.....</b>	<b>684</b>
Options Menu.....	684
System .....	685
Port .....	686
Layer 2 Switching .....	686
Network Interface.....	687
Redundancy.....	687
Network Service .....	688
Routing .....	688
Security .....	689
Diagnostics.....	690
Industrial Application .....	691

# Chapter 1

---

# Overview



# Introduction

Welcome to the MX-NOS user manual. This comprehensive guide is designed to help you understand and navigate the UI features, technical concepts, and tasks you may encounter while using your device. Our goal is to simplify your experience and make the setup process easier.

# About MX-NOS

## **MX-NOS**

Moxa's next-generation Ethernet switches are powered by MX-NOS, a tailored firmware platform that seamlessly integrates with your Moxa devices. This unlocks their full potential, transforming your switches into powerful tools with consistent functionality and a user-friendly interface.

How does Moxa achieve this? By providing a platform-based management OS, Moxa offers several key advantages, including:

- **Streamlined software management with regular updates:** Moxa keeps your switches up-to-date with the latest technologies throughout their lifetime. Continuous bug fixes and vulnerability synchronization ensure high software quality and improved network security.
- **Robust security by design:** Moxa adheres to IEC 62443-4-1 for software development lifecycles. As a result, MX-NOS provides a solid foundation for the switches running on it to build security features based on IEC 62443-4-2.
- **Consistent user experience:** MX-NOS features an intuitive UI that provides a consistent user experience across different browsing devices, minimizing training time and maximizing efficiency.

MX-NOS is more than just a firmware platform; it's a significant leap towards a superior user experience.

# What's in This Document

This document includes the following sections:

- **Overview:** This section introduces this document and how to use it.
- **Quick Start:** This section tells you how to connect to your device so you can start using and configuring it.
- **UI Reference:** This section goes through the web user interface (UI) of your device to help you quickly understand what settings are available. This section also shows you the valid ranges and defaults for settings, and any limitations there may be when configuring your device.
- **Appendix:** This section provides additional reference information for your device.

# Supported Series and Firmware Versions

Moxa Switch Series	Firmware Version
RKS-G4000 Series	v5.0

**Note**

We are continually improving and developing our software. Check regularly to see if there is an updated version of the software that provides you with additional benefits. You can find information and software downloads on the Moxa product pages at <https://www.moxa.com/en/support/product-support/software-and-documentation>.

# Product Series Feature Comparison Table

Refer to the table below for a full overview of the supported features for each product series model covered by this manual.

1. **YES:** Supported
2. **PARTIAL:** Partially supported
3. **-:** Unsupported

For more details on partially supported features, refer to their respective sections in this manual.

## Options Menu

Settings	RKS-4000-L3
Change Language	YES
Change Mode: Standard/Advanced Mode	YES
Disable Auto Save	YES
Locator	YES
Reboot	YES
Reset to Default Settings	YES
Log Out	YES

## System

Settings	RKS-4000-L3
System Management	YES

Settings	RKS-4000-L3
<b>Information Settings</b>	YES
<b>Firmware Upgrade</b>	YES
<b>Config Backup and Restore</b>	YES
<b>Account Management</b>	<b>YES</b>
<b>User Accounts</b>	YES
<b>Online Accounts</b>	YES
<b>Password Policy</b>	YES
<b>Management Interface</b>	<b>YES</b>
<b>User Interface</b>	YES
<b>Hardware Interfaces</b>	YES
<b>SNMP</b>	YES
<b>RMON1 (Only in CLI)</b>	YES
<b>Time</b>	<b>YES</b>
<b>System Time</b>	YES
<b>NTP Server</b>	YES
<b>Time Synchronization</b>	YES

## Port

Settings	RKS-4000-L3
<b>Port Interface</b>	<b>YES</b>
<b>Port Settings</b>	YES
<b>Linkup Delay</b>	YES

Settings	RKS-4000-L3
Link Aggregation	YES
PoE (for PoE models)	YES

## Layer 2 Switching

Settings	RKS-4000-L3
VLAN	YES
GARP	YES
MAC	YES
Static Unicast	YES
MAC Address Table	YES
QoS	YES
Classification	YES
Ingress Rate Limit	YES
Scheduler	YES
Egress Shaper	YES
Multicast	YES
IGMP Snooping	YES
GMRP	YES
Static Multicast	YES

## Network Interface

Settings	RKS-4000-L3
Network Interface	YES

## Redundancy

Settings	RKS-4000-L3
Layer 2 Redundancy	YES
Spanning Tree	YES
Turbo Ring v2	YES
Turbo Chain	YES
MRP	YES
Multiple Dual Homing	YES
Multiple Network Coupling	YES
Layer 3 Redundancy	YES
VRRP	YES
Tracking	YES

## Network Service

Settings	RKS-4000-L3
DHCP Server	-
DHCP Relay Agent	YES
DNS Server	YES



# Routing

Settings	RKS-4000-L3
<b>Unicast Route</b>	<b>YES</b>
<b>Static Routing</b>	YES
<b>OSPF Settings</b>	YES
<b>OSPF Status</b>	YES
<b>Routing Table</b>	YES
<b>Multicast Route</b>	<b>YES</b>
<b>PIM-DM</b>	YES
<b>PIM-SM Settings</b>	YES
<b>PIM-SM Status</b>	YES
<b>Multicast Local Route</b>	YES
<b>Multicast Routing Table</b>	YES

# Security

Settings	RKS-4000-L3
<b>Device Security</b>	<b>YES</b>
<b>Login Policy</b>	YES
<b>Trusted Access</b>	YES
<b>SSH &amp; SSL</b>	YES
<b>Network Security</b>	<b>YES</b>
<b>IEEE 802.1X</b>	YES

Settings	RKS-4000-L3
<b>MAC Authentication Bypass</b>	YES
<b>MAC Security</b>	YES
<b>Port Security</b>	YES
<b>Traffic Storm Control</b>	YES
<b>Access Control List</b>	YES
<b>Network Loop Protection</b>	YES
<b>Binding Database</b>	YES
<b>DHCP Snooping</b>	YES
<b>IP Source Guard</b>	YES
<b>Dynamic ARP Inspection</b>	YES
<b>Authentication</b>	<b>YES</b>
<b>Login Authentication</b>	YES
<b>RADIUS</b>	YES
<b>TACACS+</b>	YES

## Diagnostics

Settings	RKS-4000-L3
<b>System Status</b>	<b>YES</b>
<b>Resource Utilization</b>	YES
<b>Fiber Check</b>	YES
<b>Module Information</b>	YES
<b>Network Status</b>	<b>YES</b>

Settings	RKS-4000-L3
<b>Network Statistics</b>	YES
<b>LLDP</b>	YES
<b>ARP Table</b>	YES
<b>Tools</b>	<b>YES</b>
<b>Port Mirroring</b>	YES
<b>Ping</b>	YES
<b>Event Logs and Notifications</b>	<b>YES</b>
<b>Event Logs</b>	YES
<b>Event Notifications</b>	YES
<b>Syslog General</b>	YES
<b>Syslog Authentication</b>	YES
<b>SNMP Trap/Inform</b>	YES
<b>Email Settings</b>	YES
<b>Relay Alarm</b>	YES

## Industrial Application













Settings	RKS-4000-L3
<b>IEC 61850</b>	<b>YES</b>
<b>MMS</b>	YES
<b>GOOSE Check</b>	YES
<b>Modbus TCP</b>	<b>YES</b>
<b>EtherNet/IP</b>	<b>YES</b>
















<b>Settings</b>	<b>RKS-4000-L3</b>
<b>PROFINET</b>	<b>YES</b>

# Icons Used in the Web Interface

This table shows various icons used in the web interface and their corresponding meanings.

You can also hover your mouse over an icon to show an explanatory mouseover tip.

Symbols	Meanings
	Add
	Read detailed information
	Column selection
	Refresh
	Enable/Disable Auto Save When Auto Save is disabled, users need to click this icon to save changes to the startup configuration. Refer to <a href="#">Configuration Types</a> for more information.
	Export
	Edit
	Auto Refresh enabled
	Auto Refresh disabled
	Delete
	Clear all
	Panel view

Symbols	Meanings
	Expand
	Collapse
	Hint information
	Menu icon
	Change mode
	Locator
	Reboot
	Reset to default
	Log out
	Data comparison
	Increase
	Decrease
	Equal
	Menu
	Search

**Symbols**   **Meanings**



Copy



Warning



Reorder



Reorder priority



Set up related event notifications



Show text



Hide text



Remove



Select a file



Change language



Sync to the latest state or reauthenticate



View list



Remove the account



Relay alarm cut-off



How to set up

## Chapter 2

---

# Quick Start



# Using a Web Browser to Configure the Industrial Ethernet Switch

The device's web interface provides a convenient way to modify the switch's configuration and access the built-in monitoring and network administration functions.

## Note

When using the device's web interface, we recommend using the following browsers and versions. Please note that Internet Explorer (IE) is not supported.

- Chrome: 2 most recent versions
- Firefox: Latest version and the Extended Support Release (ESR)
- Edge: 2 most recent major versions
- Safari: 2 most recent major versions
- iOS: 2 most recent major versions
- Android: 2 most recent major versions

Perform the following steps to access the device's web interface:

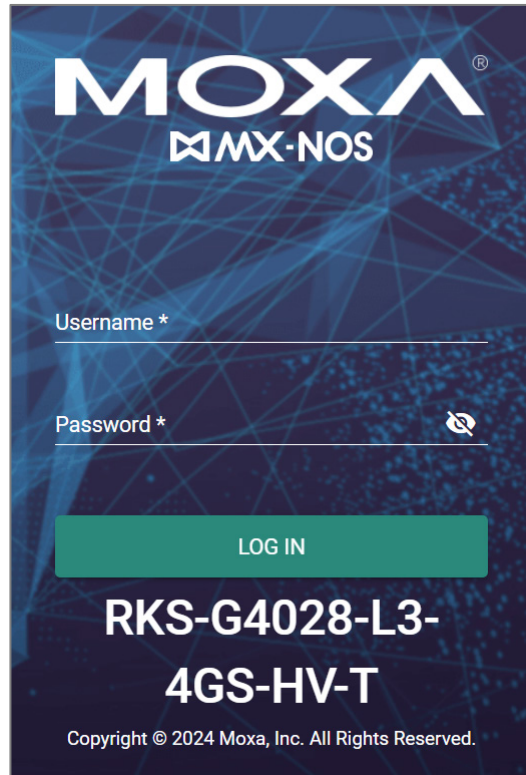
1. Make sure your PC host is connected to your device's LAN port, and is on the same subnet as your device.
2. Open a web browser and type the device's LAN IP address (**192.168.127.254** by default) into the address bar and press Enter.



3. The web login page will open. Enter the username (**admin** or **user**) and password (the same as the Console password) and click **LOG IN** to continue.

## Note

The default username is admin and the default password is moxa. We strongly recommend changing the password as soon as possible to ensure the security of your device.



You may need to wait a few moments for the web interface to appear.

4. After successfully connecting to the switch, the **Device Summary** screen will automatically appear. Use the menu tree on the left side of the window to open the function pages to access each of the switch's functions.

# Using a RS-232 Console to Configure the Device

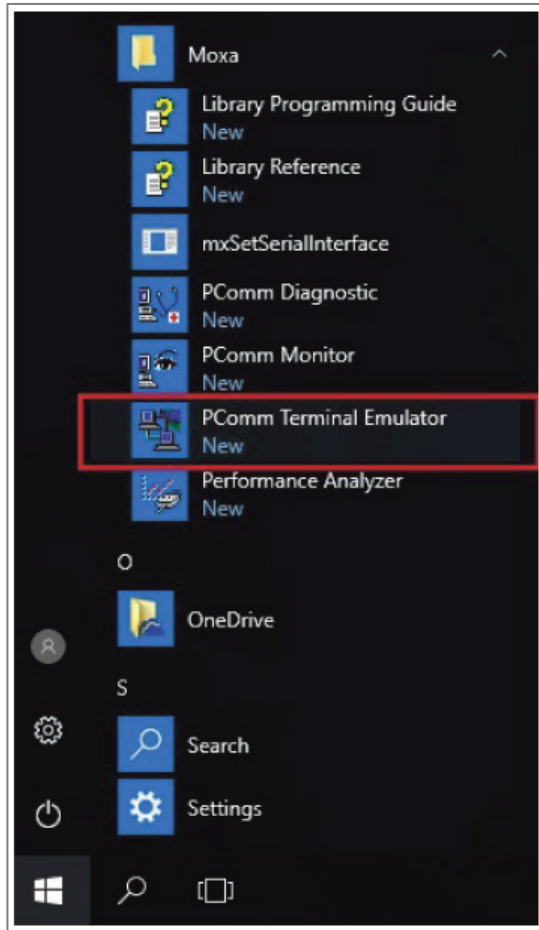
You can connect to your device's serial console port to configure settings.

Perform the following steps to connect to the serial console port:

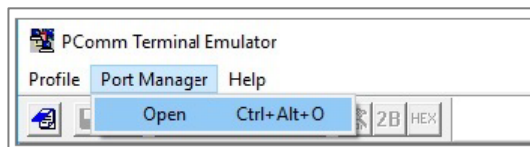
1. Prepare an RS-232 serial cable with an RJ45 interface.
2. Connect the RJ45 interface end to the console port on the device, and the other end to your computer.
3. We recommend you use PComm Terminal Emulator for serial communication. The software can be downloaded free of charge from Moxa's website.

Perform the following steps to configure your connection to access the device's console (PComm Terminal Emulator is used for these steps):

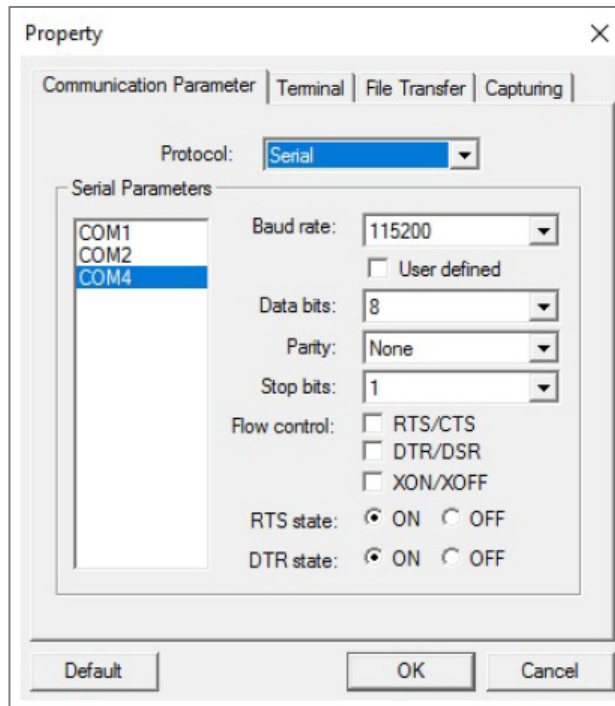
1. From the Windows desktop, click **Start > Moxa > PComm Terminal Emulator**.



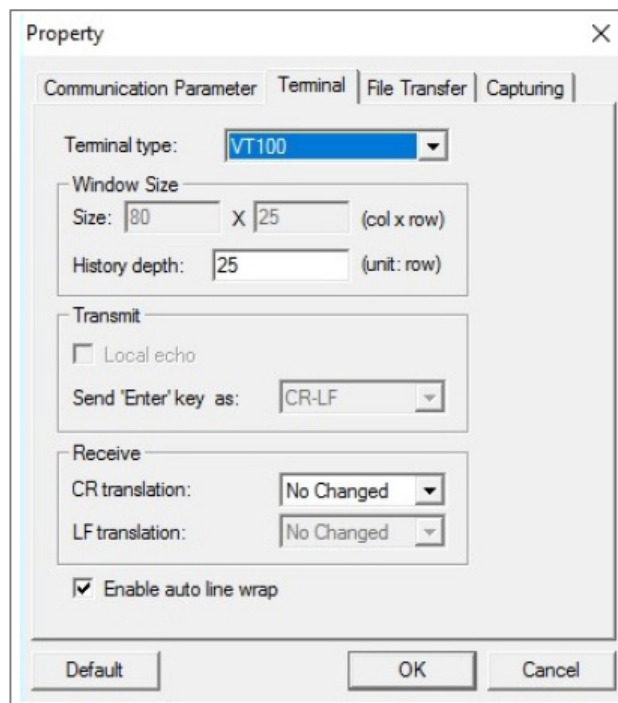
2. Select **Open** under the **Port Manager** menu to open a new connection.



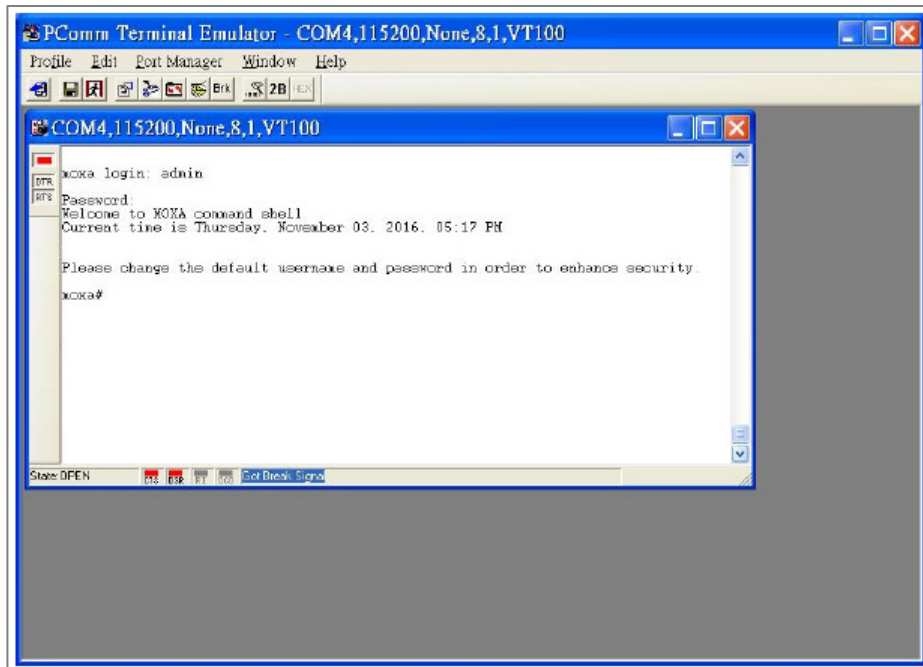
3. The **Property** window should open. In the **Communication Parameter** tab for **Ports**, select the COM port that is being used for the console connection. Set the other fields as follows: **115200** for **Baud Rate**, **8** for **Data Bits**, **None** for **Parity**, and **1** for **Stop Bits**.



4. In the **Terminal** tab, select **VT100** for **Terminal Type**, and then click **OK** to continue.



- The console will prompt you to log in. The default login name is **admin**, and the default password is **moxa**. This password will be required to access any of the consoles (web, serial, Telnet).



- After successfully connecting to the device's serial console, you can start configuring the its parameters by using command line instructions. Refer to the Moxa Command Line Interface Manual for details.

**Note**

By default, the password is moxa.

Make sure you change the default password after you first log in to help keep your system secure.

# Using Telnet to Configure the Device

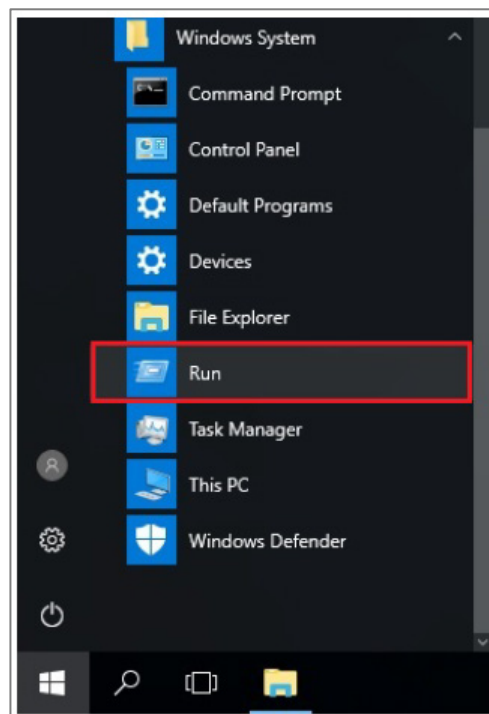
You can use Telnet to connect to the device and configure it. This requires the host and the target device to configure to be on the same logical subnet, so you may need to adjust your PC host's IP address and subnet mask. By default, the device IP address is **192.168.127.253** and the default subnet mask is **255.255.255.0**. For example, your PC's IP address must be set to 192.168.xxx.xxx if the subnet mask is 255.255.0.0, or to 192.168.127.xxx if the subnet mask is 255.255.255.0.

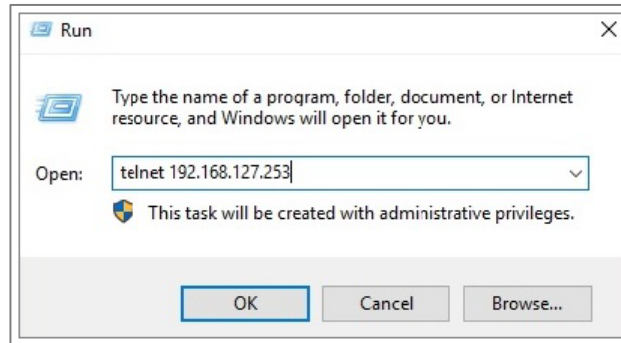
## Note

When connecting to the device using Telnet or its web interface, first connect one of the device's Ethernet ports to your Ethernet LAN, or directly to your PC's Ethernet port. You can use either a straight-through or cross-over Ethernet cable.

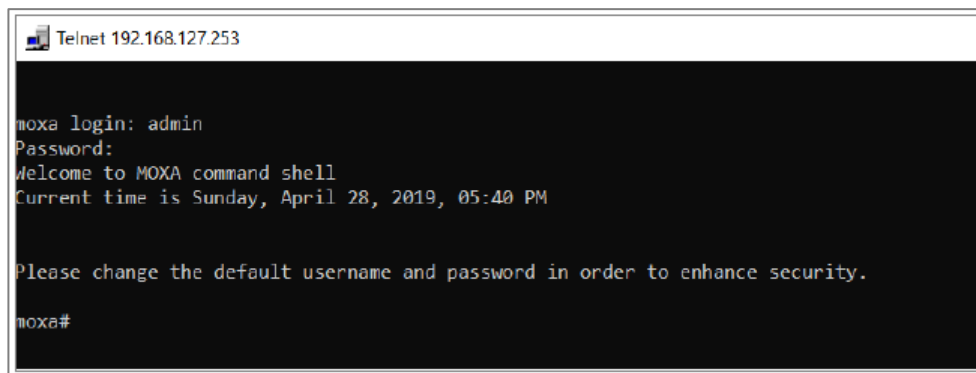
After making sure that the device is connected to the same LAN and logical subnet as your PC, perform these steps to connect to your device:

1. Click **Start > Run** from the Windows Start menu, then enter telnet followed by the device's IP address. You can also issue the Telnet command from a DOS prompt.





2. The Telnet console will prompt you to log in. The default login name is **admin**, and the default password is **moxa**. This password will be required to access any of the consoles (web, serial, Telnet).



3. After successfully logging in, you can start configuring the switch parameters by using command line instructions. Refer to the **Moxa Command Line Interface Manual**.

**Note**

By default, the password assigned to the Moxa switch is moxa.

Make sure you change the default password after you first log in to help keep your system secure.



## Chapter 3

---

# UI Reference

# UI Reference Overview

This section provides you with a quick reference to the different settings and options of your device.

To help you understand how to use the user interface, the following sections are included:

- The MX-NOS User Interface
- Options Menu

The rest of this section follows the order of the menu areas in the user interface:

# The MX-NOS User Interface

Moxa's managed switches offer a user-friendly web interface for easy configuration, reducing system maintenance and configuration effort.

This section describes how the web interface is laid out to make it easier for you to find and access the different function pages.

Here is an overview of the MX-NOS user interface:

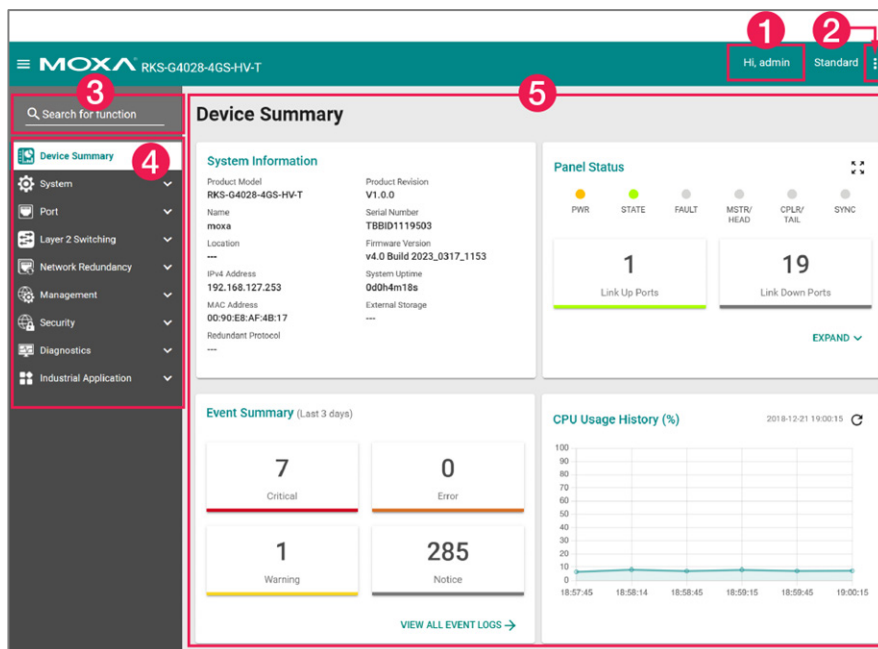


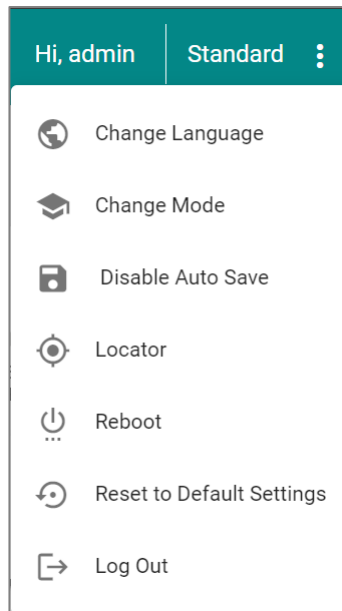
Figure 1 MX-NOS v4.0

1. **Login Name:** Shows the name of the currently logged in user.
2. **Configuration Mode:** Shows which configuration mode is being used:
  - **Standard Mode:** Some features and parameters will be hidden to make configuration simpler (enabled by default).
  - **Advanced Mode:** More features and parameters will be shown to allow for more detailed configuration.
3. **Search Bar:** Type in a function name to filter to the function menu.
4. **Function Menu:** All functions of the switch are shown here. Click the function you want to view or configure.

5. **Device Summary:** Shows device information and settings for the selected function.

# Options Menu

Clicking the **Options** ( ⋮ ) icon in the upper-right corner of the page will open the options menu.




## Options Menu - User Privileges

Privileges to settings are granted to the different authority levels as follows. Refer to [System > Account Management > User Accounts](#) for more information on user accounts.

Settings	Admin	Supervisor	User
<b>Change Language</b>	R/W	R/W	R/W
<b>Change Mode: Standard/Advanced Mode</b>	R/W	R/W	R/W
<b>Disable Auto Save</b>	R/W	R/W	-
<b>Locator</b>	R/W	R/W	R
<b>Reboot</b>	R/W	R/W	-
<b>Reset to Default Settings</b>	R/W	-	-
<b>Log Out</b>	R/W	R/W	R/W


## Change Language

To change the language of the interface, click the **Options** (  ) icon in the upper-right corner of the page, and select **Change Language**.

## Change Mode

There are two configuration modes available for users: **Standard Mode** and **Advanced Mode**.

- In **Standard Mode**, some of the features/parameters will be hidden to make it easier to perform configurations. This is the default setting.
- In **Advanced Mode**, advanced features/parameters will be available for users to adjust these settings.


To switch between modes, click the **Options** (  ) icon in the upper-right corner of the page, and select **Change Mode**.

## Disable/Enable Auto Save

Auto Save allows users to save all changes to the device's running configuration to the startup configuration immediately and automatically, so all changes will persist even after the device has restarted. Refer to [Configuration Types](#) for more information about the different configurations your device uses.

### **Note**

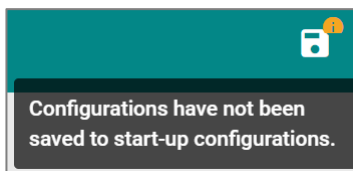
Auto Save is enabled by default.

To disable Auto Save, click the **Options** (  ) icon in the upper-right corner of the page, and select **Disable Auto Save**.

To save configuration changes to the startup configuration, click the **Save** (  ) icon.

**Note**

When auto save is disabled, if changes have not been saved and the device is restarted, all changes will be lost and the device will revert to its startup configuration.

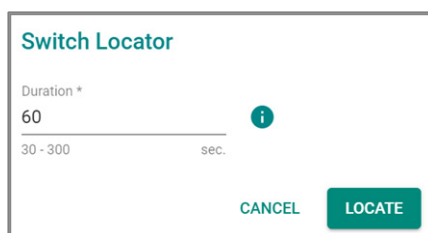


To re-enable Auto Save, click the **Options ( ⋮ )** icon in the upper-right corner of the page, and select **Enable Auto Save**.

## Locator

The Locator feature will cause the LED indicators on the device to flash, making it easier to locate and identify the specific device when installed at a field site.

To trigger the device locator, click the **Options ( ⋮ )** icon in the upper-right corner of the page, and select **Locator**. Select how long in seconds the LEDs should flash for, then click **LOCATE**.



## Reboot

To manually reboot the device, click the **Options ( ⋮ )** icon in the upper-right corner of the page, and select **Reboot**.

## Reset to Default Settings

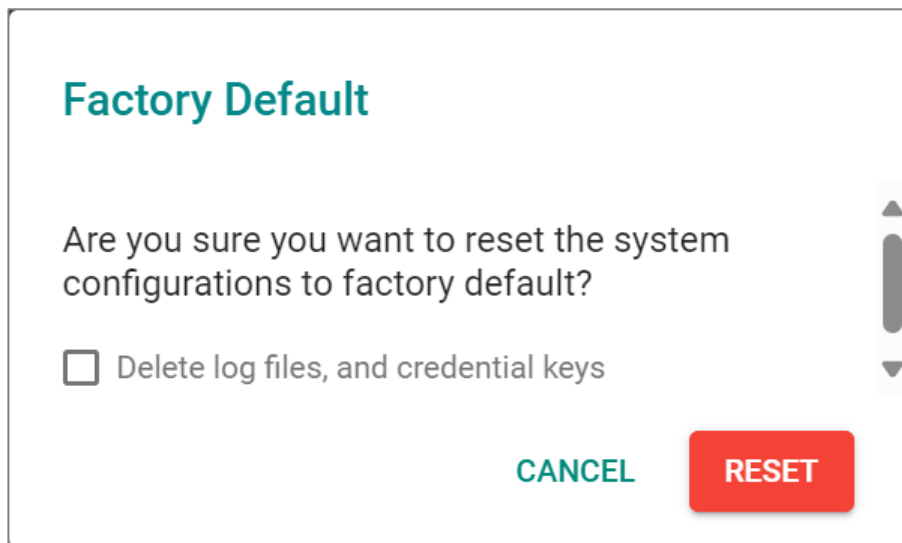
To reset the device to its default settings, click the **Options** ( ⋮ ) icon in the upper-right corner of the page, and select **Reset to Default Settings**.

If you want to delete all event logs and the certificate database, check the **Delete log files and credential keys** option. This will delete all information on the device and reset everything to its factory default value.

Click **RESET** to reset your device to the default settings.

### ▲ Warning

When resetting your device to the factory default settings, all your current configuration settings will be permanently deleted.



## Log Out

To log out of the device, click the **Options** ( ⋮ ) icon in the upper-right corner of the page, and select **Log Out**.



# Device Summary

## Menu Path: Device Summary

This page lets you see the current status of your device through a variety of display panels.

## System Information

This display shows basic information about your device and its current status.

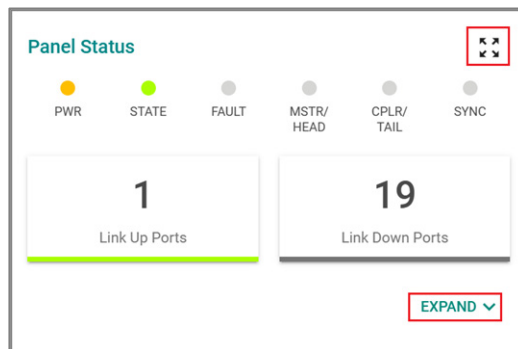
System Information	
Product Model	Product Revision
RKS-G4028-4GS-HV-T	V1.0.0
Name	Serial Number
moxa	TBBID1119503
Location	Firmware Version
---	v4.0 Build 2023_0317_1153
IPv4 Address	System Uptime
192.168.127.253	0d0h27m3s
MAC Address	External Storage
00:90:E8:AF:4B:17	---
Redundant Protocol	
---	

UI Setting	Description
<b>Product Model</b>	Shows the product model of the device.
<b>Name</b>	Shows the name of the device. Refer to <a href="#">System &gt; System Management &gt; Information Settings</a> for more information.
<b>Location</b>	Shows the location of the device. Refer to <a href="#">System &gt; System Management &gt; Information Settings</a> for more information.
<b>IPv4 Address</b>	Shows the IPv4 address of the device.
<b>MAC Address</b>	Shows the MAC address of your device.
<b>Redundant Protocol</b>	Shows the current redundancy protocol for this switch.
<b>Product Revision</b>	Shows the product revision of the device.

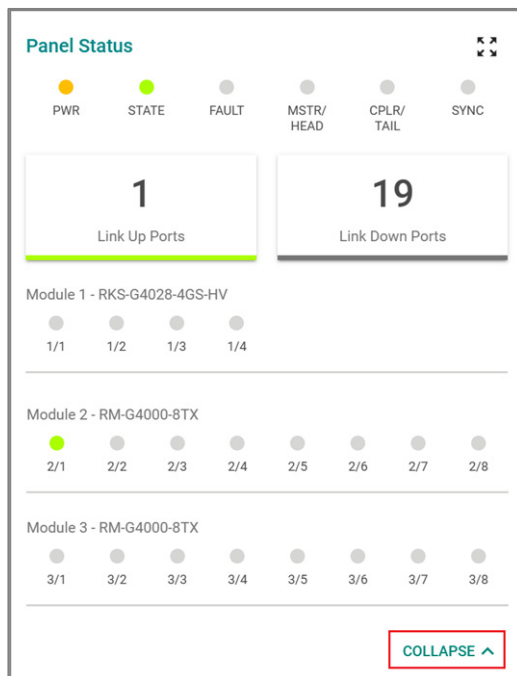
UI Setting	Description
<b>Serial Number</b>	Shows the serial number of your device.
<b>Firmware Version</b>	Shows the firmware version of your device.
<b>System Uptime</b>	Shows the amount of time your device has been continuously running for.
<b>External Storage</b>	Shows the external storage device currently connected to your device, if applicable.

## Panel Status

This display reflects the current status of the physical LEDs on your device, and shows how many ports currently have a link up or link down status. Grey is used to indicate an LED is off. For more information about status LEDs and their behavior, please refer to the QIG.



Click **EXPAND** to view more detailed information, or click **COLLAPSE** to return to the compact view.



## Panel View

By clicking the **Expand** (⌕) icon in **Panel Status**, you can see a visual representation of your device's ports.

Green ports have an active link. You can move your cursor over a port to show a mouseover with more information about that port.

Click the **Close** (✕) icon to close the **Panel View** and show **Panel Status** again.

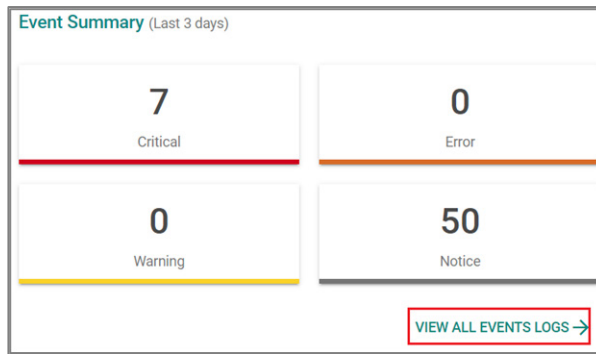
**Note**

The Panel View figure may vary depending on the device and the modules installed in it.



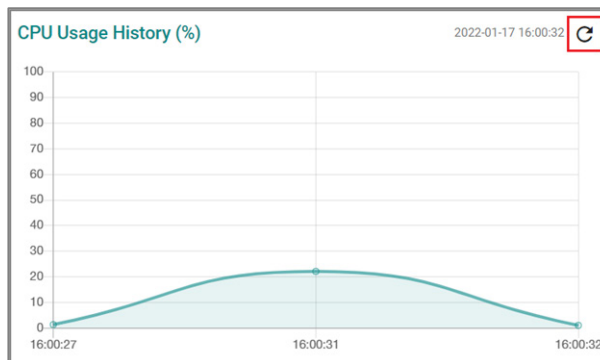
## Event Summary (Last 3 days)

This display shows an event summary for the past three days. Click **VIEW ALL EVENT LOGS** to go to the Diagnostics > Event Logs and Notifications > Event Logs page to view more detailed information.



## CPU Usage History (%)

This display shows the device's CPU usage shown as a percentage over time. Click the **Refresh** (🔄) icon to refresh the graph.



# System

## Menu Path: System

This section lets you adjust various system settings.

This section includes these pages:

- System Management
- Account Management
- Management Interface
- Time

## System - User Privileges

Privileges to System settings are granted to the different authority levels as follows.

Refer to [System > Account Management > User Accounts](#) for more information on user accounts.

Settings	Admin	Supervisor	User
<b>Device Summary</b>	R	R	R
<b>System Management</b>			
<b>Information Settings</b>	R/W	R/W	R
<b>Firmware Upgrade</b>	R/W	-	-
<b>Config Backup and Restore</b>	R/W	-	-
<b>Account Management</b>			
<b>User Accounts</b>	R/W	-	-
<b>Online Accounts</b>	R/W	-	-
<b>Password Policy</b>	R/W	-	-
<b>Management Interface</b>			

Settings	Admin	Supervisor	User
<b>User Interface</b>	R/W	-	-
<b>Hardware Interfaces</b>	R/W	R/W	R
<b>SNMP</b>	R/W	R	-
<b>Time</b>			
<b>System Time</b>	R/W	R/W	R
<b>NTP Server</b>	R/W	R/W	R
<b>Time Synchronization</b>	R/W	R/W	R

## System Management

### Menu Path: System > System Management

This section lets you adjust various system management related settings.

This section includes these pages:

- Information Settings
- Firmware Upgrade
- Config Backup and Restore

### Information Settings

#### Menu Path: System > System Management > Information Settings

This page lets you add additional information about the device to make it easier to identify different switches that are connected to your network. When finished, click APPLY to save your changes.

### Information Settings

Device Name \*  
 4 / 64

Location  
 0 / 255

Description  
 0 / 255

Contact Information  
 0 / 255

APPLY

UI Setting	Description	Valid Range	Default Value
<b>Device Name</b>	Specify a name for the device. This helps you differentiate between the roles or applications of different devices.	1 to 64 characters <ul style="list-style-type: none"> <li>characters: a-z, A-Z, 0-9</li> <li>special characters: . -</li> <li>The device name cannot start with-(dash) and cannot end with-(dash).</li> </ul>	moxa
<b>Location</b>	Specify a location for the device. This helps you differentiate between different locations or sites for different devices.	0 to 255 characters <ul style="list-style-type: none"> <li>characters: a-z, A-Z, 0-9</li> <li>special characters: ~ ! @ # \$ % ^ &amp; * ( ) { } [ ] &lt; &gt; _ + - = \ ; , . /</li> </ul>	N/A
<b>Description</b>	Specify a description for the device. This helps you keep a more detailed description of the device.	0 to 255 characters	N/A
<b>Contact Information</b>	Specify the contact information of the person in charge of the device. You can enter information such as an email address or telephone number for a person to contact if problems occur.	0 to 255 characters	N/A

## Firmware Upgrade

### Menu Path: System > System Management > Firmware Upgrade

You can upgrade the firmware through the following methods:

- Local
- TFTP
- SFTP
- USB

#### Note

It is highly recommended that you back up your device's configuration before upgrading the firmware. Refer to System > System Management > Configuration Backup and Restore for more information.

#### Note

If it is necessary to verify the integrity and signature of the application when the system is running, the administrator can use the show integrity check CLI command.

#### Warning

Upgrading the firmware should be only be done by qualified personnel, as it is possible to render the device inoperable if the upgrade is not done properly. If you are not familiar with the process, please request the assistance of qualified personnel. You can also consult with Moxa support and we will provide you with the necessary assistance.

Before performing a firmware upgrade, make sure you take the following precautions:

- Back up your configuration before upgrading the firmware
- Ensure that the device has power during the entire process
- Ensure that your computer stays connected to the device you are upgrading the firmware on
- Make sure the connection to the firmware source is not interrupted during the upgrade process

### Firmware Upgrade - Local

If you select **Local** as your **Method**, these settings will appear. The Local method lets you upload firmware directly from local storage on the host device.



**Note**

Before performing a firmware upgrade, download the updated firmware (\*.rom) file first from Moxa's website (www.moxa.com).

The screenshot shows the 'Firmware Upgrade' form with the 'Method' dropdown menu set to 'Local'. Below the dropdown is a 'Select File \*' field with a folder icon. A green 'UPGRADE' button is located at the bottom left of the form.

UI Setting	Description	Valid Range	Default Value
<b>Select File</b>	Select the new firmware file (*.rom) to use from your computer.	Select a file from your computer	N/A

### Firmware Upgrade - TFTP

If you select **TFTP** as your **Method**, these settings will appear. The TFTP method lets you upload and install firmware stored on a remote TFTP server.

The screenshot shows the 'Firmware Upgrade' form with the 'Method' dropdown menu set to 'TFTP'. Below the dropdown are two text input fields: 'Server IP Address \*' and 'File Name \*'. A green 'UPGRADE' button is located at the bottom left of the form.

UI Setting	Description	Valid Range	Default Value
<b>Server IP Address</b>	Specify the IP address of the TFTP server where the new firmware file (*.rom) is located.	Valid IP address	N/A
<b>File Name</b>	Specify the filename of the new firmware.	File name	N/A

## Firmware Upgrade - SFTP

If you select **SFTP** as your **Method**, these settings will appear. The SFTP method lets you upload and install firmware stored on a remote SFTP server.

### Firmware Upgrade

Method \*  
SFTP

Server IP Address \*

File Name \*

Account \*

Password \*

UI Setting	Description	Valid Range	Default Value
<b>Server IP Address</b>	Specify the IP address of the SFTP server where the new firmware file (*.rom) is located.	Valid IP address	N/A
<b>File Name</b>	Specify the filename of the new firmware.	File name can only contain A-Z, a-z, 0-9 or the symbols -._().	N/A
<b>Account</b>	Enter the SFTP server account name to use to connect to the SFTP server.	Account	N/A
<b>Password</b>	Enter the SFTP server account password to use to connect to the SFTP server.	Password	N/A

## Firmware Upgrade - USB


If you select **USB** as your **Method**, these settings will appear. The USB method allows you to upgrade the firmware via Moxa's USB-based ABC-02 configuration tool.

### **Note**

To use this feature, USB Function must be enabled in System > Management Interface > Hardware Interface.

## Firmware Upgrade

Method \*  
USB

Select File \* 

**UPGRADE**

UI Setting	Description	Valid Range	Default Value
<b>Select File</b>	Select the new firmware file (*.rom) to use from your USB device.	Select a file from the USB device	N/A

## Firmware Upgrade - microSD

If you select **microSD** as your **Method**, these settings will appear. The microSD method allows you to upgrade the firmware via Moxa's USB-based ABC-03 configuration tool.

### **Note**

To use this feature, microSD Function must be enabled in System > Management Interface > Hardware Interfaces.

UI Setting	Description	Valid Range	Default Value
<b>Select File</b>	Select the new firmware file (*.rom) to use from your USB device.	Select a file from the microSD device	N/A

## Configuration Backup and Restore

**Menu Path:** [System](#) > [System Management](#) > [Configuration Backup and Restore](#)

This page helps you back up and restore your device configuration.

This page includes these tabs:

- Backup
- Restore
- File Encryption
- File Signature

### Configuration Backup and Restore - Backup

**Menu Path:** [System](#) > [System Management](#) > [Configuration Backup and Restore - Backup](#)

This section lets you create a backup of the current device configuration.

There are multiple methods of backing up the device configuration:

- Local
- TFTP

- SFTP
- USB
- microSD

**Note**

For security reasons, we strongly recommend that you back up the system configuration to a secure storage location periodically.

### Configuration Backup - Local

If you select **Local** as your **Method**, these settings will appear. The Local method will export the configuration backup file to the local host.

Method \*

Local

---

Select Configuration \*

Running Configuration

---

Default Configuration \*

Not Included

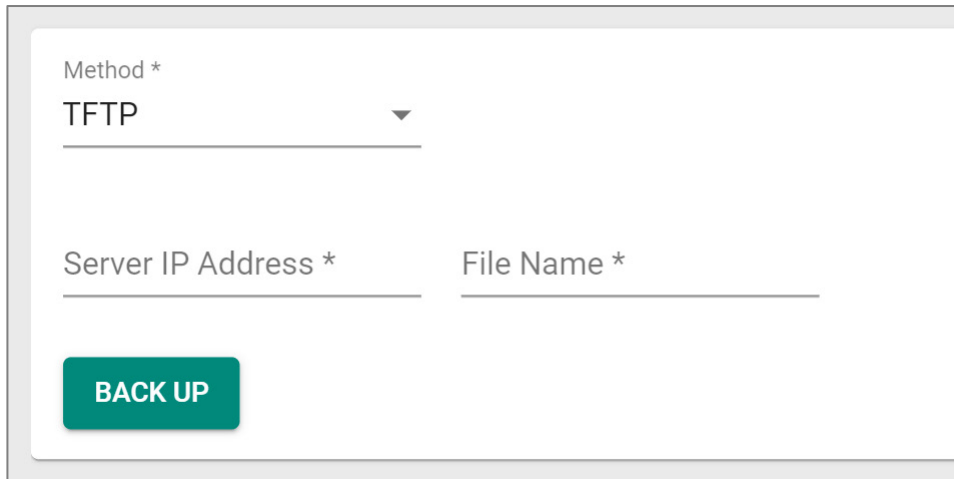
---

**BACK UP**

UI Setting	Description	Valid Range	Default Value
<b>Select Configuration</b>	Choose to back up the running configuration or the startup configuration of the switch.	Running Configuration / Startup Configuration	Running Configuration
<b>Default Configuration</b>	Choose to back up the configuration without or with default settings.	Not Included / Included	Not Included

## Configuration Backup - TFTP

If you select **TFTP** as your **Method**, these settings will appear. The TFTP method lets you upload the configuration backup file to a remote TFTP server.



The screenshot shows a configuration form for TFTP backup. It includes a dropdown menu for 'Method \*' with 'TFTP' selected. Below it are two text input fields: 'Server IP Address \*' and 'File Name \*'. A green 'BACK UP' button is positioned at the bottom left of the form area.


UI Setting	Description	Valid Range	Default Value
<b>Server IP Address</b>	Specify the IP address of the TFTP server to upload the backup to.	Valid IP address	N/A
<b>File Name</b>	Specify a filename for the backup.	N/A	N/A

## Configuration Backup - SFTP

If you select **SFTP** as your **Method**, these settings will appear. The SFTP method lets you upload the configuration backup file to a remote SFTP server.

Method \*  
SFTP

Server IP Address \*      File Name \*

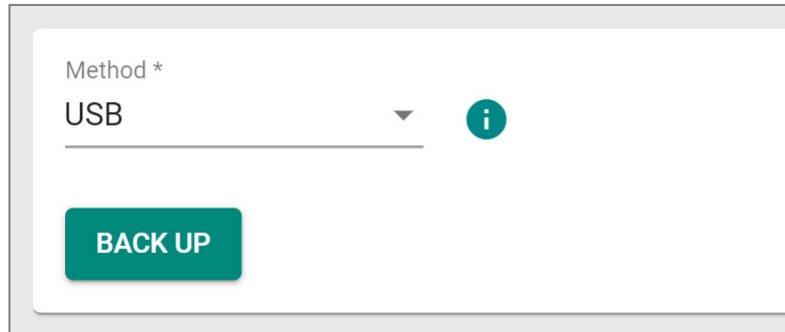
Account \*      Password \* 

**BACK UP**

UI Setting	Description	Valid Range	Default Value
<b>Server IP Address</b>	Specify the IP address of the SFTP server to upload the backup to.	Valid IP address	N/A
<b>File Name</b>	Specify a filename for the backup.	File name can only contain A-Z, a-z, 0-9 or the symbols -._().	N/A
<b>Account</b>	Enter the SFTP server account name to use to connect to the SFTP server.	N/A	N/A
<b>Password</b>	Enter the SFTP server account password to use to connect to the SFTP server.	N/A	N/A

### Configuration Backup - USB

If you select **USB** as your **Method**, these settings will appear. The USB method allows you to export the configuration backup file to a Moxa ABC-02 configuration tool connected to the device. Insert a Moxa ABC-02 configuration tool into the USB port of the switch, then click **BACK UP** to back up the system configuration file.



### Configuration Backup - microSD

If you select **microSD** as your **Method**, these settings will appear. The microSD method allows you to export the configuration backup file to a microSD card inserted into your device.

#### Note

To use this feature, microSD Function must be enabled in System > Management Interface > Hardware Interfaces.

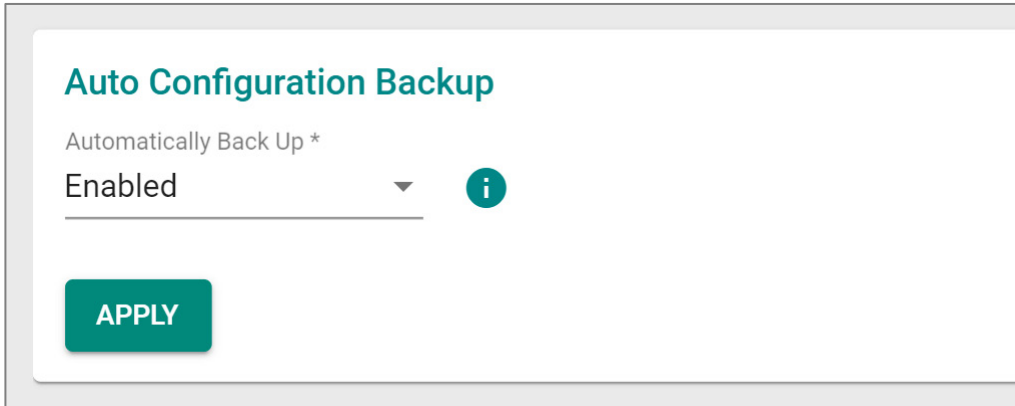


### Auto Configuration Backup

Auto configuration backup lets you automatically back up the configuration file to an ABC-02 configuration tool or microSD card whenever the configuration is changed.

To enable automatic backup, select **Enabled** from the drop-down list, then click **APPLY**.





UI Setting	Description	Valid Range	Default Value
<b>Automatically Back Up</b>	<p>When enabled, this will back up the current configuration to an inserted ABC-02 configuration tool or microSD card.</p> <div style="background-color: #f0f0f0; padding: 10px; margin: 10px 0;"> <p><b>Note</b></p> <p>To use an ABC-02 configuration tool, <b>USB Function</b> must be enabled in <b>System &gt; Management Interface &gt; Hardware Interface</b>.</p> <p>To use a microSD card, <b>microSD Function</b> must be enabled in <b>System &gt; Management Interface &gt; Hardware Interfaces</b>.</p> </div> <div style="background-color: #f0f0f0; padding: 10px; margin: 10px 0;"> <p><b>Note</b></p> <p>If both an ABC-02 configuration tool and a microSD card are inserted into the device, the ABC-02 configuration tool will be used.</p> </div>	Enabled / Disabled	Enabled

## Configuration Backup and Restore - Restore

**Menu Path: System > System Management > Configuration Backup and Restore - Restore**

This page lets you restore a previously backed up configuration.

There are multiple methods of restoring the device configuration:

- Local
- TFTP
- SFTP
- USB
- microSD

**Note**

To ensure that configuration files can be successfully imported, do not manually modify them.

### Configuration Restore - Local

If you select **Local** as your **Method**, these settings will appear. The Local method will restore from a configuration file on the local host.

## Configuration Backup and Restore

Backup
Restore
File Encryption
File Signature

Method \*

Local ▼

---

Select File \*

📁

RESTORE

UI Setting	Description	Valid Range	Default Value
<b>Select File</b>	Select the configuration file to use from your computer.	Select a file from your computer	N/A

## Configuration Restore - TFTP

If you select **TFTP** as your **Method**, these settings will appear. The TFTP method lets you download and install a configuration stored on a remote TFTP server.

### Configuration Backup and Restore

- Backup
- Restore**
- File Encryption
- File Signature

Method \*  
TFTP

Server IP Address \*      File Name \*

**RESTORE**

UI Setting	Description	Valid Range	Default Value
<b>Server IP Address</b>	Specify the IP address of the TFTP server.	Valid IP address	N/A
<b>File Name</b>	Specify the file name of the configuration file to restore from.	Up to 54 characters, including file extension	N/A

## Configuration Restore - SFTP

If you select **SFTP** as your **Method**, these settings will appear. The SFTP method lets you download and install a configuration stored on a remote SFTP server.

## Configuration Backup and Restore

Backup
Restore
File Encryption
File Signature

Method \*  
SFTP ▾

Server IP Address \*      File Name \*

Account \*                  Password \*

RESTORE

UI Setting	Description	Valid Range	Default Value
<b>Server IP Address</b>	Specify the IP address of the SFTP server.	Valid IP address	N/A
<b>File Name</b>	Specify the file name of the configuration file to restore from.	File name can only contain A-Z, a-z, 0-9 and special character -._().	N/A
<b>Account</b>	Enter the SFTP server account name to use to connect to the SFTP server.	Account	N/A
<b>Password</b>	Enter the SFTP server account password to use to connect to the SFTP server.	Password	N/A

### Configuration Restore - USB


If you select USB as your **Method**, these settings will appear. The USB method allows you to restore the configuration from a file via Moxa's USB-based ABC-02 configuration tool.


**Note**

To use this feature, USB Function must be enabled in System > Management Interface > Hardware Interface.

## Configuration Backup and Restore

Backup   **Restore**   File Encryption   File Signature

Method \*  
USB 

Select File \* 

**RESTORE**

UI Setting	Description	Valid Range	Default Value
<b>Select File</b>	Select the configuration file to use from your USB device.	Select a file from the USB device	N/A

### Configuration Restore - microSD

If you select **microSD** as your **Method**, these settings will appear. The microSD method allows you to restore the configuration from a microSD card inserted into your device.

**Note**

To use this feature, microSD Function must be enabled in System > Management Interface > Hardware Interfaces.

UI Setting	Description	Valid Range	Default Value
<b>Select File</b>	Select the configuration file to use from the microSD card.	Select a file from the microSD card	N/A

### Auto Configuration Restore

Auto configuration restore lets you restore the device's configuration from an inserted ABC-02 configuration tool or microSD card whenever the device is rebooted.

To enable automatic restore, select **Enabled** from the drop-down list, then click **APPLY**.

UI Setting	Description	Valid Range	Default Value
<b>Automatically Restore</b>	When enabled, this will restore the device's configuration from an inserted ABC-02 configuration tool or microSD card whenever the device is rebooted.	Enabled / Disabled	Enabled
<div style="background-color: #f0f0f0; padding: 10px; margin: 10px 0;"> <p><b>Note</b></p> <p>To use an ABC-02 configuration tool, <b>USB Function</b> must be enabled in <b>System &gt; Management Interface &gt; Hardware Interface</b>.</p> <p>To use a microSD card, <b>microSD Function</b> must be enabled in <b>System &gt; Management Interface &gt; Hardware Interfaces</b>.</p> </div>			
<div style="background-color: #f0f0f0; padding: 10px; margin: 10px 0;"> <p><b>Note</b></p> <p>If both an ABC-02 configuration tool and a microSD card are inserted into the device, the ABC-02 configuration tool will be used.</p> </div>			

## Configuration Backup and Restore - File Encryption

**Menu Path: System > System Management > Configuration Backup and Restore - File Encryption**

This page lets you configure data encryption settings for exported configuration files.

### Configuration Backup and Restore

Backup
Restore
File Encryption
File Signature

Configuration File Encryption \*

Disabled ▼

Password 🔑

..... 0 / 60

APPLY

UI Setting	Description	Valid Range	Default Value
<b>Configuration File Encryption</b>	Enable/disable encryption of configuration files.	Enabled / Disabled	Disabled
<b>Password</b>	Specify the password used to encrypt configuration files.	1 to 60 characters	N/A

## File Signature

### Menu Path: System > System Management > Configuration Backup and Restore - File Signature

This page lets you enable use of file signatures to help ensure the file integrity and authenticity of your configuration files.

#### Note

Before enabling file signatures, you will need to add a private/public key to the table on this page.



### 🔒 Limitations

You can add up to 1 key to use for file signatures.

## Signed Configuration

The screenshot shows the 'Configuration Backup and Restore' interface with the 'File Signature' tab selected. The 'Signed Configuration' dropdown is set to 'Disabled'. Below it is an 'APPLY' button. A table below the button is empty, with headers 'Key', 'Label', 'Algorithm', and 'Length'. The table indicates a maximum of 1 key and currently shows 0 of 0 keys.

UI Setting	Description	Valid Range	Default Value
<b>Signed Configuration</b>	Enables or disables the use of a digital signature to check the integrity of configuration files.  <b>Note</b> To enable this feature, a private/public key must be installed first. Refer to <a href="#">Adding a Custom Key</a> for more information.	Enabled / Disabled	Disabled

## File Signature Key List

The screenshot shows a table with one key entry. The table has headers 'Key', 'Label', 'Algorithm', and 'Length'. The entry is 'Private/Certificate' with label 'Test', algorithm 'RSA', and length '2048'. The table indicates a maximum of 1 key and currently shows 1 - 1 of 1 keys.

UI Setting	Description
<b>Key</b>	Shows whether the key is a public or private key.
<b>Label</b>	Shows the label used to help identify the key.
<b>Algorithm</b>	Shows the algorithm used for the key, such as RSA or ECDSA.
<b>Length</b>	Shows the length of the key in bits.

## Adding a Custom Key

### Menu Path: System > System Management > Configuration Backup and Restore - File Signature

Clicking the **Add** (🔑) icon on the **System > System Management > Configuration Backup and Restore - File Signature** page will open this dialog box. This dialog lets you add a custom key to use for file signatures.

Click **CREATE** to save your changes and add the new key.

UI Setting	Description	Valid Range	Default Value
<b>Label</b>	Specify a label to help describe the certificate and the key.	0 to 16 characters	N/A
<b>Certificate</b>	Select a certificate file to import from your computer.	Select a certificate file from your computer	N/A
<b>Key</b>	Select a key file to import from your computer.	Select a key file from your computer	N/A

# Account Management

## Menu Path: System > Account Management

This section lets you manage user accounts for your device. You can enable different accounts with different roles to facilitate convenient management and safe access.

This section includes these pages:

- User Accounts
- Online Accounts
- Password Policy

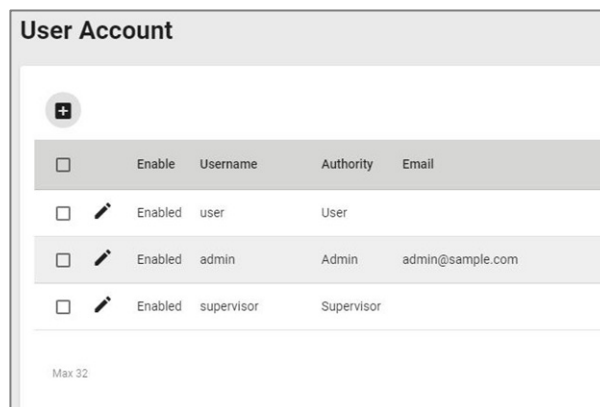
## User Accounts




### Menu Path: System > Account Management > User Accounts

This page lets you manage the user accounts for your device.

#### Note

By default, there is only one account: admin



<input type="checkbox"/>	Enable	Username	Authority	Email
<input type="checkbox"/>		Enabled user	User	
<input type="checkbox"/>		Enabled admin	Admin	admin@sample.com
<input type="checkbox"/>		Enabled supervisor	Supervisor	

Max 32

UI Setting	Description
<b>Enable</b>	Shows whether the account is enabled or disabled.
<b>Username</b>	Shows the username of the account.

UI Setting	Description
<b>Authority</b>	Shows the authority level of the account.
<b>Email</b>	Shows the email address of the account.

## User Accounts - Create a New Account

### Menu Path: System > Account Management > User Accounts


Clicking the **Add (+)** icon on the **System > Account Management > User Accounts** page will open this dialog box. This dialog lets you create a new user account. Click **CREATE** to save your changes and add the new account.


### Create a New Account

Enable \*

Username \*  
  
Minimum 4 characters 0 / 32


Authority \*

New Password \*    
Minimum 4 characters 0 / 63

Confirm Password \*    
Minimum 4 characters 0 / 63


Email  
  
0 / 63

UI Setting	Description	Valid Range	Default Value
<b>Enable</b>	Enable or disable the user account.	Enabled / Disabled	Enabled
<b>Username</b>	Specify a username for this account.	4 to 32 characters	N/A

UI Setting	Description	Valid Range	Default Value
<b>Authority</b>	<p>Specify the authority level of the account. Refer to the <a href="#">Account Privileges List</a> for a list of what read/write access privileges are granted for the different authority levels.</p> <ul style="list-style-type: none"> <li>• <b>Admin:</b> This account has read/write access of all configuration parameters.</li> <li>• <b>Supervisor:</b> This account has read/write access for a limited set of configuration parameters.</li> <li>• <b>User:</b> This account can only view a limited set of configuration parameters.</li> </ul> <div style="background-color: #f0f0f0; padding: 10px; margin-top: 10px;"> <p> <b>Note</b></p> <p>In order to enhance security, we suggest you create a new account with the User authority.</p> </div>	Admin / Supervisor / User	N/A
<b>New Password</b>	Specify the new password for this account.	4 to 63 characters, additional requirements are based on settings in <b>System &gt; Account Management &gt; Password Policy</b>	N/A
<b>Confirm Password</b>	Reenter the password to confirm.	4 to 63 characters, must match <b>New Password</b>	N/A
<b>Email</b>	Specify an email address for the account (optional).	Valid email address, 0 to 63 characters	N/A

## User Accounts - Edit This Account

### Menu Path: **System > Account Management > User Accounts**

Clicking the **Edit** () icon on the **System > Account Management > User Accounts** page will open this dialog box. This dialog lets you edit an existing user account. Click **APPLY** to save your changes.

### Edit This Account

Enable \*  
 Enabled ▼

Username  
 admin CHANGE PASSWORD

Minimum 4 characters 5 / 32

Authority \*  
 Admin ▼

Email  
 admin@sample.com 16 / 63

CANCEL APPLY

UI Setting	Description	Valid Range	Default Value
<b>Enable</b>	Enable or disable the user account.	Enabled / Disabled	Enabled
<b>Username</b>	Shows the username of the account.	N/A	N/A
	<p> <b>Note</b></p> <p>The username cannot be edited after creating an account.</p>		
<b>Authority</b>	<p>Specify the authority level of the account. Refer to the Account Privileges List for a list of what read/write access privileges are granted for the different authority levels.</p> <ul style="list-style-type: none"> <li><b>Admin:</b> This account has read/write access of all configuration parameters.</li> <li><b>Supervisor:</b> This account has read/write access for a limited set of configuration parameters.</li> <li><b>User:</b> This account can only view a limited set of configuration parameters.</li> </ul>	Admin / Supervisor / User	N/A
<b>Change Password</b>	Click <b>CHANGE PASSWORD</b> to change the account password. Refer to <a href="#">Edit the Account Password</a> for more information.	N/A	N/A


UI Setting	Description	Valid Range	Default Value
<b>Email</b>	Specify an email address for the account (optional).	Valid email address, 0 to 63 characters	N/A


## Edit the Account Password

Clicking **CHANGE PASSWORD** in the **Edit This Account** dialog will open this dialog box. This dialog lets you change the password for an account. Click **APPLY** to save your changes.


### Edit the Account Password

Username  
 Test  
 Minimum 4 characters 4 / 32

New Password \*   
 Minimum 4 characters 0 / 63

Confirm Password \*   
 Minimum 4 characters 0 / 63

[BACK](#)
[APPLY](#)

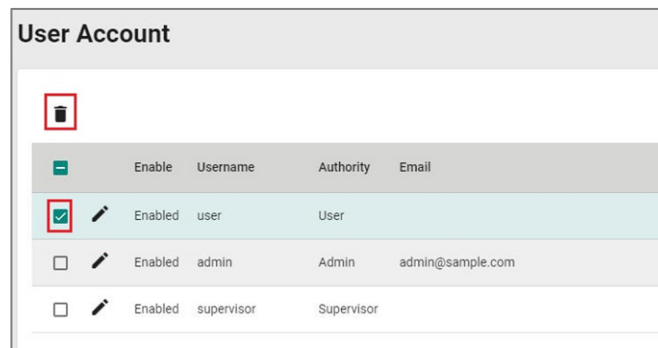
UI Setting	Description	Valid Range	Default Value
<b>Username</b>	Shows the username of the account.	N/A	N/A
	<div style="background-color: #f0f0f0; padding: 5px; border: 1px solid #ccc;"> <p> <b>Note</b>                      The username cannot be edited after creating an account.</p> </div>		
<b>New Password</b>	Specify the new password for this account.	4 to 63 characters, additional requirements are based on settings in <b>System &gt; Account Management &gt; Password Policy</b>	N/A

UI Setting	Description	Valid Range	Default Value
<b>Confirm Password</b>	Reenter the password to confirm.	4 to 63 characters, must match <b>New Password</b>	N/A

## User Accounts - Delete Account

### Menu Path: System > Account Management > User Accounts

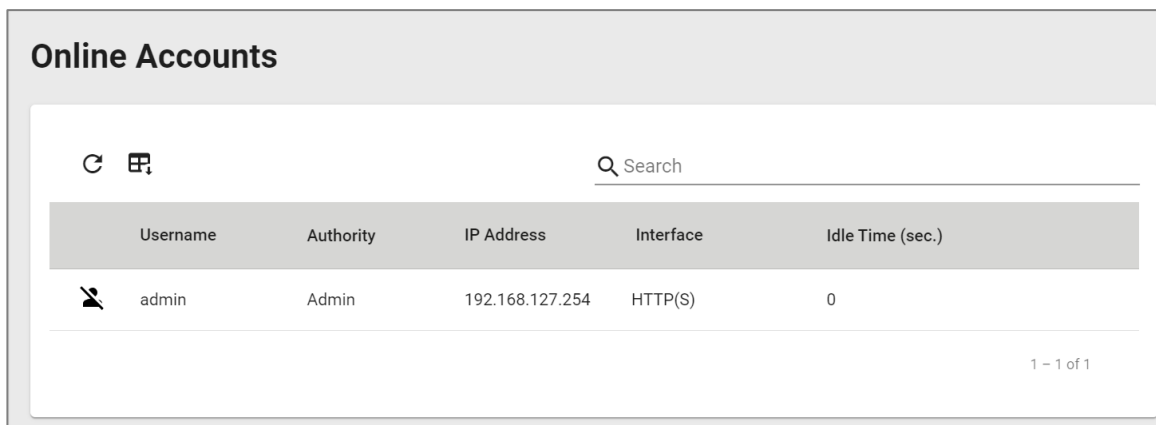
You can delete an account by using the checkboxes to select the entries you want to delete, then clicking the **Delete** (🗑️) icon.



## Online Accounts

### Menu Path: System > Account Management > Online Accounts

This page lets you view a list of connected user and also lets you disconnect users.





UI Setting	Description
<b>Username</b>	Shows the username of the online account.
<b>Authority</b>	Shows the authority level of the online account.
<b>IP Address</b>	Shows the IP address of the online account.
<b>Interface</b>	Shows the interface that the online account is using.
<b>Idle Time (sec.)</b>	Show the idle time in seconds for the online account.

## Online Accounts - Remove This Online Account

### Menu Path: System > Account Management > Online Accounts

You can disconnect a user by clicking its **Remove** (🗑️) icon. Click **REMOVE** to save your changes and remove the online account.

## Password Policy

### Menu Path: System > Account Management > Password Policy

This page lets you create a robust password policy to safeguard your system against hackers. By enforcing minimum length and complexity requirements, you can empower users to choose strong passwords that are difficult to crack. Additionally, you can set a maximum password lifetime to ensure regular password changes, further enhancing security. Click **APPLY** to save your changes.

#### Note

To improve the security of your device and network, we recommend that you:

- Set the Minimum Length for passwords to 16
- Enable the Password complexity strength check and enable all the requirements
- Set a Maximum Password Lifetime to ensure that users change their password regularly

## Password Policy

Minimum Password Length \*

4

4 - 63

### Password Complexity Strength Check

- Must contain at least one digit (0-9)
- Must contain at least one uppercase letter (A-Z)
- Must contain at least one lowercase letter (a-z)
- Must contain at least one special character ({ } [ ] ( ) | ; ~ ! @ # % ^ \* \_ + = , .)

Maximum Password Lifetime \*

0

0 - 365 day

APPLY

UI Setting	Description	Valid Range	Default Value
<b>Minimum Password Length</b>	Specify the minimum required password length.	4 to 16 characters	4
<b>Password Complexity Strength Check</b>	Select the complexity requirements that will apply to new passwords. <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p><b>Note</b></p> <p>New requirements will only apply when creating or changing a password. They will not apply to existing passwords.</p> </div>	Must contain at least one digit (0-9) / Must contain at least one uppercase letter (A-Z) / Must contain at least one lowercase letter (a-z) / Must contain at least one special character ({ } [ ] ( )   ; ~ ! @ # % ^ * _ + = , .)	N/A
<b>Maximum Password Lifetime</b>	Specify how long in days passwords will be valid for. When the password expires, the system will require the user to change their password. <p>If this is set to 0, passwords will not expire.</p>	0 to 365 days	0

# Management Interface

## Menu Path: [System](#) > [Management Interface](#)

This section lets you configure the interfaces used to manage the device.

This section includes these pages:

- [User Interface](#)
- [Hardware Interfaces](#)
- [SNMP](#)

## User Interface

### Menu Path: [System](#) > [Management Interface](#) > [User Interface](#)

This page lets you configure which interfaces can be used to access the device. Click **APPLY** to save your changes.

**Note**



For security reasons, users should access the device using secure HTTPS and SSH interfaces.


### User Interface

HTTP *	Enabled	HTTP - TCP Port *	80
			80, 1024 - 65535
HTTPS *	Enabled	HTTPS - TCP Port *	443
			443, 1024 - 65535
Telnet *	Disabled	Telnet - TCP Port *	23
			23, 1024 - 65535
SSH *	Enabled	SSH - TCP Port *	22
			22, 1024 - 65535
SNMP *	Disabled	SNMP - UDP Port *	161
			161, 1024 - 65535
Moxa Service *	Enabled	Moxa Service (Encrypted) - TCP Port	443
		Moxa Service (Encrypted) - UDP Port	40404
			1 - 65535
			1 - 65535
Maximum Number of Login Sessions for HTTP+HTTPS *			
5			
1 - 10			
Maximum Number of Login Sessions for Telnet+SSH *			
1			
1 - 5			

**APPLY**

UI Setting	Description	Valid Range	Default Value
<b>HTTP</b>	Enable or disable HTTP connections.	Enabled / Disabled	Enabled
<b>HTTP - TCP Port</b>	Specify the TCP port to use for HTTP connections.	80, 1024 to 65535	80

UI Setting	Description	Valid Range	Default Value
<b>HTTPS</b>	<p>Enable or disable HTTPS connections.</p> <div style="background-color: #f0f0f0; padding: 10px; margin-top: 10px;"> <p> <b>Note</b></p> <p>The administrator can manually import a self-signed certificate (in .p12 format) for web server (HTTPS) services. However, the administrator should check the root certificate and validity of the signature before importing, according to the organization's security procedures and requirements. After importing a certificate, the administrator should check if the certificate has been revoked and if so, the certificate must be replaced. When a browser verifies the signature and accesses the device, it will return a subject name which the administrator can use to confirm the connected device is authorized.</p> </div> <div style="background-color: #f0f0f0; padding: 10px; margin-top: 20px;"> <p> <b>Note</b></p> <p>The encryption algorithm of keys should be selected based on internationally recognized and proven security practices and recommendations.</p> <p>The lifetime of certificates generated for web server (HTTPS) services should be short and in accordance with the organization's security procedures and requirements.</p> </div>	Enabled / Disabled	Enabled
<b>HTTPS - TCP Port</b>	Specify the TCP port to use for HTTPS connections.	443, 1024 to 65535	443
<b>Telnet</b>	Enable or disable Telnet connections.	Enabled / Disabled	Disabled
<b>Telnet - TCP Port</b>	Specify the TCP port to use for Telnet connections.	23, 1024 to 65535	23
<b>SSH</b>	Enable or disable SSH connections.	Enabled / Disabled	Enabled
<b>SSH - TCP Port</b>	Specify the TCP port to use for SSH connections.	22, 1024 to 65535	22
<b>SNMP</b>	Enable or disable SNMP connections.	Enabled / Disabled	Disabled
<b>SNMP - UDP Port</b>	Specify the UDP port to use for SNMP connections.	161, 1024 - 65535	161

UI Setting	Description	Valid Range	Default Value
<b>MOXA Service</b>	Enable or disable Moxa Service connectivity. <div style="border: 1px solid #ccc; background-color: #f9f9f9; padding: 10px; margin-top: 10px;"> <p> <b>Note</b> Moxa Service is only used for Moxa network management software, and is only available for user accounts with admin privileges.</p> </div>	Enabled / Disabled	Enabled
<b>Moxa Service (Encrypted) - TCP Port</b>	Shows the TCP port used for Moxa Service. This setting cannot be changed.	N/A	443
<b>Moxa Service (Encrypted) - UDP Port</b>	Shows the UDP port used for Moxa Service. This setting cannot be changed.	N/A	40404
<b>Maximum Number of Login Sessions for HTTP+HTTPS</b>	Specify the maximum combined number of users that can be logged in using HTTP and HTTPS.	1 to 10	5
<b>Maximum Number of Login Sessions for Telnet+SSH</b>	Specify the maximum combined number of users that can be logged in using Telnet and SSH.	1 to 5	1

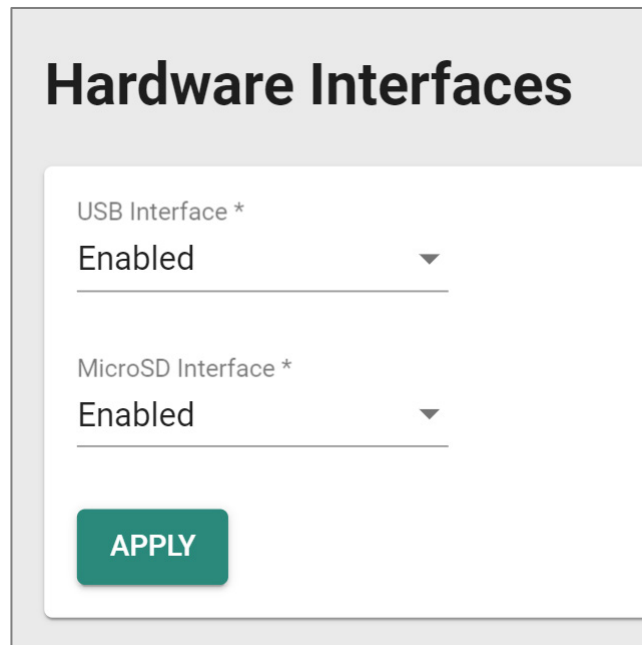
## Hardware Interfaces

### Menu Path: System > Management Interface > Hardware Interfaces

This page lets you enable or disable the USB interface on the device for use with an ABC-02 backup configurator tool.

Click **APPLY** to save your changes.

## Hardware Interfaces Settings



**Hardware Interfaces**

USB Interface \*  
Enabled

MicroSD Interface \*  
Enabled

**APPLY**

UI Setting	Description	Valid Range	Default Value
<b>USB Interface</b>	Enable or disable the USB interface on the device.	Enabled / Disabled	Enabled
<b>MicroSD Interface</b>	Enable or disable the microSD interface on the device.	Enabled / Disabled	Enabled

## Configuring Simple Network Management Protocol

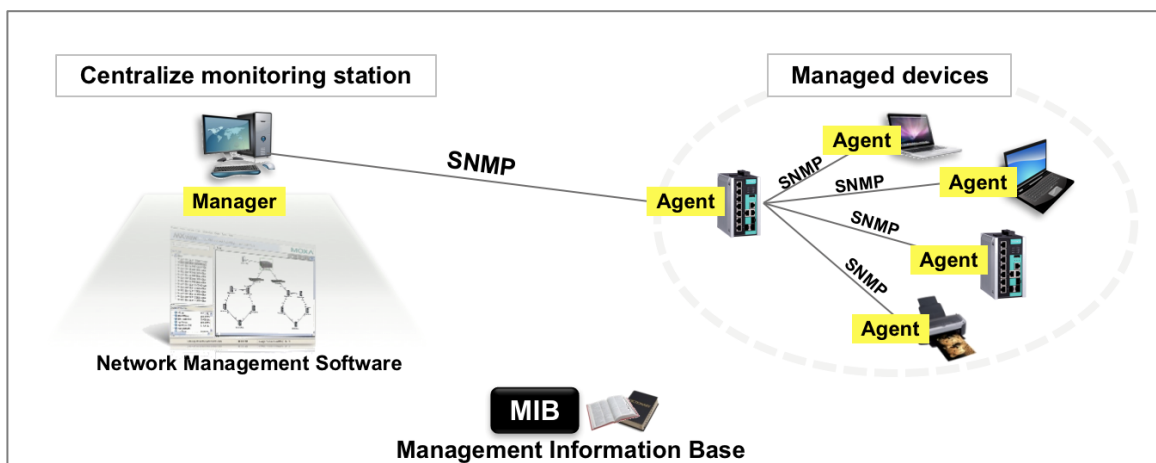
Simple Network Management Protocol (SNMP) be used to manage and monitor network devices.

It is an application-layer protocol that allows administrators to manage network performance, diagnose network problems, and gather information about network devices such as routers, switches, servers, printers, and other network equipment. SNMP works by using agents installed on network devices, which provide information to a central management system known as an SNMP manager. The manager sends requests to the agent to retrieve information about the device, such as CPU utilization, memory usage, network traffic, and other metrics.

## About SNMP

An SNMP deployment consists of Managers, Agents, and Management Information Bases (MIBs).

- **Management Information Base (MIB):** A database of information about network devices and their performance metrics. The MIB is organized hierarchically and uses a tree-like structure.
- **SNMP Manager:** The central management system that monitors and manages network devices. It sends requests to the SNMP agents to gather information and configure network devices.
- **SNMP Agent:** A software module installed on network devices that provides information about the device to the SNMP manager. The agent responds to requests from the manager and sends notifications to the manager when certain events occur, such as a device failure.



SNMP agents expose management data on the managed systems as variables. The protocol also permits active management tasks, such as configuration changes, through remote modification of these variables. The variables accessible via SNMP are organized in hierarchies. SNMP itself does not define which variables a managed system should offer. Rather, SNMP uses an extensible design that allows applications to define their own hierarchies. These hierarchies are described as a management information base (MIB). MIBs describe the structure of the management data of a device subsystem; they use a hierarchical namespace containing object identifiers (OID). Each OID identifies a variable that can be read or set via SNMP.



## Creating an SNMP Account


You must configure an SNMP account on each of your devices to manage them.

Some account settings are contingent on SNMP account settings. Protocol versions earlier than v3 do not support authentication or encryption, and require shared community keys. Go to **System > Management Interface > SNMP**, click **General**, and choose an SNMP Version. For insecure versions, also specify community strings.

### **Note**

SNMP versions earlier than v3 do not support authentication or encryption, and provide no security. It is strongly recommended to choose V3 Only unless compatibility absolutely requires earlier versions and security risks have been thoroughly evaluated.



To configure SNMP accounts:

1. Sign in to the device using administrator credentials.
2. Go to **System > Management Interface > SNMP**, and then click **SNMP Account**.
3. Click  **[Add]**.



The Create an SNMP Account screen appears.

4. Specify all of the following, and then click **Create**:

Option	Value
<b>Username</b>	Specify a username for the account with up to 32 characters
<b>Authority</b>	Choose from: <ul style="list-style-type: none"><li>• <b>Read/Write</b></li><li>• <b>Read</b></li></ul>

Option	Value
<b>Authentication Type</b>	Choose from: <ul style="list-style-type: none"> <li>• <b>None</b></li> <li>• <b>MD5</b></li> <li>• <b>SHA</b></li> <li>• <b>SHA-256</b></li> <li>• <b>SHA-512</b></li> </ul> <div style="border: 1px solid #ccc; background-color: #f0f0f0; padding: 5px; margin-top: 10px;"> <p> <b>Note</b> Authentication requires SNMP v3.</p> </div>
<b>Authentication Password</b>	If an authentication type has been specified, specify a password for the account between 8 and 64 characters long.
<b>Encryption Key</b>	<ul style="list-style-type: none"> <li>• <b>Disabled</b></li> <li>• <b>DES</b></li> <li>• <b>AES</b></li> </ul> <div style="border: 1px solid #ccc; background-color: #f0f0f0; padding: 5px; margin-top: 10px;"> <p> <b>Note</b> Encryption requires SNMP v3.</p> </div>
<b>Encryption Key</b>	If an encryption method has been chosen, specify an Encryption Key between 8 and 64 characters long.

The account appears in the **SNMP Account** table.

You can Edit or Delete from the list by clicking the corresponding  **[Edit]** or  **[Delete]**.

## SNMP

**Menu Path: System > Management Interface > SNMP**

This page lets you configure SNMP settings for your device.

This page includes these tabs:

- General

- SNMP Account

## SNMP - General

**Menu Path:** System > Management Interface > SNMP - General

This page lets you specify the SNMP versions used to manage your device.

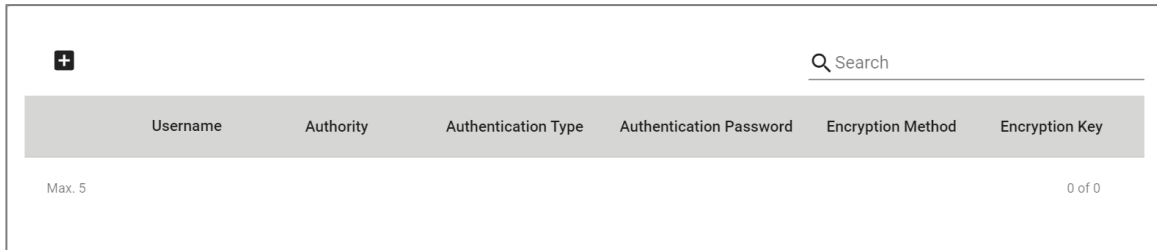
UI Setting	Description	Valid Range	Default Value
<b>SNMP Version</b>	Specify the SNMP protocol version used to manage your device. <ul style="list-style-type: none"> <li>• <b>V1, V2c, V3:</b> Enable SNMP V1, V2c, and V3.</li> <li>• <b>V1, V2c:</b> Enable SNMP V1 and V2c only.</li> <li>• <b>V3 only:</b> Enable SNMP V3 only.</li> </ul>	V1, V2c, V3 / V1, V2c / V3 only	V1, V2C / V3
<b>Read Community</b>	Specify a string name for the SNMP Read Community.	4 to 32 characters	public
<b>Read/Write Community</b>	Specify a string name for the SNMP Read/Write Community.	4 to 32 characters	private

## SNMP Account

### Menu Path: System > Management Interface > SNMP - SNMP Account

This page lets you configure the SNMP management accounts for the device. SNMP management accounts are provided for Admin and User-level authority.

## SNMP Account List



Username	Authority	Authentication Type	Authentication Password	Encryption Method	Encryption Key
Max. 5					
0 of 0					

UI Setting	Description
<b>Username</b>	Shows the username of the SNMP account.
<b>Authority</b>	Shows the authority level of the management account.
<b>Authentication Type</b>	Shows the authentication type used for the account.
<b>Authentication Password</b>	Shows ***** if there is an authentication password for the account.
<b>Encryption Method</b>	Shows the encryption method used for the account.
<b>Encryption Key</b>	Shows ***** if there is an encryption key for the account.

## Creating an SNMP Account

### Menu Path: System > Management Interface > SNMP - SNMP Account

Clicking the **Add (+)** icon on the **System > Management Interface > SNMP - SNMP Account** page will open this dialog box. This dialog lets you create an SNMP account.

Click **CREATE** to save your changes and add the new account.

## Create an SNMP Account

Username \*

Minimum 4 characters 0 / 32

Authority \*

Read/Write ▼

Authentication Type \*

SHA-256 ▼

Authentication Password \*



Minimum 8 characters 0 / 64

Encryption Method \*

AES ▼

Encryption Key \*



Minimum 8 characters 0 / 64

CANCEL

CREATE

UI Setting	Description	Valid Range	Default Value
<b>Username</b>	Specify a username for the SNMP account.	1 to 32 characters <ul style="list-style-type: none"> <li>Valid characters: a-z, A-Z, 0-9</li> <li>Valid special characters: . _ -</li> </ul>	N/A
<b>Authority</b>	Specify the authority level of the management account. <ul style="list-style-type: none"> <li><b>Read/Write:</b> Can read and write configuration settings</li> <li><b>Read:</b> Can only read configuration settings</li> </ul>	Read/Write / Read	Read/Write
<b>Authentication Type</b>	Specify the authentication type to use for the account.	None / MD5 / SHA / SHA-256 / SHA-512	N/A
<b>Authentication Password</b> <b>(If Authentication Type is not None)</b>	Specify the authentication password for the account.	8 to 64 characters <ul style="list-style-type: none"> <li>Valid characters: a-z, A-Z, 0-9</li> <li>Valid special characters: . , - _ + =   : ; @ ! ~ # % ^ * ( ) [ ] { }</li> </ul>	N/A

UI Setting	Description	Valid Range	Default Value
<b>Encryption Method (If Authentication Type is not None)</b>	Specify the encryption method to use for the account.	Disabled / DES / AES	Disabled
<b>Encryption Key (If Encryption Method is not Disabled)</b>	Specify the encryption key for the account.	8 to 64 characters <ul style="list-style-type: none"> <li>Valid characters: a-z, A-Z, 0-9</li> <li>Valid special characters: . , - _ + =   : ; @ ! ~ # % ^ * ( ) [ ] { }</li> </ul>	N/A

## Editing an SNMP Account

### Menu Path: System > Management Interface > SNMP - SNMP Account

Clicking the **Edit** (✎) icon for an account on the **System > Management Interface > SNMP - SNMP Account** page will open this dialog box. This dialog lets you edit an existing account.

Click **APPLY** to save your changes.

Click **CHANGE PASSWORD** to change the authentication password for the account.

Click **CHANGE ENCRYPTION KEY** to change the encryption key for the account.

## Edit This SNMP Account

Username \*

maintainer

Minimum 4 characters 10 / 32

Authority \*

Read/Write

Authentication Type \*

SHA-256

CHANGE PASSWORD



Encryption Method \*

AES

CHANGE ENCRYPTION KEY


CANCEL

APPLY

UI Setting	Description	Valid Range	Default Value
<b>Username</b>	Specify a username for the SNMP account.	1 to 32 characters <ul style="list-style-type: none"> <li>Valid characters: a-z, A-Z, 0-9</li> <li>Valid special characters: . _ -</li> </ul>	N/A
<b>Authority</b>	Select the authority level of the management account. <ul style="list-style-type: none"> <li><b>Read/Write:</b> Can read and write configuration settings</li> <li><b>Read:</b> Can only read configuration settings</li> </ul>	Read/Write / Read	Read/Write
<b>Authentication Type</b>	Select the authentication type to use for the account.	None / MD5 / SHA / SHA-256 / SHA-512	N/A
<b>Encryption Method (If Authentication Type is not None)</b>	Select the encryption method to use for the account.	Disabled / DES / AES	Disabled

## Deleting an SNMP Account

**Menu Path:** [System](#) > [Management Interface](#) > [SNMP - SNMP Account](#)

You can delete an account by clicking the **Delete** (  ) icon next to the account.

## Time

**Menu Path:** [System](#) > [Time](#)

This page lets you configure the time related settings.

This page includes these tabs:

- System Time
- NTP Server
- Time Synchronization

## About System Time

Correct system time is required for automatic warning emails to include a time and date stamp.

### Note

Make sure to update the Current Time and Current Date after the switch has been powered off for three days or more. This is particularly important when no NTP server or Internet connection are available.

This section describes how to configure the **System Time**, **NTP Server**, and **Time Synchronization** settings for the switch. The switch has a time calibration function based on information from an NTP server or a user-specified time and date, allowing functions such as automatic warning emails to include a time and date stamp.

## Configuring System Time

To configure System Time, do the following:

1. Sign in to the device using administrator credentials.
2. Go to **System** > **Time** > **System Time**, and then click on the **Time** tab.
3. Set **Clock Source** to **Enabled**.



4. Configure the **Date**, **Time**, and **Time Zone**. Specify **Daylight Savings** details if appropriate for your region.
5. Click **Apply** to save your settings.

## System Time

**Menu Path:** [System](#) > [Time](#) > [System Time](#)

This page lets you configure the system time.

This page includes these tabs:

- Time
- NTP Authentication

## System Time - Time

**Menu Path:** [System](#) > [Time](#) > [System Time - Time](#)

This page lets you configure your device's system time.

### System Time

Time
NTP Authentication

Current Time  
2024-07-30 02:10:43 UTC+00:00

---

Clock Source \*  
Local

Date \*  
2024-07-30

Time \*  
上午 02:10

Time Zone \*  
UTC+00:00

**Daylight Saving**  
Daylight Saving \*  
Enabled


Offset  
01:00

**Start**  
Month \* Week \* Day \* Hour \* Minute \*  
Mar last Sun 01 00

**End**  
Month \* Week \* Day \* Hour \* Minute \*  
Oct last Sun 01 00

APPLY
SYNC FROM BROWSER

UI Setting	Description	Valid Range	Default Value
<b>Current Time</b>	Show the current time according to your local default settings.	N/A	N/A
<b>Clock Source</b>	Specify whether to set the time manually (Local), from an SNTP server, from an NTP server, or from a PTP master.	Local / SNTP / NTP / PTP	Local
<b>Date</b> <b>(If Clock Source is Local)</b>	Select the current date from the calendar.	Calendar	Local Date
<b>Time</b> <b>(If Clock Source is Local)</b>	Specify the current time. You can manually input the time, or you can click <b>SYNC FROM BROWSER</b> to set the time based on the time used by your web browser.	Timestamp	N/A

UI Setting	Description	Valid Range	Default Value
<b>Time Zone</b> (If Clock Source is Local)	Specify the time zone used for the device.	Drop-down list of time zones	UTC+00:00
<b>1st Time Server: IP Address/Domain Name</b> (If Clock Source is SNTP or NTP)	Specify the IP or domain address of the 1st SNTP/NTP server to use (e.g., 192.168.1.1, <a href="http://time.stdtime.gov.tw">time.stdtime.gov.tw</a> , or <a href="http://time.nist.gov">time.nist.gov</a> ).	Valid IP address or domain name	<a href="http://time.nist.gov">time.nist.gov</a>
<b>2nd Time Server: IP Address/Domain Name</b> (If Clock Source is SNTP or NTP)	Specify the IP or domain address of the 2nd SNTP/NTP server to use if the first SNTP/NTP server fails to connect.	Valid IP address or domain name	N/A
<b>Query Interval</b> (If Clock Source is SNTP)	Specify the query interval time.	Drop-down list of intervals	9 (512 sec.)
<b>Authentication</b> (If Clock Source is NTP)	Select an NTP authentication key to use, or disable authentication for the time server.  <div style="background-color: #f0f0f0; padding: 5px; margin-top: 10px;"> <p> <b>Note</b></p> <p>To use authentication, you need to create an NTP authentication entry first. Refer to <a href="#">NTP Authentication</a> for more information.</p> </div>	Disabled / Drop-down list of NTP key IDs	Disabled

## Daylight Saving

UI Setting	Description	Valid Range	Default Value
<b>Daylight Saving</b>	Enable or disable use of daylight saving time adjustment.	Enabled / Disabled	Disabled
<b>Offset</b>	Specify the number of hours and minutes to add during the daylight saving time period.	01:00	N/A

UI Setting	Description	Valid Range	Default Value
<b>Start</b> <b>Month/Week/Day/Hour/Minute</b>	Specify the start time for the daylight seaving period.	Month: Drop-down list of months  Week: 1st / 2nd / 3rd / 4th / last  Day: Drop-down list of days of the week  Hour: Drop-down list of hours  Minute: Drop-down list of minutes	Mar/last/Sun/01/00
<b>End</b> <b>Month/Week/Day/Hour/Minute</b>	Specify the end time of the daylight saving period.	Month: Drop-down list of months  Week: 1st / 2nd / 3rd / 4th / last  Day: Drop-down list of days of the week  Hour: Drop-down list of hours  Minute: Drop-down list of minutes	Oct/last/Sun/01/00

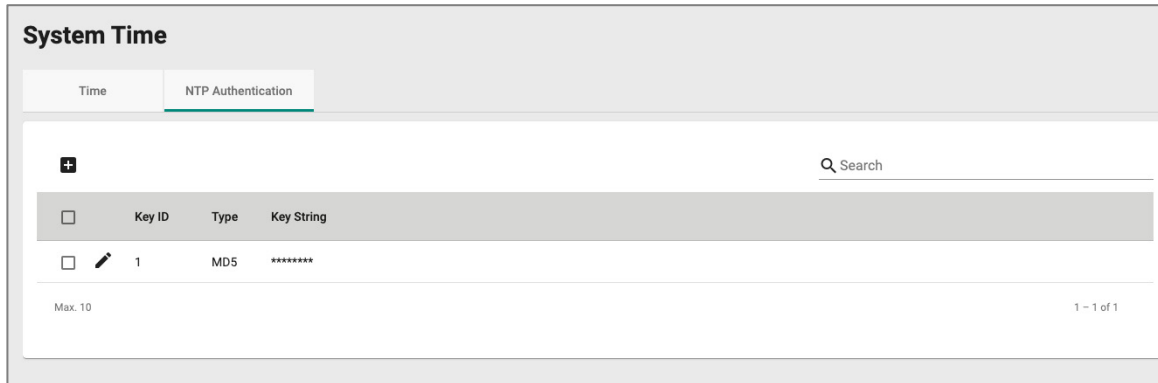
## NTP Authentication

### Menu Path: [System](#) > [Time](#) > [System Time - NTP Authentication](#)

This page lets you configure NTP authentication for when the device is acting as an NTP client. This helps ensure that received NTP responses are from the NTP server and have not been modified in transit.

## 🔒 Limitations

You can create up to 10 NTP authentication entries.



UI Setting	Description
<b>Key ID</b>	Shows the key ID for NTP authentication.
<b>Type</b>	Shows the authentication type.
<b>Key String</b>	Shows the password used for authentication.

## Creating an NTP Authentication Entry

### Menu Path: System > Time > System Time - NTP Authentication

Clicking the **Add (+)** icon on the **System > Time > System Time - NTP Authentication** page will open this dialog box. This dialog lets you create an NTP authentication entry.

Click **CREATE** to save your changes and add the new account.

**Create Entry**

Key ID \*  
1 - 65535

Type \*  
MD5

Key String \* 0 / 32

CANCEL CREATE

UI Setting	Description	Valid Range	Default Value
<b>Key ID</b>	Specify the Key ID to use for NTP authentication.	1 to 65535	N/A
<b>Type</b>	Specify the authentication type.	MD5	MD5
<b>Key String</b>	Specify the password to use for the authentication key.	0 to 32 characters	N/A

## About NTP Servers

Network Time Protocol (NTP) is used to synchronize the clocks of computers and other devices on a network, and is widely used on the Internet and in local networks to ensure accurate timekeeping. NTP operates by exchanging time information between servers and clients.

### NTP Servers In Depth

Typically, there are several hierarchical strata of NTP servers.

- **Stratum 1 servers** are directly connected to highly accurate time sources, such as atomic clocks or GPS receivers.
- **Stratum 2 servers** synchronize their time with Stratum 1 servers.
- **Client devices** synchronize their clocks with NTP servers, which helps maintain accurate time across the network.

You can configure your device to act as an NTP client to sync the system time with a specified NTP server.

You can also configure your device to act as an NTP server to provide time sync service to end devices on the network. When enabling the NTP server function, the device will answer the NTP queries sent from NTP client and provide the device's time to the client.

## NTP Server

**Menu Path:** System > Time > NTP Server

This page lets you configure your device to act as an NTP server.

UI Setting	Description	Valid Range	Default Value
<b>NTP Server</b>	Enable or disable the NTP server.	Enabled / Disabled	Disabled
<b>Client Authentication</b>	Enable or disable NTP client authentication.	Enabled / Disabled	Disabled

## About Time Synchronization

Time synchronization synchronizes the clocks of different devices to the same time. Precision Time Protocol (PTP) is a Time Synchronization protocol designed to synchronize clocks through Ethernet networks. The accuracy for IEEE 1588 PTP v2 can be measured in microseconds or nanoseconds.

There are three profiles provided for this feature:

- IEEE 1588 Default 2008
- IEC 61850-9-3-2016

- IEEE C37.238-2017

## Enable Time Synchronization and configuring relative parameters on the switch

Configuring Time Synchronization on the switch and selecting profile suites based on your application requirements and configuring the relative parameters.

1. Click **General**.
2. **Enable Time Synchronization**.
3. Select a Profile from the list: **IEEE 1588 Default 2008**, **IEC 61850-9-3-2016**, or **IEEE C37.238-2017**. Parameters such as Delay Mechanism will be fixed to Peer-to-Peer and Transport Mode will be fixed to **3 Ethernet** if IEC 61850-9-3-2016 or IEEE C37.238-2017 is selected.
4. Select a Clock Type from the list: **Boundary Clock** or **Transparent Clock**.
5. Specify Priority 1 and Priority 2 for Grandmaster election.
6. Specify a Domain Number for the device to join the time synchronization domain. Only one domain is allowed to be specified for each device.
7. Select a Clock Mode from the list: **One Step** will not use follow-up packets, and **Two Step** will use follow-up packets.
8. Specify the Accuracy Alert threshold. When the time offset exceeds the threshold, an event notification will be sent.
9. Specify the Maximum Steps Removed: Time synchronization packets will be dropped when the maximum number of steps has been reached, and the Grandmaster will then be re-elected.
10. Click **APPLY** to save the configuration changes.
11. Click **Port Settings** to configure the time synchronization parameters by port.
12. Scroll down the page and click edit for each port.
13. Enable **Time Synchronization** by port. For profiles **IEC 61850-9-3-2016** and **IEEE C37.238-2017** in the **General** tab, the configurations for **Announce Interval**, **Announce Receipt Timeout**, and **Sync Interval** are fixed. For the **IEEE 1588 Default 2008** profile, the parameters can be selected or specified



within a range. Copy the configurations to the ports the user expects to share the same settings with from the list and click **APPLY** to save the configurations.

## Time Synchronization

### Menu Path: [System](#) > [Time](#) > [Time Synchronization](#)

This page lets you enable the time synchronization feature and view its status.

This page includes these tabs:

- General
- Port Settings
- Status
- Port Status

#### **Note**

This feature is only available on RKS Series devices.

## Time Synchronization - General

### Menu Path: [System](#) > [Time](#) > [Time Synchronization - General](#)

This page lets you select and configure a profile for time synchronization.

# Time Synchronization

General	Port Settings	Status	Port Status
Time Synchronization *			
Disabled ▼			
Profile *			
IEEE 1588 Default-2008 ▼			
Clock Type *	Delay Mechanism *	Transport Mode *	
Boundary Clock ▼	End-to-End ▼	IEEE 802.3 Ethernet ▼	
Priority 1 *	Priority 2 *		
128	128		
0 - 255	0 - 255		
Domain Number *	Clock Mode *		
0	Two-step ▼		
0 - 255			
Accuracy Alert *	Maximum Steps Removed *		
1000	255		
50 - 250000000	2 - 255		
	ns		
<b>APPLY</b>			

UI Setting	Description	Valid Range	Default Value
<b>Time Synchronization</b>	Enable or disable time synchronization.	Enabled / Disabled	Disabled
<b>Profile</b>	Specify the time synchronization profile to use.	IEEE 1588 Default-2008 / IEC 61850-9-3-2016 / IEEE C37.238-2017	IEEE 1588 Default-200
<b>Clock Type</b>	Select the clock type to use.	Boundary Clock / Transparent Clock	Boundary Clock

UI Setting	Description	Valid Range	Default Value
<b>Delay Mechanism</b> (If Profile is IEEE 1588 Default-2008)	Select the delay mechanism to use.  <div style="background-color: #f0f0f0; padding: 5px;"> <p><b>Note</b></p> <p>For <b>IEC 61850-9-3-2016</b> and <b>IEEE C37.238-2017</b> profiles, <b>Delay Mechanism</b> is fixed to <b>Peer-to-Peer</b>.</p> </div>	End-to-End / Peer-to-Peer	End-to-End
<b>Transport Mode</b> (If Profile is IEEE 1588 Default-2008)	Select the transport mode to use.  <div style="background-color: #f0f0f0; padding: 5px;"> <p><b>Note</b></p> <p>For <b>IEC 61850-9-3-2016</b> and <b>IEEE C37.238-2017</b> profiles, <b>Transport Mode</b> is fixed to <b>802.3 Ethernet</b>.</p> </div>	802.3 Ethernet / UDP IPv4	802.3 Ethernet
<b>Priority 1</b> (If Clock Type is Boundary Clock)	Set the priority 1 value.	0 to 255	128
<b>Priority 2</b> (If Clock Type is Boundary Clock)	Set the priority 2 value.	0 to 255	128
<b>Domain Number</b>	Set domain number value.	0 to 255	0
<b>Clock Mode</b>	Select the clock mode to use.	One Step / Two Step	Two Step
<b>Accuracy Alert</b>	Set the accuracy alert threshold in nanoseconds. When the offset is under this threshold, the synchronization status will change from syncing to locked.	50 to 250000000	1000
<b>Maximum Steps Removed</b> (If Clock Type is Boundary Clock)	Specify the maximum number of steps that can be removed.	2 to 255	255
<b>Grandmaster ID</b> (If Profile is IEEE C37.238-2017 and Clock Type is Boundary Clock)	Specify the ID to use if this device becomes the grandmaster clock.	0 to 65535	255

UI Setting	Description	Valid Range	Default Value
<b>BMCA</b> <b>(If Clock Type is Transparent Clock)</b>	Enable or disable use of the Best Master Clock Algorithm (BMCA) when using transparent clock.	Enabled / Disabled	Enabled

## Time Synchronization - Port Settings

### Menu Path: System > Time > Time Synchronization - Port Settings

This page lets you enable time synchronization and configure related parameters for each port.

If the profile's **Clock Type** is **Boundary Clock**, this table will appear.

### Time Synchronization

General
Port Settings
Status
Port Status

IEEE 1588 Default-2008 Profile

	Port	Time Synchronization	Announce Interval	Announce Receipt Timeout (times) ↑	Sync Interval	Delay-Request Interval
	1/1	Disabled	1 (2 sec.)	3	0 (1 sec.)	0 (1 sec.)
	1/2	Disabled	1 (2 sec.)	3	0 (1 sec.)	0 (1 sec.)
	1/3	Disabled	1 (2 sec.)	3	0 (1 sec.)	0 (1 sec.)
	1/4	Disabled	1 (2 sec.)	3	0 (1 sec.)	0 (1 sec.)
	2/1	Disabled	1 (2 sec.)	3	0 (1 sec.)	0 (1 sec.)
	2/2	Disabled	1 (2 sec.)	3	0 (1 sec.)	0 (1 sec.)
	2/3	Disabled	1 (2 sec.)	3	0 (1 sec.)	0 (1 sec.)







UI Setting	Description
<b>Port</b>	Shows which port the entry describes.
<b>Time Synchronization</b>	Shows whether time synchronization is enabled for the port.

UI Setting	Description
<b>Announce Interval</b>	Shows the interval for sending PTP announce messages for the port.
<b>Announce Receipt Timeout</b>	Shows the announce message receipt timeout value for the port.
<b>Sync Interval</b>	Shows the synchronization message transmit interval for the port.
<b>Delay-Request Interval (If the profile's Delay Mechanism is End-to-End)</b>	Shows the interval for sending delay request messages for the port.
<b>Pdelay-Request Interval(If the profile's Delay Mechanism is Peer-to-Peer)</b>	Shows the interval for sending peer delay request messages for the port.

If the profile's **Clock Type** is **Transparent Clock**, this table will appear.

**IEEE 1588 Default-2008 Profile**

🔍 Search

	Port	Time Synchronization	Pdelay-Request Interval
	1/1	Disabled	0 (1 sec.)
	1/2	Disabled	0 (1 sec.)
	1/3	Disabled	0 (1 sec.)
	1/4	Disabled	0 (1 sec.)
	2/1	Disabled	0 (1 sec.)
	2/2	Disabled	0 (1 sec.)

UI Setting	Description
<b>Port</b>	Shows which port the entry describes.
<b>Time Synchronization</b>	Shows whether time synchronization is enabled for the port.

UI Setting	Description
<b>Pdelay-Request Interval(If the profile's Delay Mechanism is Peer-to-Peer)</b>	Shows the interval for sending peer delay request messages for the port.

## Time Synchronization - Edit Port Settings

### Menu Path: System > Time > Time Synchronization - Port Settings

Clicking the **Edit** (✎) icon for a port on the **System > Time > Time Synchronization - Port Settings** page will open this dialog box. This dialog lets you configure time synchronization settings for the port. Click **APPLY** to save your changes.

### Edit Port 1/1 Settings

Time Synchronization \*





Announce Interval \*       Announce Receipt Timeout \*   
2 - 10 times

Sync Interval \*

Delay-Request Interval \*

Copy configurations to ports  ⓘ

UI Setting	Description	Valid Range	Default Value
<b>Time Synchronization</b>	Enable or disable time synchronization for the port.	Enabled / Disabled	Disabled

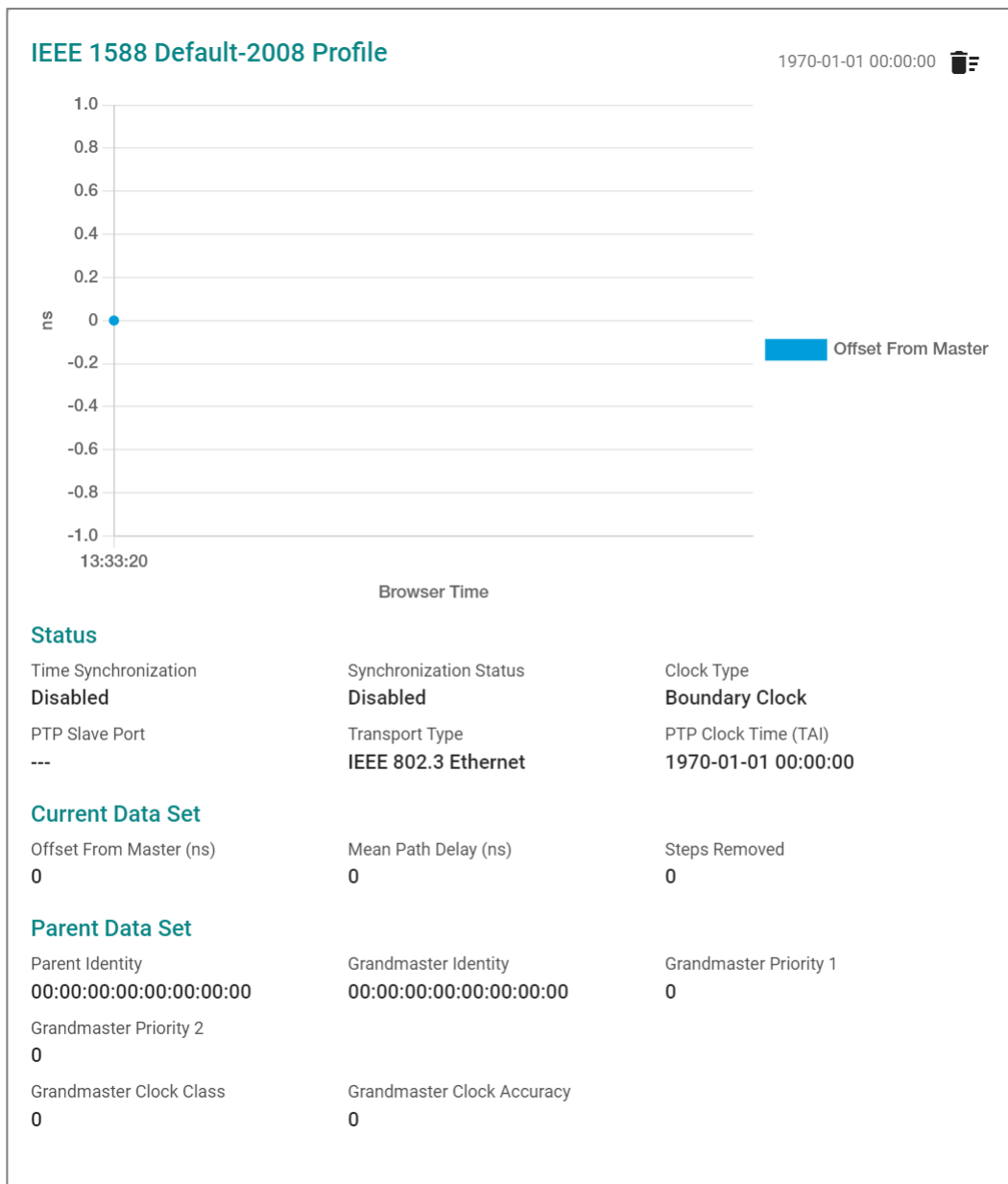
UI Setting	Description	Valid Range	Default Value
<b>Announce Interval</b>	Select the interval to send announce messages for the port.  <div style="background-color: #f0f0f0; padding: 5px;"> <p> <b>Note</b> For <b>IEC 61850-9-3-2016</b> and <b>IEEE C37.238-2017</b> profiles, <b>Announce Interval</b> is fixed to <b>0 (1 sec.)</b>.</p> </div>	0 (1 sec.) / 1 (2 sec.) / 2 (4 sec.) / 3 (8 sec.) / 4 (16 sec.)	1 (2 sec.)
<b>Announce Receipt Timeout</b>	Specify the number of timeouts allowed for announce receipts for the port.  <div style="background-color: #f0f0f0; padding: 5px;"> <p> <b>Note</b> For <b>IEC 61850-9-3-2016</b> and <b>IEEE C37.238-2017</b> profiles, <b>Announce Receipt Interval</b> is fixed to <b>3</b>.</p> </div>	2 to 10 (times)	3
<b>Sync Interval</b>	Select the synchronization interval for the port.  <div style="background-color: #f0f0f0; padding: 5px;"> <p> <b>Note</b> For <b>IEC 61850-9-3-2016</b> and <b>IEEE C37.238-2017</b> profiles, <b>Sync Interval</b> is fixed to <b>0 (1 sec.)</b>.</p> </div>	-3 (0.125 sec.) / -2 (0.25 sec.) / -1 (0.5 sec.) / 0 (1 sec.) / 1 (2 sec.) / 3 (4 sec.) / 4 (8 sec.) / 5 (32 sec.)	0 (1 sec.)
<b>Delay-Request Interval</b> <b>(If the profile's Delay Mechanism is End-to-End)</b>	Select the interval for sending delay-request messages for the port.	-3 (0.125 sec.) / -2 (0.25 sec.) / -1 (0.5 sec.) / 0 (1 sec.) / 1 (2 sec.) / 3 (4 sec.) / 4 (8 sec.) / 5 (32 sec.)	0 (1 sec.)
<b>Pdelay-Request Interval</b> <b>(If the profile's Delay Mechanism is Peer-to-Peer)</b>	Select the interval for sending peer delay-request messages for the port.  <div style="background-color: #f0f0f0; padding: 5px;"> <p> <b>Note</b> For <b>IEC 61850-9-3-2016</b> and <b>IEEE C37.238-2017</b> profiles, <b>Pdelay-Request Interval</b> is fixed to <b>0 (1 sec.)</b>.</p> </div>	-3 (0.125 sec.) / -2 (0.25 sec.) / -1 (0.5 sec.) / 0 (1 sec.) / 1 (2 sec.) / 3 (4 sec.) / 4 (8 sec.) / 5 (32 sec.)	0 (1 sec.)
<b>Copy configurations to ports</b>	Select the ports you want to copy this configuration to.	Drop-down list of ports	N/A

## Time Synchronization - Status

### Menu Path: System > Time > Time Synchronization - Status

This page lets you view the detailed time synchronization status of your device.

If the profile's **Clock Type** is **Boundary Clock**, this display will appear. The graph shows the offset from the master clock in nanoseconds over time.





## Status

UI Setting	Description
<b>Time Synchronization</b>	Shows whether time synchronization is enabled.
<b>Synchronization Status</b>	Shows the current synchronization status. <b>Disabled</b> means that the time synchronization feature is disabled.
<b>Clock Type</b>	Shows the clock type being used.
<b>PTP Slave Port</b>	Shows the port acting as a PTP slave.
<b>Transport Type</b>	Shows the transport type being used.
<b>PTP Clock Time (TAI)</b>	Shows the current PTP clock time.

## Current Data Set

UI Setting	Description
<b>Offset From Master (ns)</b>	Shows the current offset from the master clock in nanoseconds.
<b>Mean Path Delay (ns)</b>	Shows the mean path delay in nanoseconds.
<b>Steps Removed</b>	Shows the number of steps removed.

## Parent Data Set

UI Setting	Description
<b>Parent Identity</b>	Shows the clock ID of the parent identity.
<b>Grandmaster Identity</b>	Shows the clock ID of the grandmaster identity.
<b>Grandmaster Priority 1</b>	Shows the priority 1 value for the grandmaster clock.
<b>Grandmaster Priority 2</b>	Shows the priority 2 value for the grandmaster clock.

UI Setting	Description
<b>Grandmaster Clock Class</b>	Shows the class value for the grandmaster clock.
<b>Grandmaster Clock Accuracy</b>	Shows the accuracy value for the grandmaster clock.

If the profile's **Clock Type** is **Transparent Clock**, this display will appear.

<b>IEEE 1588 Default-2008 Profile</b>		1970-01-01 00:00:00
<b>Status</b>		
Time Synchronization	Synchronization Status	Clock Type
Disabled	Disabled	Transparent Clock
Transport Type		
UDP IPv4		

## Status

UI Setting	Description
<b>Time Synchronization</b>	Shows whether time synchronization is enabled.
<b>Synchronization Status</b>	Shows the current synchronization status. <b>Disabled</b> means that the time synchronization feature is disabled.
<b>Clock Type</b>	Shows the clock type being used.
<b>Transport Type</b>	Shows the transport type being used.

## Time Synchronization - Port Status

**Menu Path: System > Time > Time Synchronization - Port Status**

This page lets you view the time synchronization status of individual ports.

## Time Synchronization Port Status Table

Time Synchronization			
General	Port Settings	Status	Port Status
IEEE 1588 Default-2008 Profile			
C			
Port	Port State	Path Delay (ns)	
1/1	Disabled	0	
1/2	Disabled	0	
1/3	Disabled	0	
1/4	Disabled	0	
2/1	Disabled	0	
2/2	Disabled	0	
2/3	Disabled	0	
2/4	Disabled	0	

UI Setting	Description
<b>Port</b>	Shows the port the entry is for.
<b>Port State</b>	Shows the operating state of time synchronization for the port.
<b>Path Delay</b>	Shows the path delay in milliseconds for the port.

## Configuring NTP Server

Moxa devices can serve as network time protocol (NTP) servers to allow other devices to synchronize their clocks over the network.

NTP operates by exchanging time information between servers and clients.

Typically, there are several hierarchical strata of NTP servers. Stratum 1 servers are directly connected to highly accurate time sources, such as atomic clocks or GPS receivers. Stratum 2 servers synchronize their time with Stratum 1 servers, and so on. Client devices synchronize their clocks with NTP servers, which helps maintain accurate time across the network.

NTP is widely used on the internet and in local networks to ensure accurate timekeeping, and it has been a critical component of network infrastructure for decades.

Our switch can act as NTP client to sync the system time with the configured NTP server (Stratum 1). Our switch can also act as an NTP server (Stratum 2) to propagate the synchronized time to other clients on the network.

## Enabling NTP Server

1. Sign in to the device using administrator credentials.
2. Go to **System > Time > NTP Server**.
3. Set **NTP Server** to **Enabled**.
4. To Enable Client Authentication and create keys, do the following:
5. Set **Client Authentication** to **Enabled**.
6. Go to **System > Time > System Time > NTP Authentication**, and then click **Add**.

The **Create Entry** screen appears.

7. Key ID Type Key String Configure all of the following, and then click **Create**:

Option	Value
<b>Key ID</b>	Specify a number to identity the key
<b>Type</b>	<b>MD5</b>
<b>Key String</b>	Specify a key at least one character long.

# Port

## Menu Path: Port

This section lets you configure various port-specific functions for the switch.

This section includes these pages:

- Port Interface
- Link Aggregation
- PoE

## PoE - User Privileges

Privileges to settings are granted to the different authority levels as follows. Refer to [System > Account Management > User Accounts](#) for more information on user accounts.

Settings	Admin	Supervisor	User
<b>Port Interface</b>			
<b>Port Settings</b>	R/W	R/W	R
<b>Linkup Delay</b>	R/W	R/W	R
<b>Link Aggregation</b>	R/W	R/W	R
<b>PoE</b>	R/W	R/W	R

## Port Interface

### Menu Path: Port > Port Interface

This section lets you configure the port interface functions.

This section includes these pages:

- Port Settings
- Linkup Delay

## About Port Settings

Port Settings allows you to manage and configure the various parameters of your device's individual network ports. By letting you adjust settings such as speed, duplex, and flow control, it helps you optimize the performance of your network connections.

## Port Settings

**Menu Path: Port > Port Interface > Port Settings**

This page lets you configure the port settings.

This page includes these tabs:

- Settings
- Status

### Port Settings - Settings

**Menu Path: Port > Port Interface > Port Settings - Settings**

This page lets you configure basic port settings.

Port	Admin Status	Media Type	Description	Speed/Duplex	Flow Control	MDI/MDIX	Tracking ID
1/1	Enabled	SFP-1GLXLC-T		---	Disabled	---	---
1/2	Enabled	SFP-1GLXLC		---	Disabled	---	---
1/3	Enabled	1000FX/miniGBIC		---	Disabled	---	---
1/4	Enabled	1000FX/miniGBIC		---	Disabled	---	---
2/1	Enabled	100TX,RJ45		Auto	Disabled	Auto	---

UI Setting	Description
<b>Port</b>	Shows which port the entry describes.
<b>Admin Status</b>	Shows whether admin status is enabled for data transmission through the port.

UI Setting	Description
<b>Media Type</b>	Shows the detected media type for the port.
<b>Description</b>	Shows the description used to help identify the port.
<b>Speed/Duplex</b>	Shows the port speed and duplex option selected for the port.
<b>Flow Control</b>	Shows whether flow control is enabled for the port.
<b>MDI/MDIX</b>	Shows the MDI/MDIX option used for the port.
<b>Tracking ID</b>	Shows the tracking ID for the port.

## Editing Port Settings

### Menu Path: Port > Port Interface > Port Settings - Settings

Clicking the **Edit** (✎) icon for the desired port on the **Port > Port Interface > Port Settings - Settings** page will open this dialog box. This dialog lets you configure the port settings parameters.

Click **APPLY** to save your changes.

**Edit Port 1/1 Settings**

Admin Status \*  
Enabled

Media Type  
SFP-1GLXLC-T

Description  
0 / 127

Speed/Duplex




Flow Control \*  
Disabled ⓘ

MDI/MDIX

Tracking ID

Copy configurations to ports

CANCEL APPLY

UI Setting	Description	Valid Range	Default Value
<b>Admin Status</b>	Enable or disable data transmission through the port.	Enabled / Disabled	Enabled
<b>Media Type</b>	Displays the detected media type for each port. This setting cannot be changed.	Detected media type	N/A
<b>Description</b>	Specify a description to help identify the port.	0 to 127 characters	N/A
<b>Speed/Duplex</b>	<p>Select the speed/duplex mode to use for the port.</p> <p>Select <b>Auto</b> to enable the port to negotiate the optimal speed using the IEEE 802.3u protocol with connected devices. The port and connected devices will determine the most suitable speed for the connection.</p> <p>Alternatively, choose a fixed speed and duplex option if the connected Ethernet device has trouble with auto-negotiation. This can be useful for connecting legacy devices without auto-negotiation support.</p> <div style="background-color: #f0f0f0; padding: 5px; margin-top: 10px;"> <p> <b>Note</b></p> <p>Speed/Duplex cannot be set for fiber ports.</p> </div>	Auto / 10M Half / 10M Full / 100M Half / 100M Full	Auto
<b>Flow Control</b>	<p>Enable or disable flow control for the port.</p> <div style="background-color: #f0f0f0; padding: 5px; margin-top: 10px;"> <p> <b>Note</b></p> <p>The switch and connected device will automatically determine the final result.</p> </div> <div style="background-color: #f0f0f0; padding: 5px; margin-top: 10px;"> <p> <b>Note</b></p> <p>Flow Control can be enabled, but it is only effective at full duplex.</p> <p>Back Pressure is automatically enabled, but it is only effective at half duplex.</p> </div>	Enabled / Disabled	Disabled



UI Setting	Description	Valid Range	Default Value
<b>MDI/MDIX</b>	<p>Select the MDI/MDIX mode to use for the port.</p> <p>Select <b>Auto</b> to allow the port to auto-detect the port type of the connected Ethernet device, and change the port type accordingly.</p> <p>Alternatively, manually select <b>MDI</b> or <b>MDIX</b> if the device has trouble auto-detecting the port type.</p> <div style="background-color: #f0f0f0; padding: 5px; margin-top: 10px;"> <p> <b>Note</b></p> <p>MDI/MDIX cannot be set for fiber ports.</p> </div>	Auto / MDI / MDIX	Auto
<b>Tracking ID</b>	<p>Select a tracking ID for the port. This setting is optional.</p>	List of tracking IDs	N/A
<b>Copy configurations to ports</b>	<p>Select the ports you want to copy this configuration to.</p> <div style="background-color: #f0f0f0; padding: 5px; margin-top: 10px;"> <p> <b>Note</b></p> <p>The copy configuration feature cannot be used with fiber ports.</p> </div>	Drop-down list of ports	N/A

## Port Settings - Status

**Menu Path: Port > Port Interface > Port Settings - Status**

This page lets you view the status and configuration of the device's ports.

Port Settings						
Settings		Status				
		<input type="text" value="Search"/>				
Port	Media Type	Link Status	Description	Flow Control	MDI/MDIX	Port State
1/1	1000TX,RJ45	Link Down		Disabled	Invalid	Blocking
1/2	1000TX,RJ45	1G, Full (Auto)		Disabled	MDI (Auto)	Forwarding
1/3	1000TX,RJ45	Link Down		Disabled	Invalid	Blocking
1/4	1000TX,RJ45	Link Down		Disabled	Invalid	Blocking

UI Setting	Description
<b>Admin Status</b>	Shows whether admin status is enabled for data transmission through the port.
<b>Media Type</b>	Shows the detected media type for the port.
<b>Link Status</b>	Shows the port's link status. <b>Link Down</b> will be shown If the link is down. Otherwise, the port's speed and duplex will be shown.
<b>Description</b>	Shows the description used to help identify the port.
<b>Flow Control</b>	Shows whether flow control is enabled for the port.
<b>MDI/MDIX</b>	Shows the MDI/MDIX option used for the port.
<b>Port State</b>	Shows whether the port status is blocking or forwarding.

## About Linkup Delay

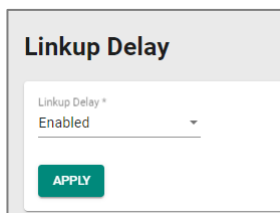
Linkup delay, also known as link flap prevention, is used to prevent a port alternating between link up and link down statuses, and is useful when a link connection is unstable. An unstable connection might be caused by situations such as a faulty cable, faulty fiber transceiver, duplex mismatch, etc. Linkup delay helps you mitigate the risk of an unstable network, particularly when the topology changes frequently.

## Linkup Delay

**Menu Path:** [Port](#) > [Port Interface](#) > [Linkup Delay](#)






This page lets you configure the linkup delay for device's ports.

### Linkup Delay Settings - All Ports



UI Setting	Description	Valid Range	Default Value
<b>Linkup Delay</b>	Enable or disable linkup delay for all ports.	Enabled / Disabled	Disabled


## Linkup Delay - Port List

	Port	Enable	Delay Time	Remaining Time
	1	Disabled	2	0
	2	Disabled	2	0
	3	Disabled	2	0
	4	Disabled	2	0
	5	Disabled	2	0

UI Setting	Description
<b>Enable</b>	Shows whether linkup delay is enabled or disabled for the port.
<b>Delay Time</b>	Shows the delay time in seconds for the port.
<b>Remaining Time</b>	Shows the remaining time in seconds for the port to alternate between link up and link down.

## Linkup Delay - Edit Port Settings

### Menu Path: [Port](#) > [Port Interface](#) > [Linkup Delay](#)

To configure linkup delay for a port, click the **Edit** () icon on the desired port on the **Port > Port Interface > Linkup Delay** page will open this dialog box. This dialog lets you configure the linkup delay parameters for the port.

Click **APPLY** to save your changes.

UI Setting	Description	Valid Range	Default Value
<b>Linkup Delay</b>	Enable or disable linkup delay for the port.	Enabled / Disabled	Disabled
<b>Delay Time</b>	Specify the delay time in seconds before the port alternates between link up and link down.	1 to 1000	2
<b>Copy configurations to ports</b>	Select the ports you want to copy this configuration to.	Drop-down list of ports	N/A

## About Link Aggregation

Link aggregation, also known as port channels or port trunking, helps balance, optimize, and facilitate a device's throughput. This method combines multiple network communication interfaces in parallel to maximize data throughput, increasing data communication efficiency for each port. In addition, it also acts as a useful method for network redundancy when a link fails. In general, link aggregation supports combining multiple physical switch ports into a single, bandwidth-efficient data communication route. This can improve network load sharing and increase network reliability.

### Static Trunk

For some networking applications, a situation can arise where traffic from multiple ports is required to be filtered through a single port. For example, if there are 30 UHD IP surveillance cameras deployed and connected in a ring, traffic can reach up to 1 Gbps, causing a surge in traffic that can increase network loading by up to 50%. Hence, the

uplink port needs to use static trunking to provide additional bandwidth and redundancy protection.

## LACP

Link Aggregation Control Protocol (LACP) is a protocol defined by IEEE 802.3ad that allows a network device to negotiate automatic bundling of several ports by sending LACP packets to the peer, a directly connected device that also uses LACP.

## Link Aggregation Algorithms

In link aggregation, three load-sharing hash algorithms can be used to optimize packet forwarding:

- **SMAC:** Source MAC (SMAC) uses the source MAC address for a packet to optimize packet forwarding to ensure that packets from the same source address follow the same path consistently to optimize connection stability and reduce the chance of out-of-order packet delivery.
- **DMAC:** Destination MAC (DMAC) uses the destination MAC address for a packet to optimize packet forwarding to ensure that packets being sent to the same destination address are consistently sent over the same link to optimize connection stability and traffic distribution.
- **SMAC + DMAC:** SMAC and DMAC can be used together for more complex hash algorithms, but tends to be used only when a network has few clients and servers.

## Link Aggregation Settings

### Menu Path: [Port](#) > [Link Aggregation](#)

This page lets you configure link aggregation groups for each port. A link aggregation group combines multiple physical ports into a single logical link.

## 🔒 Limitations

You can create up to 14 link aggregation groups.

## Link Aggregation List

<input type="checkbox"/>	Port Channel (Trunk)	Enable	Type	Algorithm	Configure Member	Active Member
<input type="checkbox"/>	1	Enabled	Manual	SMAC + DMAC	1, 2	2
<input type="checkbox"/>	2	Enabled	LACP	SMAC + DMAC	3, 4	

Max. 10

UI Setting	Description
<b>Port Channel (Trunk)</b>	Shows the Port Channel (Trunk) number of the link aggregation group.
<b>Enable</b>	Shows whether the link aggregation group is enabled.
<b>Type</b>	Shows the method for configuring the link aggregation group.
<b>Algorithm (Only in Advanced Mode)</b>	Shows the load-sharing hash algorithms being used for the link aggregation group.
<b>Configure Member</b>	Shows the configured member ports in the link aggregation group.
<b>Active Member</b>	Shows the active member ports in the link aggregation group.

## Creating a Link Aggregation Group

### Menu Path: Port > Link Aggregation

Clicking the **Add** (🛠️) icon on the **Port > Link Aggregation** page will open this dialog box. This dialog lets you create a link aggregation group.

Click **CREATE** to save your changes and add the new link aggregation group.

### Create Link Aggregation

LA Group Status \*  
Enabled ▼

Type \*  
▼

Config Member Port \* ▼ i

Algorithm \*  
SMAC + DMAC ▼

CANCEL
CREATE

UI Setting	Description	Valid Range	Default Value
<b>LA Group Status</b>	Enable or disable the link aggregation group.	Enabled/ Disabled	Enabled
<b>Type</b>	<p>Select the method to use for configuring the link aggregation group.</p> <p><b>Manual:</b> This allows you to specify the ports to be included in the LA Group.</p> <p><b>LACP:</b> LACP protocol will be used to automatically negotiate link aggregation configuration between devices.</p>	Manual / LACP	N/A
<b>Config Member Port</b>	<p>Select the ports to add to the link aggregation group.</p> <div style="background-color: #f0f0f0; padding: 10px; margin-top: 10px;"> <p><b>Note</b></p> <p>A port cannot be assigned to multiple link aggregation groups. This is because each port can only be a member of a single link aggregation group at a time.</p> <p>A link aggregation group (Port-channel) cannot be created when selected ports are operating at different speeds.</p> </div>	Device ports	N/A
<b>Algorithm (Only in Advanced Mode)</b>	Select the load-sharing hash algorithms to be used for configuring link aggregation.	SMAC / DMAC / SMAC+DMAC	SMAC+DMAC

## Editing a Link Aggregation Group

### Menu Path: Port > Link Aggregation

Clicking the **Edit** (✎) icon on the **Port > Link Aggregation** page will open this dialog box. This dialog lets you edit Link Aggregation group settings.

Click **APPLY** to save your changes.







UI Setting	Description	Valid Range	Default Value
<b>LA Group Status</b>	Enable or disable the link aggregation group.	Enabled/ Disabled	Enabled
<b>Type</b>	Select the method to use for configuring the link aggregation group.  <b>Manual:</b> This allows you to specify the ports to be included in the LA Group. <b>LACP:</b> LACP protocol will be used to automatically negotiate link aggregation configuration between devices.	Manual / LACP	N/A
<b>Config Member Port</b>	Select the ports to add to the link aggregation group.  <b>Note</b> A port cannot be assigned to multiple link aggregation groups. This is because each port can only be a member of a single link aggregation group at a time.  A link aggregation group (Port-channel) cannot be created when selected ports are operating at different speeds.	Device ports	N/A



UI Setting	Description	Valid Range	Default Value
<b>Algorithm</b> (Only in Advanced Mode)	Select the load-sharing hash algorithms to be used for configuring link aggregation.	SMAC / DMAC / SMAC+DMAC	SMAC+DMAC

## Link Aggregation - Port Settings for LACP


This table lets you see the LACP settings for each port.

Port	Mode	Timeout (sec.)	Wait Time (sec.)	Port Channel (Trunk)
 1	Active	90	2	1
 2	Active	90	2	1
 3	Active	90	2	2
 4	Active	90	2	2
 5	Active	90	2	
 6	Active	90	2	

UI Setting	Description
<b>Port</b>	Shows which port the entry describes.
<b>Mode</b>	Shows the LACP mode for the port.
<b>Timeout (sec.)</b>	Shows the LACP inactivity timeout in seconds for the port.
<b>Wait Time (sec.)</b>	Shows the LACP wait time in seconds for the port.
<b>Port Channel (Trunk)</b>	Shows the link aggregation group (Port channel) number for the port.

## Editing Port Settings for LACP

### Menu Path: [Port](#) > [Link Aggregation](#)


Clicking the **Edit** () icon by a port on the **Port > Link Aggregation** page will open this dialog box. This dialog lets you edit the port settings for LACP parameters if your link aggregation type is set to LACP.

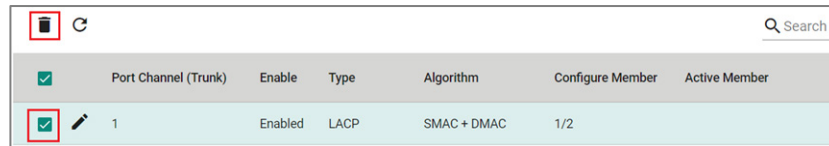
Click **APPLY** to save your changes.

UI Setting	Description	Valid Range	Default Value
<b>Port Channel (Trunk)</b>	Shows the link aggregation group (Port channel) number of the port. This setting cannot be changed.	Port Channel Number	N/A
<b>Mode</b>	<p>Select the LACP mode to decide how the ports establish LACP links.</p> <ul style="list-style-type: none"> <li>• <b>Active:</b> Ports will actively query link partners for LACP by sending LACP PDUs. If the partner is also LACP-enabled, the ports will establish an LACP link.</li> <li>• <b>Passive:</b> Ports can respond to LACP queries from active ports and passively establish LACP links. They will not initiate any LACP negotiation on their own.</li> </ul> <p>For LACP to establish a link, at least one port for the link must use active mode. If both ports are passive, no LACP PDUs will be sent, and no link will be established.</p>	Active / Passive	Active
<b>Timeout</b>	Specify the LACP inactivity timeout in seconds. This is the amount of time that must elapse without receiving any LACP PDUs before a link is considered to have failed.	3 / 90	90
<b>Wait Time</b>	Specify the LACP wait time in seconds. This is the amount of time that must elapse after a LACP link comes up before it is added to the link aggregation group.	0 to 10	2
<b>Copy configurations to ports</b>	Select the ports you want to copy this configuration to.	Drop-down list of ports	N/A

## Deleting a Link Aggregation Group (Port Channel)

### Menu Path: Port > Link Aggregation

You can delete a link aggregation group by using the checkboxes to select the entries you want to delete, then clicking the **Delete** (  ) icon.



<input checked="" type="checkbox"/>	Port Channel (Trunk)	Enable	Type	Algorithm	Configure Member	Active Member
<input checked="" type="checkbox"/>	1	Enabled	LACP	SMAC + DMAC	1/2	

## PoE

Power over Ethernet (PoE) provides power along with network connectivity to PoE network devices (PDs), allowing them to be powered and connected to the network using a single network cable. This can greatly simplify installation, maintenance, and troubleshooting of these PoE devices, especially when they are installed in areas that are difficult to reach or do not have power outlets nearby.

PoE is frequently used with a variety of devices:

- Surveillance cameras
- Security I/O sensors
- Industrial wireless access points
- Emergency IP phones

Moxa devices also support the high-power PoE+ standard and advanced PoE management functions such as PD failure check, legacy PD detection, and auto power cutting. These work together to provide critical security systems with a convenient and reliable Ethernet network that is easier to manage.


## PoE Settings

### Menu Path: Port > PoE

This page lets you configure your device's Power over Ethernet (PoE) settings. PoE allows your Moxa device to power other connected PoE Ethernet devices—such as security cameras, wireless access points, and sensors—through the Ethernet cable.

This page includes these tabs:

- General
- PD Failure Check
- Scheduling
- Status

 **Note**

PoE functionality is only available on specific PoE-enabled Moxa device models. Connected PoE devices must support the IEEE 802.3af/at standard in order to use this feature.

 **Limitations**

Only PoE Type 1 (802.3af) and Type 2 (802.3at) are supported, with a maximum of Class 4 and 30 W per port.

## PoE - General

**Menu Path:** [Port](#) > [PoE - General](#)

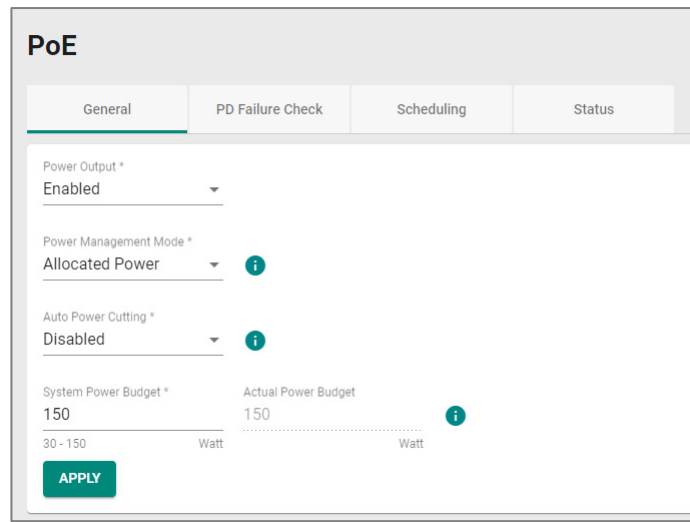
This page lets you enable PoE power output and configure system-level PoE settings.

**Note**

When the PoE function is activated, PoE-enabled ports should only be connected to standard/legacy powered devices.

If there is a need to connect non-powered devices to a PoE-enabled port, it is recommended to disable PoE for the port to prevent unnecessary PoE detection behavior.

## PoE Settings



UI Setting	Description	Valid Range	Default Value
<b>Power Output</b>	Enable or disable PoE.	Enabled / Disabled	Enabled
<b>Power Management Mode</b>	Specify whether the power budget for all ports should be calculated. <ul style="list-style-type: none"><li><b>Allocated Power</b>: This calculates the power budget based on the Power Allocation settings of all ports. For more information on per-port power allocation, refer to <a href="#">PoE - Edit Port Settings</a>.</li><li><b>Consumed Power</b>: This calculates the power budget based on actual power consumed by all ports.</li></ul>	Allocated Power / Consumed Power	Consumed Power Allocated Power
<b>Auto Power Cutting</b>	Enable or disable auto power cutting, which allows PoE to be disabled for ports when total power consumption exceeds the system power budget threshold. Ports with lower priority will be disabled before ports with higher priority.	Enabled / Disabled	Disabled









UI Setting	Description	Valid Range	Default Value
<b>System Power Budget</b>	Specify the "total measured power" limit in watts to use for all PoE ports combined.	<i>(Depends on your device model)</i>	<i>(Depends on your device model)</i>
<b>Actual Power Budget</b>	Show the system power budget in watts. This setting cannot be changed.	N/A	150

## PoE - Port List

### Note

For the TN-4500B PSE chip:

- Standard PD: Resistance: 17 ~ 29 kΩ and Capacitance: 0~1 μF
- Legacy PD: Resistance: 0.86 ~17 kΩ or Resistance: 29~100 kΩ or Capacitance: 1 ~ 12 μF

		Q Search				
	Port	PoE Supported	Power Output	Output Mode	Power Allocation	Priority
	1	Yes	Enabled	Auto	0	Low
	2	Yes	Enabled	Auto	0	Low
	3	Yes	Enabled	Auto	0	Low
	4	Yes	Enabled	Auto	0	Low
	5	Yes	Enabled	Auto	0	Low
	6	Yes	Enabled	Auto	0	Low
	7	Yes	Enabled	Auto	0	Low
	8	Yes	Enabled	Auto	0	Low

1 - 24 of 24

UI Setting	Description
<b>Port</b>	Shows which port the entry describes.

UI Setting	Description
<b>PoE Supported</b>	Shows whether the port supports PoE.
<b>Power Output</b>	Shows whether PoE is enabled for the port.
<b>Output Mode</b>	Shows the output mode for the port.
<b>Power Allocation</b>	Shows the power allocation value for the port. When the output mode is <b>Auto</b> , this value is fixed as 0.
<b>Priority</b>	Shows the port priority: Critical (highest) / High / Low.

## PoE - Edit Port Settings

### Menu Path: Port > PoE - General

Clicking the **Edit** (✎) icon for a port on the **Port > PoE - General** page will open this dialog box. This dialog lets you edit PoE settings for the port.

Click **APPLY** to save your changes.

### Edit Port 1 Settings

Power Output \*

Output Mode \*

Power Allocation  
  
 .....  
 0 - 30 Watt

Priority \*

Copy configurations to ports  ⓘ







UI Setting	Description	Valid Range	Default Value
<b>Power Output</b>	Enable/disable PoE for this port.	Enabled / Disabled	Enabled
<b>Output Mode</b>	Specify whether to set the PoE output mode to Auto or Force. <b>Auto:</b> Power output will be determined by using 802.3at auto-detection. <b>Force:</b> Power output will be determined by the <b>Power Allocation</b> setting for the port. This may be necessary for PDs that do not follow 802.3af/at standards.	Auto / Force	Auto
<b>Power Allocation</b>	Specify the power in watts to allocate to a connected PD when the <b>Output Mode</b> is set to <b>Force</b> . <ul style="list-style-type: none"> <li>When the output mode is <b>Auto</b>, the value is fixed as 0.</li> <li>When the output mode is set to <b>Force</b>, input a value from 0 to 30.</li> </ul>	0 to 30	N/A
<b>Priority</b>	Specify the priority of the port to use with the <b>Auto Power Cutting</b> feature. If Auto Power Cutting is enabled, PoE will be disabled for ports with lower priority when total power consumption exceeds the system power budget threshold. Ports with lower priority will be disabled before ports with higher priority. Refer to <a href="#">PoE - General</a> for more information.	Critical / High / Low	Low
<b>Copy configurations to ports</b>	Select the ports you want to copy this configuration to.	Drop-down list of ports	N/A

## PD Failure Check

### Menu Path: Port > PoE - PD Failure Check

This tab lets you monitor the status of a powered device (PD) through its IP address. If the PD fails, the switch will not receive a PD response after the defined period, and the PoE powering process will be restarted. This function is extremely useful for ensuring network reliability and simplifying management.




PoE							
General		PD Failure Check			Status		
		Q Search					
Port	PoE Supported	Enable	Device IP	Check Frequency (sec.)	No Response Times	Action	
 1	Yes	Disabled	0.0.0.0	10	3	No Action	
 2	Yes	Disabled	0.0.0.0	10	3	No Action	
 3	Yes	Disabled	0.0.0.0	10	3	No Action	
 4	Yes	Disabled	0.0.0.0	10	3	No Action	
 5	Yes	Disabled	0.0.0.0	10	3	No Action	

UI Setting	Description
<b>Port</b>	Shows which port this row describes.
<b>PoE Supported</b>	Shows whether the port supports PoE.
<b>Enable</b>	Shows whether PD failure checking is enabled or disabled for the port.
<b>Device IP</b>	Shows what IP will be monitored for PD failure checking for the port.
<b>Check Frequency (sec.)</b>	Shows how often PD failure checks will be performed for the port.
<b>No Response Times</b>	Shows how many IP checking cycles will be tried before determining a PD is not responding.
<b>Action</b>	Shows what action will be taken if a PD failure is detected for the port.

## PD Failure Check - Edit Port Settings

### Menu Path: Port > PoE - PD Failure Check

Clicking the **Edit** () icon for an port on the **Port > PoE - PD Failure Check** page will open this dialog box. This dialog lets you configure the PD failure check settings for each port.

Click **APPLY** to save your changes.

## Edit Port 1 Settings

Enable \*  
 Disabled ▼

Device IP \*  
 0.0.0.0

Check Frequency \*  
 10  
 5 - 300 sec.

No Response Times \*  
 3  
 1 - 10 times

Action \*  
 No Action ▼

Copy configurations to ports ▼ ⓘ

CANCEL APPLY

UI Setting	Description	Valid Range	Default Value
<b>Enable</b>	Enable or disable PD failure checks for the port to check the status of PDs via ICMP.	Enabled / Disabled	Disabled
<b>Device IP</b>	Specify the IP address of the PD connected to the port to send ping packets to check for PD connection failure.	Valid IP address	0.0.0.0
<b>Check Frequency</b>	Specify how frequently in seconds ping packets will be sent to to the <b>Device IP</b> . If there is no reply, a "no response" will be detected.	5 to 300	10
<b>No Response Times</b>	Specify the number of consecutive "no response" events required to detect a PD connection failure and execute the specified <b>Action</b> .	1 to 10	3

UI Setting	Description	Valid Range	Default Value
<b>Action</b>	Specify the action to take when the number of <b>No Response Times</b> is reached. <ul style="list-style-type: none"> <li>• <b>No Action:</b> No action will be taken.</li> <li>• <b>Restart PD:</b> PoE power to the PD will be stopped, then started again to restart the PD.</li> <li>• <b>Shut Down PD:</b> PoE power to the PD will be stopped.</li> </ul>	No Action / Restart PD / Shut Down PD	No Action
<b>Copy configurations to ports</b>	Select the ports you want to copy this configuration to.	Drop-down list of ports	N/A

## PoE - Scheduling

### Menu Path: Port > PoE - Scheduling

This page lets you create PoE scheduling rules that can be applied to individual ports or multiple ports.

#### 🔗 Limitations


You can create up to 20 PoE scheduling rules

## PoE - System Time Status

System Time Status		
System Time	Local TimeZone	Daylight Saving Time
04:01	UTC+00:00	Off

UI Setting	Description
<b>System Time</b>	Shows the current system time of the device.
<b>Local Time Zone</b>	Shows the time zone of the device.
<b>Daylight Saving Time</b>	Shows whether the daylight saving time is on.

## PoE Scheduling - Rule List

<input type="checkbox"/>	Rule Name	Enable	Start Date	Schedule Time	Apply the rule to the port
<input type="checkbox"/>	 poerule1	Disabled	2024-5-13	18:00 - 21:00, Daily	1

Max. 20

UI Setting	Description
<b>Rule Name</b>	Shows the name of the scheduling rule.
<b>Enable</b>	Shows whether the rule is enabled or disabled.
<b>Start Date</b>	Shows when this rule will become active.
<b>Schedule Time</b>	Shows when the PoE will supply power for the specified ports. The system will not supply PoE power outside the scheduled time.
<b>Apply the rule to the port</b>	Shows which ports will use this rule.

## PoE Scheduling - Create Rule

### Menu Path: [Port](#) > [PoE - Scheduling](#)

Clicking the **Add (+)** icon on the **Port > PoE - Scheduling** page will open this dialog box. This dialog lets you create a PoE scheduling rule.

Click **CREATE** to save your changes.

**Create Rule**

Rule Name \* 0 / 63

Rule \* ▼

Start Date \* 📅

Start Time \* 🕒      End Time \* 🕒

Repeat Execution \* ▼

Apply the rule to the ... ▼

CANCEL    CREATE

UI Setting	Description	Valid Range	Default Value
<b>Rule Name</b>	Specify a name for the scheduling rule.	1 to 63 characters	None
<b>Rule</b>	Enable or disable the scheduling rule.	Enabled / Disabled	Disable
<b>Start Date</b>	Specify a start date for the rule to become active.	mm/dd/yyyy	None
<b>Start Time</b>	Specify a start time to enable PoE.	AM/PM hh/mm	None
<b>End Time</b>	Specify an end time to disable PoE.	AM/PM hh/mm	None
<b>Repeat Execution</b>	Specify whether to repeat execution of the rule on a daily or weekly basis.	None / Daily / Weekly	None
<b>Apply the rule to port</b>	Specify which ports should use this rule.	Select port(s) from the drop-down list	None

## PoE Scheduling - Edit Rule

### Menu Path: Port > PoE - Scheduling

Clicking the **Edit** (✎) icon for a rule on the **Port > PoE - Scheduling** page will open this dialog box. This dialog lets you edit an existing PoE scheduling rule.

Click **APPLY** to save your changes.

### Edit Rule

Rule Name \*  
poerule1 8 / 63

Rule \*  
Disabled

Start Date \*  
2024-05-13

Start Time \*      End Time \*  
下午 06:00      下午 09:00

Repeat Execution \*  
Daily

Apply the rule to the port \*  
1

CANCEL
APPLY

UI Setting	Description	Valid Range	Default Value
<b>Rule Name</b>	Specify a name for the scheduling rule.	1 to 63 characters	None
<b>Rule</b>	Enable or disable the scheduling rule.	Enabled / Disabled	Disable
<b>Start Date</b>	Specify a start date for the rule to become active.	mm/dd/yyyy	None
<b>Start Time</b>	Specify a start time to enable PoE.	AM/PM hh/mm	None
<b>End Time</b>	Specify an end time to disable PoE.	AM/PM hh/mm	None
<b>Repeat Execution</b>	Specify whether to repeat execution of the rule on a daily or weekly basis.	None / Daily / Weekly	None
<b>Apply the rule to port</b>	Specify which ports should use this rule.	Select port(s) from the drop-down list	None

## PoE Scheduling - Delete Rule

### Menu Path: Port > PoE - Scheduling

You can delete a rule by using the checkboxes to select the entries you want to delete, then clicking the **Delete** (🗑️) icon.

## PoE - Status

**Menu Path:** Port > PoE - Status


This page lets you view PoE system and port status.


### PoE - System Status

## PoE

- General
- PD Failure Check
- Status**

### System Status

Power Budget Limit	Allocated Power	Consumed Power	Remaining Power Available	
150 Watts	0 Watts	0 Watts	150 Watts	

UI Setting	Description
<b>Power Budget Limit</b>	Shows the PoE power budget limit.
<b>Allocated Power</b>	Shows the total allocated PoE power.
<b>Consumed Power</b>	Shows the total consumed PoE power.
<b>Remaining Power Available</b>	Shows the remaining power available for the device.
	 <b>Note</b> Remaining Power Available is Maximum Input Power minus Allocated Power.

## PoE Status - Port List

### Note

When a higher-power 802.3bt (Class 5~8) PD is connected to a lower-power 802.3at or 802.3af PSE, the PD will simply operate at a lower power state, which is known as downgrading. In this case, the classification and the device type of the PD will appear as Class 4 and 802.3at because of inherent device limitations.

Port	PoE Supported	Power Output	Classification	Current (mA)	Voltage (V)	Consumption (W)	Device Type	Configuration suggestion	PD Failure Check Status
1	Yes	Off	Unknown	0.00	0.00	0.00	N/A	Enable PoE power output	Not alive
2	Yes	Off	Unknown	0.00	0.00	0.00	N/A	Enable PoE power output	Not alive
3	Yes	Off	Unknown	0.00	0.00	0.00	N/A	Enable PoE power output	Not alive
4	Yes	Off	Unknown	0.00	0.00	0.00	N/A	Enable PoE power output	Not alive
5	Yes	Off	Unknown	0.00	0.00	0.00	N/A	Enable PoE power output	Not alive

UI Setting	Description
<b>Port</b>	Shows the number of the PoE port.
<b>PoE Supported</b>	Shows whether the port supports PoE.
<b>Power Output</b>	Shows whether PoE power output is on or off for the port.
<b>Classification</b>	Shows the PoE power classification of the port. Each PoE power classification has a different maximum power (in watts) by PSE output as follows: <ul style="list-style-type: none"> <li>• <b>0</b>: 15.4 watts</li> <li>• <b>1</b>: 4 watts</li> <li>• <b>2</b>: 7 watts</li> <li>• <b>3</b>: 15.4 watts</li> <li>• <b>4</b>: 30 watts</li> </ul>
<b>Current (mA)</b>	Shows the amount of current (in mA) being supplied to the port.
<b>Voltage (V)</b>	Shows the voltage (in V) being used for the port.
<b>Consumption (W)</b>	Shows the power consumption (in W) of the device connected to the port.



UI Setting	Description
<b>Device Type</b>	<p>Shows the device type of the device currently connected to the port.</p> <ul style="list-style-type: none"> <li>• <b>Not Present:</b> There are no active connections to the port.</li> <li>• <b>Legacy PoE Device:</b> A legacy PD is connected to the port, and the device has detected that the voltage is too low or high, or the PD's detected capacitance is too high.</li> <li>• <b>802.3at:</b> An IEEE 802.3at PD is connected to the port.</li> <li>• <b>802.3af:</b> An IEEE 802.3af PD is connected to the port.</li> <li>• <b>NIC:</b> A NIC is connected to the port.</li> <li>• <b>Unknown:</b> An unknown PD is connected to the port.</li> <li>• <b>N/A:</b> The PoE function is disabled.</li> </ul>
<b>Configuration Suggestion</b>	<p>Shows configuration suggestions based on detected conditions.</p> <ul style="list-style-type: none"> <li>• <b>Disable PoE power output:</b> A NIC or unknown PD was detected; you may want to disable PoE power output for the port.</li> <li>• <b>Select Force Mode:</b> A higher/lower resistance or higher capacitance was detected; you may want to select <b>Force Mode</b> for the port.</li> <li>• <b>Select high power output:</b> An unknown classification was detected; you may want to select <b>High Power</b> output.</li> <li>• <b>Raise the external power supply voltage to greater than 46 VDC:</b> When the external supply voltage is detected at less than 46 V, the system suggests raising the voltage.</li> <li>• <b>Enable PoE function for detection:</b> The system suggests enabling the PoE function.</li> <li>• <b>Select IEEE 802.3at auto mode:</b> When detecting an IEEE 802.3at PD, the system suggests selecting 802.3at Auto mode.</li> <li>• <b>Select IEEE 802.3af auto mode:</b> When detecting an IEEE 802.3af PD, the system suggests selecting 802.3af Auto mode.</li> </ul>
<b>PD Failure Check</b>	<p>Shows the results of the last PD failure check, if checking is enabled. Refer to <a href="#">PD Failure Check</a> for more information.</p> <ul style="list-style-type: none"> <li>• <b>Disable:</b> PD failure checking is not enabled for the port.</li> <li>• <b>Alive:</b> The port is alive, and passed the last PD failure check.</li> <li>• <b>Not Alive:</b> The port is not alive, and failed the last PD failure check.</li> </ul>

# Layer 2 Switching

## Menu Path: Layer 2 Switching

This section lets you configure your device's Layer 2 switching features.

This section includes these pages:

- VLAN
- GARP
- MAC
- QoS
- Multicast

## Layer 2 Switching - User Privileges

Privileges to settings are granted to the different authority levels as follows. Refer to [System > Account Management > User Accounts](#) for more information on user accounts.

Settings	Admin	Supervisor	User
<b>VLAN</b>	R/W	R/W	R
<b>GARP</b>	R/W	R/W	R
<b>MAC</b>			
<b>Static Unicast</b>	R/W	R/W	R
<b>MAC Address Table</b>	R/W	R/W	R
<b>QoS</b>			
<b>Classification</b>	R/W	R/W	R
<b>Ingress Rate Limit</b>	R/W	R/W	R
<b>Scheduler</b>	R/W	R/W	R


Settings	Admin	Supervisor	User
<b>Egress Shaper</b>	R/W	R/W	R
<b>Multicast</b>			
<b>IGMP Snooping</b>	R/W	R/W	R
<b>GMRP</b>	R/W	R/W	R
<b>Static Multicast</b>	R/W	R/W	R

## About VLAN

A VLAN, or Virtual Local Area Network, is a logical grouping of devices on a network.

## Assigning VLANs to Ports

VLANs must be assigned to ports to route traffic correctly. Now that you've created the VLANs, they need to be assigned to ports so that traffic from those ports will be routed over the correct VLAN. A similar procedure must be performed on each switch or router on the network.

1. Sign in to the device using administrator credentials.
2. Go to **Layer 2 Switching**→**VLAN**→**Settings**.
3. To assign the newly created VLAN ID to a port, find the port on the **Port Table** on the lower part of the page, and then click  **[Edit]**.  
**Result:** The **Edit Port Settings** panel appears.
4. Specify the **Mode** and **PVID** that will be assigned to the port, and then click **Apply**.

### Tutorial Info:

**Access mode** is used when connecting single devices without tags. These are usually end-user devices that belong to a single VLAN, and do not need to communicate with devices in other VLANs.

**Trunk mode** allows a port to carry traffic for multiple VLANs over a single physical connection. This is useful for linking switches together that may have many different VLANs.

**Hybrid mode** is similar to a Trunk port, except users can explicitly assign tags to be removed from egress packets.

 **Note**


The port VID (PVID) setting will apply a VLAN tag only for untagged traffic coming through that port. If traffic going through the port has already been tagged with a VLAN ID, the PVID setting will not change the existing tag.

**Result:** The **Port Table** will show the new port configuration.

## Creating VLANs

Create VLANs in preparation for assigning them to ports.

To create a VLAN, do the following:

1. Sign in to the device using administrator credentials.
2. Go to **Layer 2 Switching > VLAN > Settings**.
3. To add a VLAN ID, click  **[Add]**.

**Result:** The **Create VLAN** screen appears.

4. Specify the VLAN to create in the **VID**, and then click **Create**.

Optionally:


- Type a human-readable identifier in the **Name** field
- Assign the VLAN to a **Member Port**. You also assign VLANs to ports later.

**Result:** The VLAN will appear on the VLAN table at the top of the page.

5. Repeat this process to create VLANs needed for the network topology.

**What to do next:** After you have created the VLANs needed for your topology, you can assign VLANs to ports if you have not done so already.

 **Note**

You can delete VLANs by choosing a VLAN ID from the VLAN table at the top of the page, clicking the checkbox, and then clicking  [Delete].

## VLANs in Depth

This technology allows network administrators to divide a large network into smaller, more manageable segments without the need for additional physical hardware. Devices within a VLAN can be located anywhere on the network but communicate as though they are on the same physical segment. This facilitates traffic management, as administrators can ensure traffic is directed only to devices within the same VLAN by assigning a VLAN tag to each Ethernet frame. Consequently, VLANs provide a means to segment a network beyond the constraints of physical connections, a limitation inherent in traditional network design. VLANs can be utilized to segment your network into various groups, such as:

- **Departmental groups**—One VLAN for the R&D department, another for Office Automation, etc.
- **Hierarchical groups**—One VLAN for directors, another for managers, and another for general staff.
- **Usage groups**—One VLAN for email users and another for multimedia users.

## VLAN Standards and Implementation

The functioning of VLANs is guided by IEEE 802.1Q, often referred to as Dot1q. This standard outlines the protocol for VLAN tagging on Ethernet frames within an IEEE 802.3 Ethernet network. During the transmission of data between switches, VLAN tags identify the VLAN ownership of frames. Networking equipment reads these tags and ensures that tagged frames are delivered to devices within that VLAN, maintaining the network's logical segmentation.

A VLAN tag is a specific piece of data embedded in the header of an Ethernet frame. It comprises a 4-byte field carrying key information, such as the VLAN ID (VID) and priority level. The VID is a numerical identifier that uniquely links the frame to a specific VLAN. The priority field within the tag plays a critical role in prioritizing certain types of traffic within a VLAN. This structure contributes to effective network traffic management by giving precedence to certain data when necessary.

## Benefits of VLANs

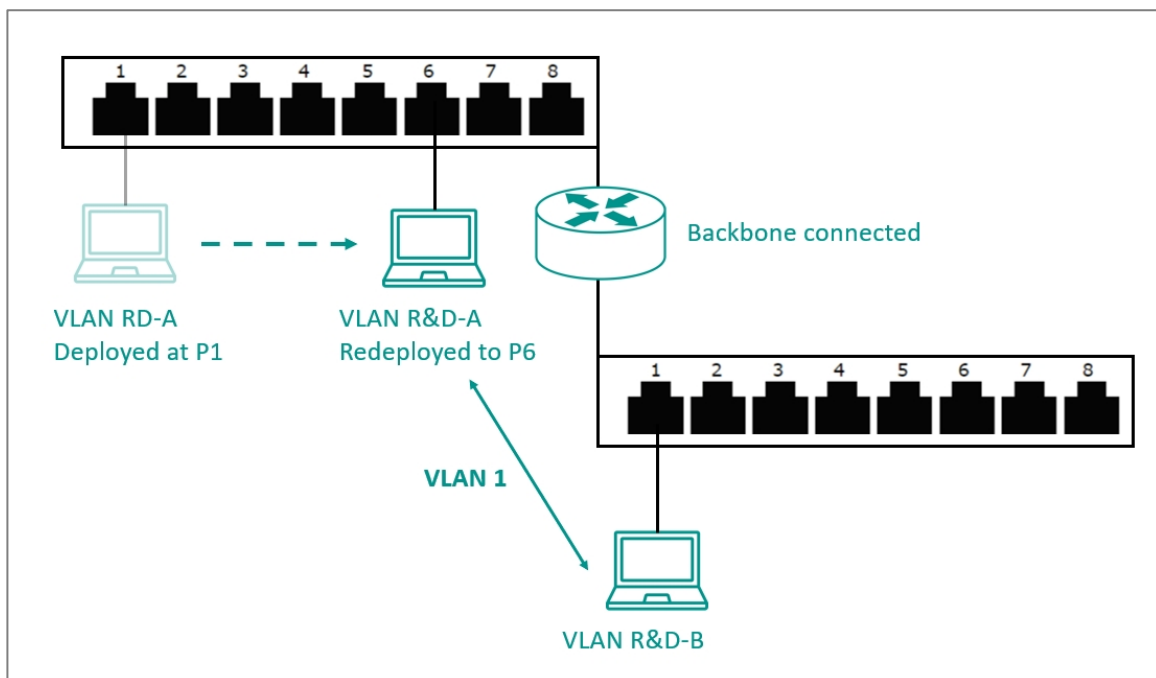
The main benefit of VLANs is that they provide a network segmentation system that is far more flexible than traditional networks. Using VLANs also provides you with three other benefits:

### VLANS help control traffic

With traditional networks, congestion can be caused by broadcast traffic that is directed to all network devices, regardless of whether or not they need it. VLANs increase the efficiency of your network because each VLAN can be set up to contain only those devices that need to communicate with each other.

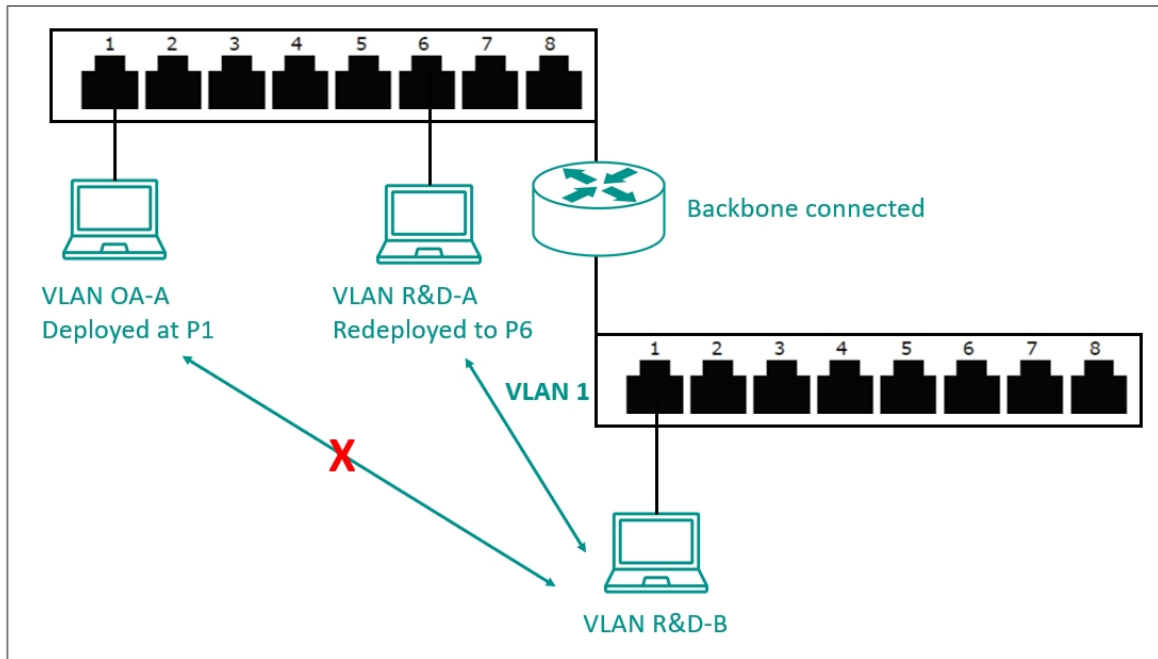
### VLANS simplify device relocation

In traditional networks, administrators spend significant time managing moves and changes, requiring manual updates of host addresses when users switch sub-networks. In contrast, VLANs simplify this process. For example, when relocating a host from Port 1 to Port 6 in a different network section, simply assign Port 6 to the relevant VLAN (e.g., VLAN R&D A). This enables seamless communication between VLANs, eliminating the need for re-cabling.



### VLANS provide extra security

Devices within each VLAN can only communicate with other devices on the same VLAN. If VLAN R&D B needs to communicate with VLAN OA(Office Automation) A, the traffic must pass through a routing device or Layer 3 switch.



**Note**

Network segmentation is not a substitute for network security. While network segmentation can provide a degree of isolation that contributes to the overall security environment, the primary benefit of VLANs is improved performance by ensuring minimal crosstalk between unrelated systems. Network segmentation should be complimented with network security procedures.

## VLAN Settings

**Menu Path: Layer 2 Switching > VLAN**

This page lets you view and configure your device's VLAN settings.

This page includes these tabs:

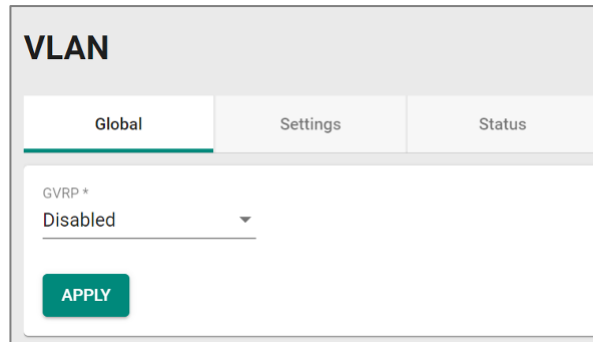
- Global
- Settings
- Status

## VLAN - Global

**Menu Path:** Layer 2 Switching > VLAN - Global

This page lets you configure the global VLAN settings.

### GVRP Settings



UI Setting	Description	Valid Range	Default Value
<b>GVRP</b>	Enable or disable GVRP for the device.	Enabled / Disabled	Disabled

**Note**

MSTP and GVRP are both VLAN-related functions. When VLAN changes dynamically, MSTP needs to re-converge, which can make the system unstable due to running complex operations. When both MSTP and GVRP are used together, this can result in network instability.

Therefore, it is recommended that network administrators avoid enabling both MSTP and GVRP.

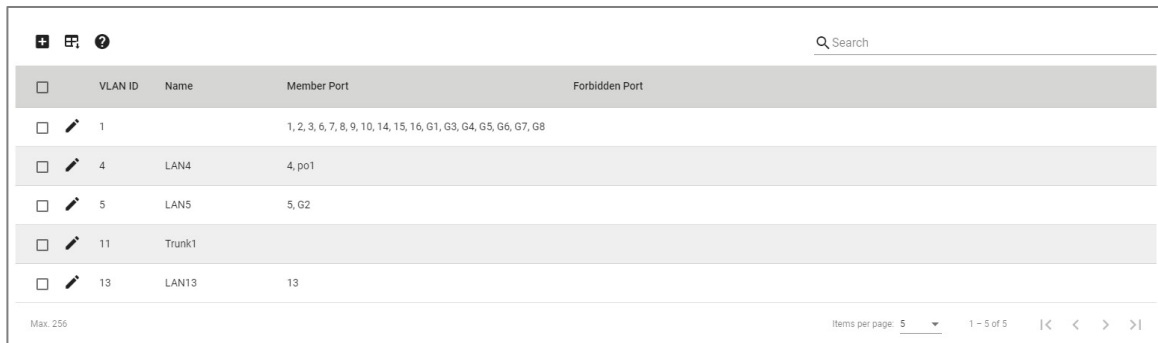
## VLAN - Settings

**Menu Path:** Layer 2 Switching > VLAN - Settings

This page lets you configure VLANs and which ports they include.



## VLAN List



<input type="checkbox"/>	VLAN ID	Name	Member Port	Forbidden Port
<input type="checkbox"/>	1		1, 2, 3, 6, 7, 8, 9, 10, 14, 15, 16, G1, G3, G4, G5, G6, G7, G8	
<input type="checkbox"/>	4	LAN4	4, po1	
<input type="checkbox"/>	5	LAN5	5, G2	
<input type="checkbox"/>	11	Trunk1		
<input type="checkbox"/>	13	LAN13	13	

Max: 256

Items per page: 5 1 - 5 of 5 |< < > >|

UI Setting	Description
<b>VLAN ID</b>	Shows the ID of the VLAN.
<b>Name</b>	Shows the name of the VLAN.
<b>Member Port</b>	Shows the member port(s) of the VLAN.
<b>Forbidden Port</b>	Shows the forbidden port(s) of the VLAN.

## VLAN - Create VLAN

### Menu Path: Layer 2 Switching > VLAN - Settings

Clicking the **Add (+)** icon for port on the **Layer 2 Switching > VLAN - Settings** page will open this dialog box. This dialog lets you create a VLAN.

Click **CREATE** to save your changes.

## Create VLAN

**Create VLAN**

VLAN ID \* i  
Max. 10 VLANs

Name 0 / 32

Member Port ▼

Forbidden Port ▼

CANCEL
CREATE

UI Setting	Description	Valid Range	Default Value
<b>VLAN ID</b>	Specify the VLAN ID.	1 to 4094	N/A
<b>Name</b>	Specify the name of the VLAN.	0 to 32 characters	N/A
<b>Member Port</b>	Specify the member port(s) of the specific VLAN.	Drop-down list of ports	N/A
<b>Forbidden Port</b>	Specify the forbidden port(s) of the specific VLAN.	Drop-down list of ports	N/A

## VLAN Port Status List

Q Search

	Port	Mode	PVID	GVRP	Untagged VLAN	Tagged VLAN
✎	1	Access	1	Disabled	1	
✎	2	Access	1	Disabled	1	
✎	3	Access	1	Disabled	1	
✎	4	Access	4	Disabled	4	
✎	5	Access	5	Disabled	5	

UI Setting	Description
<b>Port</b>	Shows the port number.

UI Setting	Description
<b>Mode</b>	Shows the mode of the port. <ul style="list-style-type: none"> <li>• <b>Access:</b> The port is connected to a single device, without tags.</li> <li>• <b>Trunk:</b> The port is connected to another 802.1Q VLAN aware switch.</li> <li>• <b>Hybrid:</b> The port is connected to another Access 802.1Q VLAN aware switch or another LAN that combines tagged and/or untagged devices.</li> </ul>
<b>PVID</b>	Shows the default VLAN ID for untagged devices connected to the port. The PVID will be added for ingress traffic, and will be removed for egress traffic for the access port only.
<b>GVRP</b>	Shows whether GVRP is enabled for the port.
<b>Untagged VLAN</b>	When the port is using <b>Hybrid</b> VLAN mode, this shows all VLAN IDs that will be removed from egress packets.
<b>Tagged VLAN</b>	When the port is using <b>Trunk</b> or <b>Hybrid</b> VLAN mode, this shows all VLAN IDs will be carried to connected devices.

## VLAN - Status

**Menu Path:** Layer 2 Switching > VLAN - Status

This page lets you monitor the status of the VLANs on your device.

### VLAN Switchport Mode Table

VLAN ID	Name	Status	Hybrid Port	Trunk Port	Access Port
1		Permanent			1, 2, 3, 6, 7, 8, 9, 10, 14, 15, 16, G1, G3, G4, G5, G6, G7, G8
4	LAN4	Permanent			4, po1
5	LAN5	Permanent			5, G2
11	Trunk1	Permanent			
13	LAN13	Permanent			13

Items per page: 5 | 1 - 5 of 5 | < > >>

UI Setting	Description
<b>VLAN ID</b>	Shows the ID of the VLAN.
<b>Name</b>	Shows the name of the VLAN.

UI Setting	Description
<b>Status</b>	Shows the status of the VLAN.
<b>Hybrid Port</b>	Shows ports acting as a Hybrid Port for the VLAN.
<b>Trunk Port</b>	Shows ports acting as a Trunk Port for the VLAN.
<b>Access Port</b>	Shows ports acting as an Access Port for the VLAN.

## VLAN Membership Table

VLAN Membership Table

🔄 🗒️ 🔍 Search

VLAN ID	Name	Status	Untagged Port	Tagged Port	Forbidden Port
1		Permanent	1, 2, 3, 6, 7, 8, 9, 10, 14, 15, 16, G1, G3, G4, G5, G6, G7, G8		
4	LAN4	Permanent	4, po1		
5	LAN5	Permanent	5, G2		
11	Trunk1	Permanent			
13	LAN13	Permanent	13		

Items per page: 5 | 1 - 5 of 5 | < > >> <<

UI Setting	Description
<b>VLAN ID</b>	Shows the ID of the VLAN.
<b>Name</b>	Shows the name of the VLAN.
<b>Status</b>	Shows the status of the VLAN.
<b>Untagged Port</b>	Shows the untagged port(s) for the VLAN.
<b>Tagged Port</b>	Shows the tagged port(s) for the VLAN.
<b>Forbidden Port</b>	Shows the forbidden port(s) for the VLAN.

# GARP

Generic Attribute Registration Protocol (GARP) is a communication protocol defined by IEEE 802.1 that offers a generic framework for bridges to register and de-register an attribute value.

In a VLAN structure, two GARP applications can be applied:



- **GARP VLAN Registration Protocol (GVRP)** is used to register VLAN trunking between multilayer switches.
- **GARP Multicast Registration Protocol (GMRP)** provides a constrained multicast flooding facility.

## GARP Settings

**Menu Path: Layer 2 Switching > GARP**

This page lets you configure GARP settings for each port.

### GARP List

	Port	Join Time	Leave Time	Leave All Time
	1	200	600	10000
	2	200	600	10000
	3	200	600	10000
	4	200	600	10000
	5	200	600	10000
	6	200	600	10000

UI Setting	Description
<b>Port</b>	Shows which port the entry is for.
<b>Join Time (sec.)</b>	Shows the join time for the port.
<b>Leave Time (sec.)</b>	Shows the leave time for the port.
<b>Leave All time (sec.)</b>	Shows the leave all time for the port.

## GARP - Edit Port Settings

### Menu Path: Layer 2 Switching > GARP

Clicking the **Edit** (✎) icon for a port on the **Layer 2 Switching > GARP** page will open this dialog box. This dialog lets you configure the GARP parameters for each port.

Click **APPLY** to save your changes.

### Edit Port 1 Settings

Join Time \*

200

---

10 - 1073741810

Leave Time \*

600

---

30 - 2147483630

Leave All Time \*

10000

---

40 - 2147483640

Copy configurations to ports ▼ ⓘ

---

CANCEL
APPLY

UI Setting	Description	Valid Range	Default Value
<b>Join Time (sec.)</b>	Specify the join time in seconds.	10 to 499999980	200
<b>Leave Time (sec.)</b>	Specify the leave time in seconds.	30 to 499999980	600
<b>Leave All time (sec.)</b>	Specify the leave all time in seconds.	30 to 499999990	10000
<b>Copy configurations to ports</b>	Select the ports you want to copy this configuration to.	Drop-down list of ports	N/A

## MAC

### Menu Path: [Layer 2 Switching](#) > [MAC](#)

This section lets you manage MAC related switching features of your device.

This section includes these pages:

- [Static Unicast](#)
- [MAC Address Table](#)

### About Static Unicast

Static Unicast lets you manually define specific forwarding paths for data packets destined for particular devices on the network.

### Static Unicast

#### Menu Path: [Layer 2 Switching](#) > [MAC](#) > [Static Unicast](#)

This page lets you manage your device's static unicast entries.

### 🔒 Limitations

You can create up to 256 static unicast entries.

## Unicast Table

	VLAN ID	MAC Address	Port
<input type="checkbox"/>	4	00:11:22:33:44:55	po1

Max. 256

UI Setting	Description
<b>VLAN ID</b>	Shows the VLAN ID used for the static unicast entry.
<b>MAC Address</b>	Shows the MAC address used for the static unicast entry.
<b>Port</b>	Shows which ports are included for the static unicast entry.

## Add a Static Unicast Entry

### Menu Path: Layer 2 Switching > MAC > Static Unicast

Clicking the **Add (+)** icon on the **Layer 2 Switching > MAC > Static Unicast** page will open this dialog box. This dialog lets you add a new static unicast entry.

Click **CREATE** to save your changes and add the new entry.

**Add a Static Unicast Entry**

VLAN ID \*      MAC Address \*

Port \*

CANCEL      CREATE



UI Setting	Description	Valid Range	Default Value
<b>VLAN ID</b>	Specify the VLAN ID.	Drop-down list of VLAN IDs	N/A
<b>MAC Address</b>	Specify the static unicast MAC address of the port.	Valid unicast MAC address	N/A
<b>Port</b>	Specify which ports you want to include in the static unicast group	Drop-down list of ports	N/A

## About MAC Address Tables

The MAC address table is a database maintained on your device that acts like a directory to keep track of all the devices currently connected to the network. Each entry in the table includes a device's unique identifier, known as its Media Access Control (MAC) address, and the specific switch port it is connected to.

### Note

Moxa devices manage MAC address learning for VLANs using IVL (Independent VLAN Learning), which uses separate MAC address tables for each VLAN so that MAC address learning for different VLANs do not interfere with each other.

A MAC table will be stored in the format of MAC + VID. This allows the same MAC address to be used in multiple VLANs without causing forwarding issues.

This may lead to a larger MAC address table size, as each VLAN maintains its own individual address table, and the number of MAC address entries will increase based on the number of VLAN member ports used.

## MAC Address Table

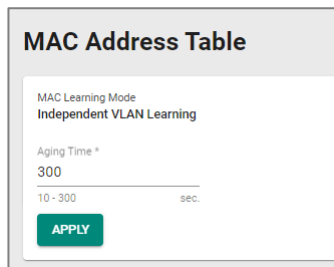
**Menu Path:** [Layer 2 Switching](#) > [MAC](#) > [MAC Address Table](#)

This page lets you view your device's MAC address table and set the aging time for MAC address entries.

### 🔒 Limitations

The MAC address table can hold up to 16384 entries.

## MAC Address Settings



MAC Address Table

MAC Learning Mode  
Independent VLAN Learning

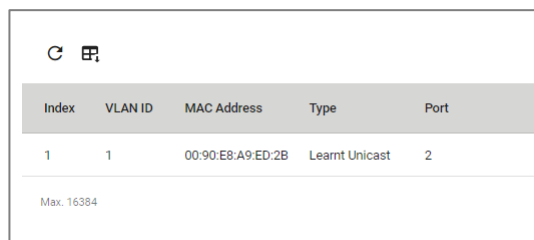
Aging Time \*  
300  
10 - 300 sec.

APPLY

UI Setting	Description	Valid Range	Default Value
<b>MAC Learning Mode</b>	Shows the current MAC learning mode.	N/A	Independent VLAN Learning
<b>Aging Time</b>	Specify the aging time for MAC address entries in seconds. The aging time determines how long entries will be kept in the MAC address table in the device's memory before expiring.	10 to 300	300

Click APPLY to save your changes.

## MAC Address Table List



Index	VLAN ID	MAC Address	Type	Port
1	1	00:90:E8:A9:ED:2B	Learnt Unicast	2

Max. 16384

UI Setting	Description
<b>Index</b>	Shows the index number of the MAC address.
<b>VLAN ID</b>	Shows which VLAN ID is being used for the MAC address.

UI Setting	Description
<b>MAC Address</b>	Shows the MAC address of the device.
<b>Type</b>	Shows what kind of MAC address entry this is: <b>Learnt Unicast:</b> Used for all learnt unicast MAC addresses. <b>Learnt Multicast:</b> Used for all learnt multicast MAC addresses. <b>Static Unicast:</b> Used for all static unicast MAC addresses. <b>Static Multicast:</b> Used for all static multicast MAC addresses.
<b>Port</b>	Shows which port on the device the MAC address is connected to.

## About QoS

Quality of Service (QoS) is a set of techniques and mechanisms used in computer networks to prioritize certain types of traffic to ensure reliable delivery of data and optimize network performance. QoS mechanisms allow network administrators to define policies and rules for managing network resources and controlling the flow of traffic based on factors such as traffic type and application requirements.

This device has the following QoS features:

- Classification
- Ingress Rate Limit
- Scheduler
- Egress Shaper

## QoS In Depth

This device provides Quality of Service (QoS) for your network by classifying and prioritizing traffic to make data delivery more reliable. Traffic can be classified by applying IEEE 802.1p/1Q Layer 2 CoS (Class of Service) tags or Layer 3 DSCP (Differentiated Services Code Point) information. The device can use these together with a set of rules that specify how each type of traffic should be treated as it passes through the device. This allows delivery of traffic to be prioritized to ensure that high-priority data is transmitted with minimum delay. Refer to Classification for more information about traffic classification.

Two scheduling algorithms, Strict Priority and Weighted Round Robin, are available to empower network administrators to choose the most suitable method for packet transmission in their field applications. Refer to Scheduler for more information.

In addition to packet classification for incoming packets and scheduling for outgoing packets, users can also establish a rate threshold for incoming data. When this limit is exceeded, they can choose to either drop or remark the packet. Refer to Ingress Rate Limit for more information.

The egress shaper helps optimize outbound traffic, maintain network stability, and ensure efficient utilization of available bandwidth resources. Refer to Egress Shaper for more information.

## QoS

### Menu Path: Layer 2 Switching > QoS

This section lets you enable and configure your device's QoS settings.

This section includes these pages:

- Classification
- Ingress Rate Limit
- Scheduler
- Egress Shaper

#### Note

For MX-NOS platform devices, QoS behavior will be consistent as long as the chipset solutions are the same. Therefore, RKS/MDS/TN devices will exhibit identical QoS behavior.

## Classification

Traffic classification and prioritization allows you to classify data for prioritization so that time-sensitive and system-critical data can be transferred smoothly and with minimal delay over a network.

Benefits of using traffic classification and prioritization include:

- Improving network performance by controlling a wide variety of traffic types and managing congestion

- Assigning priorities to different categories of traffic, such as setting higher priorities for time-critical or mission-critical applications
- Providing predictable throughput to improve the performance of multimedia applications—such as video conferencing or voice over IP—to minimize traffic delay and jitter
- Optimizing network utilization depending on application usage and usage needs, allowing the amount of traffic to increase without requiring increases in backbone bandwidth

Traffic classification and prioritization uses eight traffic queues to ensure that higher priority traffic can be forwarded separately from lower priority traffic to help guarantee quality of service (QoS) for your network.

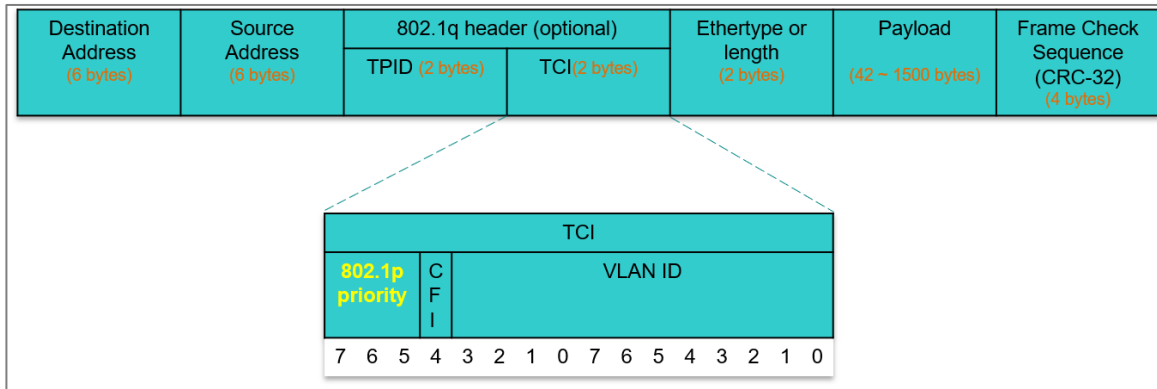
Traffic classification and prioritization for your Moxa device is based on two standards:

- **IEEE 802.1p Class of Service:** A Layer 2 QoS marking scheme
- **Differentiated Services (DiffServ) Traffic Marking:** A Layer 3 QoS marking scheme

### **IEEE 802.1p Class of Service (CoS) In Depth**

The IEEE Std 802.1D 2005 Edition marking scheme, which is an enhancement to IEEE Std 802.1D, enables Quality of Service on a LAN. Traffic service levels are defined in the IEEE 802.1Q 4-byte tag, which is used to carry VLAN identification as well as IEEE 802.1p priority information. If the 802.1q header presents and the Tag Protocol Identifier (TPID) value is 0x8100, then it means the frame is tagged. The TPID is followed by a 2-byte field Tag Control Information (TCI) which contains a 3-bit 802.1p priority field as shown in below figure.

The IEEE Std 802.1D 2005 Edition priority marking scheme assigns an IEEE 802.1p priority level between 0 and 7 to each frame, which specifies the level of service that the associated packets shall be handled.



The table below shows an example of how different traffic types can be mapped to the eight IEEE 802.1p priority levels.

IEEE 802.1p Priority (decimal)	IEEE 802.1p Priority (binary)	IEEE 802.1D Traffic Type
0	0 0 0	Best Effort
1	0 0 1	Background (lowest priority)
2	0 1 0	Reserved
3	0 1 1	Excellent Effort (business critical)
4	1 0 0	Controlled Load (streaming multimedia)
5	1 0 1	Video (interactive media)
6	1 1 0	Voice (interactive voice)
7	1 1 1	Network Control Reserved traffic

Even though the IEEE 802.1p standard is the most widely used prioritization scheme for LAN environments, it still has some restrictions:

- It requires an additional 4-byte tag in the frame, which is normally optional for Ethernet networks. Without this tag, the scheme cannot work.
- The tag is part of the IEEE 802.1Q header, so to implement QoS at Layer 2, the entire network must implement IEEE 802.1Q VLAN tagging.
- It is only supported within a LAN and does not cross the WAN boundaries, since the IEEE 802.1Q tags will be removed when the packets pass through a router.

## Differentiated Services (DiffServ) Traffic Marking In Depth

DiffServ is a Layer 3 marking scheme that uses the DiffServ Code Point (DSCP) field in the IP header to specify the packet priority. DSCP is an intelligent method of traffic marking that allows you to choose how your network prioritizes different types of traffic. The DSCP field can be set from 0 to 63 to map to user-defined service levels, enabling users to regulate and categorize traffic by application and assign different service levels.

### Advantages of DiffServ over IEEE 802.1Q

- You can prioritize and assign different traffic with appropriate latency, throughput, or reliability for each port.
- No extra tags are required.
- The DSCP priority tags are carried in the IP header, which can pass through WAN boundaries and through the Internet.
- DSCP is backwards compatible with IPv4 ToS (Type of Service), which allows operation with legacy devices that use IPv4 Layer 3.

### Default Mapping of DSCP and CoS Values

DSCP values	Mapped CoS value
0 to 7	0
8 to 15	1
16 to 23	2
24 to 31	3
32 to 39	4
40 to 47	5
48 to 55	6
56 to 63	7

## Traffic Prioritization In Depth

Moxa switches classify traffic based on Layer 2 of the OSI 7 layer model, and prioritize outbound traffic according to the priority information defined in received packets. Incoming traffic is classified based on the IEEE 802.1p service level field and is assigned to the appropriate egress priority queue.

Traffic flows through the switch as follows:

- A received packet may or may not have an 802.1p tag associated with it. If it does not, then it is given a default CoS value according to the port settings in the Classification section.
- Each egress queue has associated 802.1p priority levels that can be defined by users. Packets will be placed in the appropriate priority queue. When the packet reaches the head of its queue and is about to be transmitted, the device determines whether or not the egress port belongs to the VLAN group. If it is, then the new 802.1p tag is used in the extended 802.1D header.

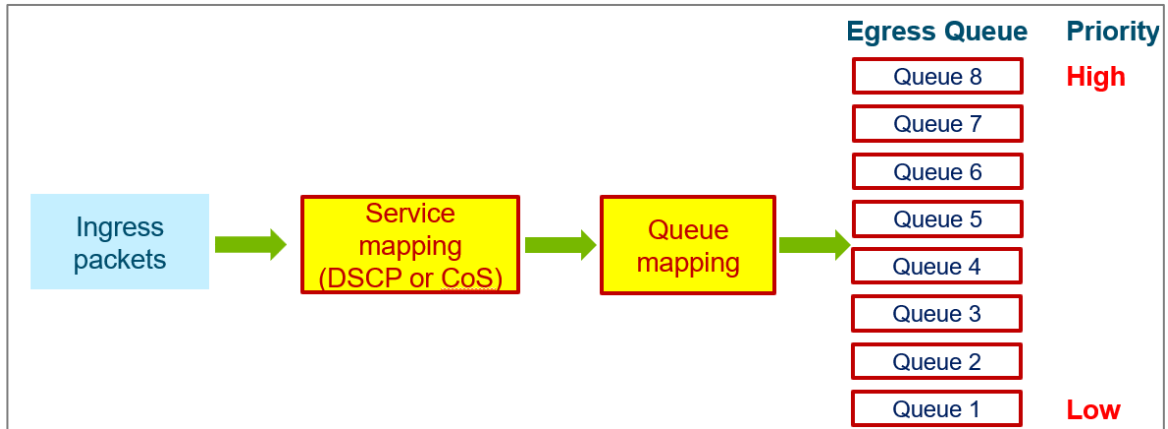
Please be aware that the priority of redundancy protocol control packets is determined by the switch and is not influenced by user-specified QoS settings. The prioritization of traffic is determined by the QoS policies configured on network devices, and remains consistent regardless of whether the interface used is a single port or a trunk port.

## Traffic Queues In Depth

Moxa switches have eight different traffic queues that allow packet prioritization to occur. The priority of these queues ranges from 1 (lowest priority) to 8 (highest priority). Higher priority traffic can pass through the switch without being delayed by lower priority traffic.

Ingress packets containing DSCP or CoS fields require classification and mapping to a priority queue. Incoming packets with a specified DSCP value at Layer 3 are remapped to a CoS value at Layer 2 before being directed to an egress queue. The corresponding mapping of DSCP to CoS and the CoS to the egress queue priority should be preconfigured on a Moxa switch. As each packet arrives at the switch, it undergoes ingress processing (which includes classification, marking/re-marking), and is then sorted into the appropriate egress queue.





Packets lacking DSCP or CoS values will be directed to the appropriate egress queue based on the settings of Untag Default Priority configured in Port Settings. Refer to Port Classification - Edit Port Setting for more information.

## Classification

### Menu Path: Layer 2 Switching > QoS > Classification

This page lets you configure your device's QoS classifications.

This page includes these tabs:

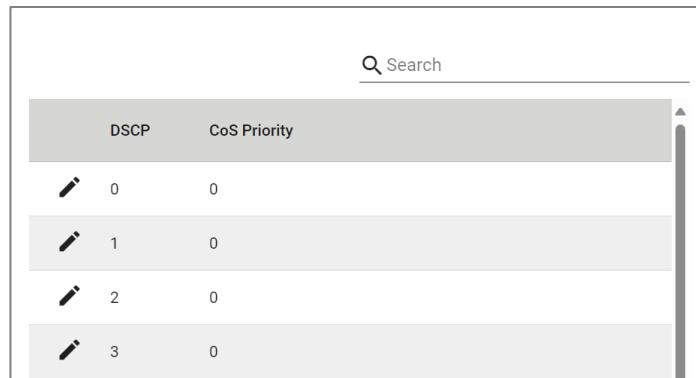
- DSCP Mapping
- CoS Mapping
- Port Settings





## DSCP Mapping

### Menu Path: Layer 2 Switching > QoS > Classification - DSCP Mapping

This page lets you view and edit your DSCP CoS mappings.

## DSCP Mapping List




	DSCP	CoS Priority
	0	0
	1	0
	2	0
	3	0

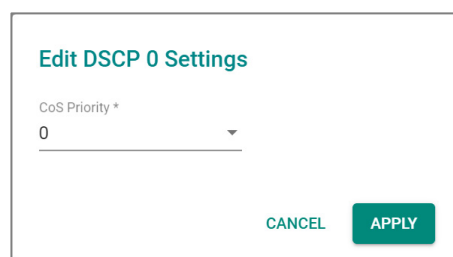
UI Setting	Description
<b>DSCP</b>	Shows the DSCP value for the entry.
<b>CoS Priority</b>	Shows the CoS priority mapped to the DSCP value.

## Edit DSCP Settings

### Menu Path: Layer 2 Switching > QoS > Classification - DSCP Mapping

Clicking the **Edit** () icon for an entry on the **Layer 2 Switching > QoS > Classification - DSCP Mapping** page will open this dialog box. This dialog lets you edit CoS priority for a DSCP value.

Click **APPLY** to save your changes.



**Edit DSCP 0 Settings**

CoS Priority \*

0

CANCEL APPLY







UI Setting	Description	Valid Range	Default Value
<b>CoS Priority</b>	Specify the CoS priority to assign to the DSCP value. Higher numbers have higher priority.	0 to 7	DSCP 0 to 7: 0 DSCP 8 to 15: 1 DSCP 16 to 23: 2 DSCP 24 to 31: 3 DSCP 32 to 39: 4 DSCP 40 to 47: 5 DSCP 48 to 55: 6 DSCP 56 to 63: 7

## CoS Mapping

**Menu Path: Layer 2 Switching > QoS > Classification - CoS Mapping**

This page lets you view and edit your CoS Queue mappings.

### CoS Mapping List

		Q Search
CoS	Queue	
 0	1	
 1	2	
 2	3	
 3	8	
 4	5	
 5	6	

UI Setting	Description
CoS	Shows the CoS value for the entry.
Queue	Shows the queue mapped to the CoS value.

## Edit CoS Settings

### Menu Path: Layer 2 Switching > QoS > Classification - CoS Mapping

Clicking the **Edit** (✎) icon for a CoS value on the **Layer 2 Switching > QoS > Classification - CoS Mapping** page will open this dialog box. This dialog lets you map a queue to a CoS value.

Click **APPLY** to save your changes.






UI Setting	Description	Valid Range	Default Value
Queue	Select a queue to map to the CoS value. Queues with higher numbers have higher priority.	1 to 8	CoS 0: 1 CoS 1: 2 CoS 2: 3 CoS 3: 4 CoS 4: 5 CoS 5: 6 CoS 6: 7 CoS 7: 8

## QoS - Port Settings

### Menu Path: Layer 2 Switching > QoS > Classification - Port Settings

This page lets you manage the trust type and CoS value for untagged packets on a per-port basis.


## Port Settings List

Q Search			
	Port	Trust Type	Priority
	1	CoS	0
	2	CoS	3
	3	CoS	3
	4	CoS	3
	5	CoS	3

UI Setting	Description
<b>Port</b>	Shows the port number for the entry.
<b>Trust Type</b>	Shows the trust type used to classify traffic for the port.
<b>Priority</b>	Shows the CoS value to use for untagged packets for the port.

## QoS - Edit Port Settings

### Menu Path: Layer 2 Switching > QoS > Classification - Port Settings

Clicking the **Edit** () icon for a port on the **Layer 2 Switching > QoS > Classification - Port Settings** page will open this dialog box. This dialog lets you edit the trust type and priority for a specific port.

Click **APPLY** to save your changes.

### Edit Port 1 Settings

Trust Type \*  
CoS

Untag Default Priority \*  
3

Copy configurations to ports i

CANCEL APPLY

UI Setting	Description	Valid Range	Default Value
<b>Trust Type</b>	Select the trust type used to classify traffic for the port.	CoS / DSCP	CoS
<b>Untag Default Priority</b>	Specify a CoS value to use for untagged packets for the port. Higher values will have higher priority.	0 to 7	3
<b>Copy configurations to ports</b>	Select the ports you want to copy this configuration to.	Drop-down list of ports	N/A

## About Ingress Rate Limits

Ingress rate limits drop—or "mark"—network traffic when it exceeds user-defined thresholds.

### Ingress Rate Limits In-depth

There are two elements to this process:

- **Meter** - An algorithm in the switch that monitors and limits traffic by applying QoS markers to data packets or dropping them entirely
- **Marker** - The DSCP/802.1p field of data packets is assigned a value or "marked" by the QoS policies, determining their handling in the network

Meter algorithms include simple token bucket and SrTCM (Single Rate Three Color Marker) (RFC2697).

In addition to ingress rate management, the switch also offers an option for the administrators to configure the shutdown of an Ethernet port that may be under attack from an excess of incoming packets, such as a Denial-of-Service attack.

### **About Port Shutdown**

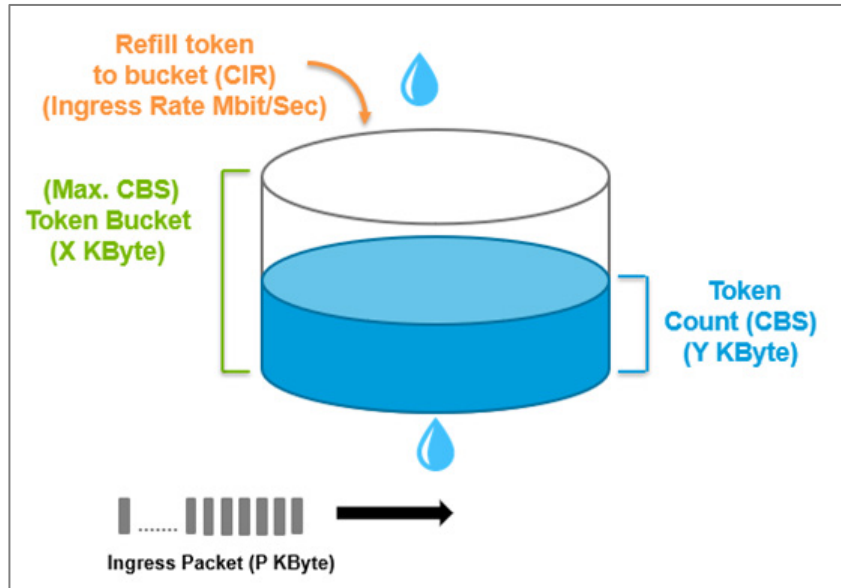
Ports can be shutdown to avoid broadcast storms.

In general, any user shall not consume unlimited bandwidth and influence others' access. One particular scenario is that a malfunctioning switch or mis-configured network might cause "broadcast storms". Moxa industrial Ethernet switches not only prevent broadcast storms, but can also regulate ingress packet rates, giving administrators full control of their limited bandwidth to prevent undesirable effects caused by unpredictable faults.

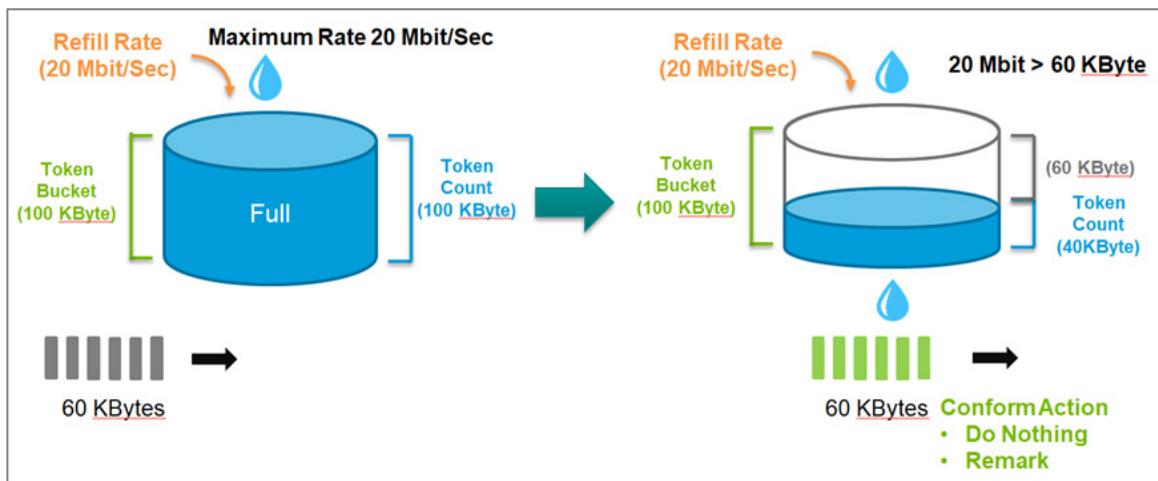
The network administrator has the option to establish a maximum throughput threshold (in Mbps) for incoming packets on a designated port and activate this function. If unexpected ingress packets are detected on that port, the physical Ethernet port will be disabled, preventing further packet transmission. Re-activation of the port can be done manually or left to occur automatically after the pre-defined release interval, specified in minutes, has elapsed.

### **About Token Buckets**

Token Bucket is an algorithm used to achieve an efficient network flow control and manage bandwidth. This algorithm is based on a token bucket that allows for a traffic surge for short periods. When a token is unavailable, no burst of packets can be sent. Under this concept, the number of tokens will be refilled in the bucket at specific intervals. Users need to configure these settings so that the tokens in the bucket are always available to ensure packets can be sent when necessary.



**CAR (Committed Access Rate)** is a traffic control mechanism used to ensure that packets meet the network rules before they enter the network. CAR can guarantee the traffic flow is under user-defined control; the packets exceeding the rule will be either dropped or remarked and transmitted again. When network traffic is jammed, these packets will be dropped first.



Token Bucket is an algorithm that is demonstrated as a container in the image below. The token can be seen as a marker to mark a packet that is allowed to be transmitted through this switch. When the token is flowing into the bucket, the length of the bucket will be consumed as the volume of the bucket is limited. When the volume of the bucket is insufficient, some packets will be dropped or remarked and transmitted again. This



algorithm can control the speed of the traffic flow by consuming the speed of the token in the bucket.

### **About Single Rate Three Color Markers**

Single Rate Three Color Markers (SrTCM) is a policing scheme for ingress rate limits. Traffic marking is based on a Committed Information Rate (CIR) and two associated burst sizes:

- Committed Burst Size (CBS)
- Excess Burst Size (EBS)

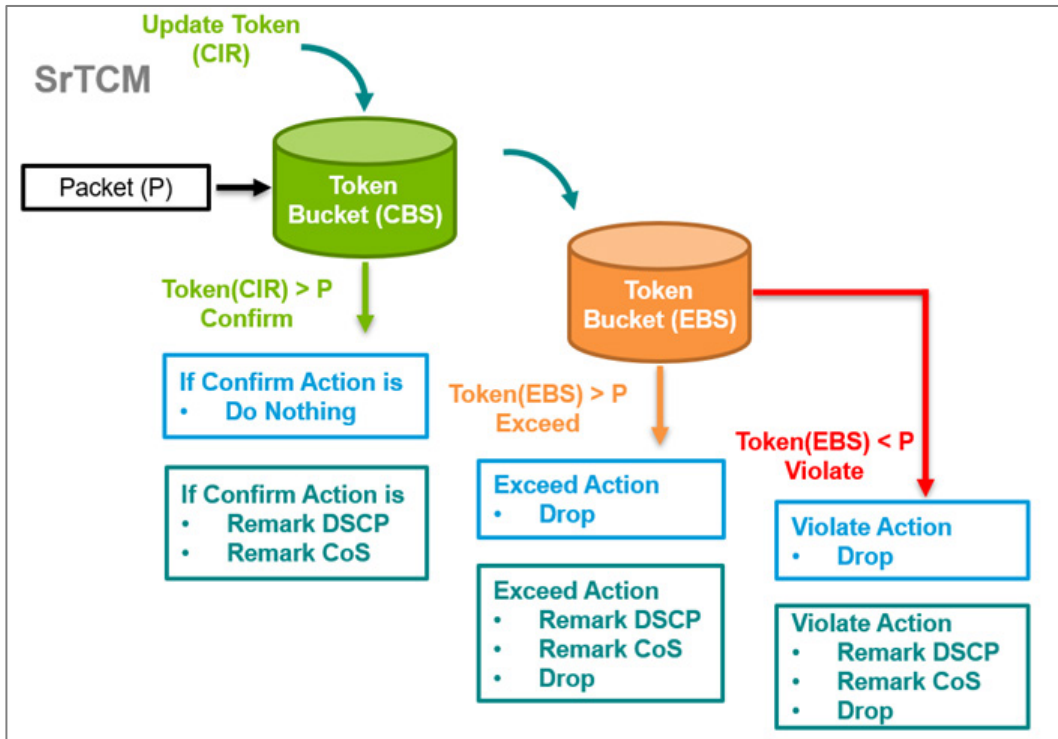
A packet is marked green if it does not exceed the CBS, yellow if it does exceed the CBS, but not the EBS, and red otherwise.

SrTCM will categorize the ingress packet by its length, and mark it as one of three colors:

- **Green:** performs the "conform" action. It could be "Do nothing", "Remark DSCP" or "Remark CoS". The Token Bucket (CBS) will deduct corresponding tokens.
- **Yellow:** performs the "exceed" action. It could be "Drop", "Remark DSCP" or "Remark CoS". The Token Bucket (EBS) will deduct corresponding tokens.
- **Red:** performs the "violate" action. It could be "Drop", "Remark DSCP" or "Remark CoS".

If you select "Do nothing" as the conform action, then "Drop" will be the only action when it enters the Exceed or Violate state.

The SrTCM is useful for ingress policing of a service, where only the length, not the peak rate, of the burst determines service eligibility.



## Dropping Limit-exceeding Incoming Packets

You can setup the ingress rate limits that will automatically drop packets exceeding limits you specify.

In this example, we will prevent the switch from being overwhelmed by unexpected large amount of ingress packets through port 1, set an ingress rate limit of 5 Mbps on port 1. Then, verify that the device connected to port 2 receives packets at no more than 5 Mbps.

### Before you begin:

- Change the configuration mode to **Advanced** mode by selecting the mode in the upper right corner of the UI.
  - Create a new **VLAN ID** with a value of **10**
  - Configure Port 1 with a **PVID** of 10 and with **Access mode** enabled
  - Configure Port 2 with a **PVID** of 10 and with **Access mode** enabled
1. Sign in to the device using administrator credentials.
  2. Go to **Layer 2 Switching**→**QoS**→**Ingress Rate Limit**→**General**.

3. Click **[Edit]** corresponding to **Port 1**.

**Result:** The **Edit Port Settings** dialogue appears.

4. In the **Ingress Rate (CIR)** field, specify 5 Mbps, and then click **Apply**.

**Result:** The new Ingress Rate (CIR) will appear in the table.

### **Results:**

When a device connected to port 1 sends out a large number of packets (for example, at a rate exceeding 10 Mbps), the switch will throttle the incoming packets to match the configured limit (5 Mbps in this example) before forwarding them to port 2.

## **Remarking Limit-exceeding Incoming Packets**

### **Abstract:**

**Short Description:** You can setup the ingress rate limits that will automatically remark packets exceeding limits you specify.

In this example, we will limit incoming packets to 5 Mbps on Port 1—maintaining a consistent ingress rate. To avoid dropping data caused by a sudden influx of packets from Port 1, the outgoing packets will be remarked with a DSCP value (0x07) before sending over Port 2.

### **Before you begin:**

- Change the configuration mode to **Advanced** mode by selecting the mode in the upper right corner of the UI.
- Create a new **VLAN ID** with a value of **10**
- Configure Port 1 with a **PVID** of 10 and with **Access mode** enabled
- Configure Port 2 with a **PVID** of 10 and with **Access mode** enabled

1. Sign in to the device using administrator credentials.
2. Go to **Layer 2 Switching**→**QoS**→**Ingress Rate Limit**→**General**.
3. Click **[Edit]** corresponding to **Port 1**.

**Result:** The **Edit Port Settings** dialogue appears.

4. Specify the following:

Value	Option
<b>Type</b>	<b>Simple Token Bucket</b>
<b>Ingress Rate (CIR)</b>	5 Mbps
<b>Conform Action</b>	<b>Remark DSCP</b>
<b>Conform Action &gt; Remark Value</b>	<b>0</b>
<b>Violate Action</b>	<b>Remark DSCP</b>
<b>Violate Action &gt; Remark Value</b>	<b>7</b>

5. Click **Apply** to save changes.

### Results:

When a device connected to port 1 sends out a large number of packets (for example, at a rate exceeding 10 Mbps), the switch will throttle the incoming packets to match the configured limit (5 Mbps in this example) and remark DSCP value (0x07) without dropping the packets. This ensures the timely transmission of data to the device connected on port 2.

### Ingress Rate Limit

#### Menu Path: [Layer 2 Switching](#) > [QoS](#) > [Ingress Rate Limit](#)

This page lets you configure your device's QoS ingress rate limit.

This page includes these tabs:


- General
- Port Shutdown

### Ingress Rate Limit - General







#### Menu Path: [Layer 2 Switching](#) > [QoS](#) > [Ingress Rate Limit - General](#)


This page lets you view and edit the ingress rate limit for each port.

### Ingress Rate Limit List

 **Note**

Some fields are only visible when using Advanced Mode.

🔍 Search									
Port	Type	Ingress Rate (CIR)	CBS	EBS	Mode	Conform Action	Exceed Action	Violate Action	
 1	Simple Token Bucket	100	1024	---	---	Do Nothing	---	Drop	
 2	Simple Token Bucket	100	1024	---	---	Do Nothing	---	Drop	
 3	Simple Token Bucket	100	1024	---	---	Do Nothing	---	Drop	
 4	Simple Token Bucket	100	1024	---	---	Do Nothing	---	Drop	
 5	Simple Token Bucket	100	1024	---	---	Do Nothing	---	Drop	
 6	Simple Token Bucket	100	1024	---	---	Do Nothing	---	Drop	

UI Setting	Description
<b>Port</b>	Shows the port number for the entry.
<b>Type</b>	Shows the ingress limit type for the port.
<b>Ingress Rate (CIR)</b>	Shows the ingress Committed Information Rate (CIR) value for the port.
<b>CBS</b>	Shows the ingress Committed Burst Size (CBS) value for the port.
<b>EBS</b>	Shows the ingress Excess Burst Size (EBS) value for the port.
<b>Mode</b>	Shows the meter mode for the port. <div style="background-color: #f0f0f0; padding: 5px; margin-top: 10px;"><p> <b>Note</b> Currently, only color-blind mode is supported for metering.</p></div>
<b>Conform Action</b>	Shows the conform action for the port.
<b>Exceed Action</b>	Shows the exceed action for the port.
<b>Violate Action</b>	Shows the violate action for the port.

## Ingress Rate Limit - Edit Port Settings

### Menu Path: Layer 2 Switching > QoS > Ingress Rate Limit - General

Clicking the **Edit** (✎) icon for a port on the **Layer 2 Switching > QoS > Ingress Rate Limit - General** page will open this dialog box. This dialog lets you select the traffic policy and configure associated actions for specific conditions on a per-port basis.

Click **APPLY** to save your changes.

### Edit Port 1 Settings

Type \*  
SrTCM

Ingress Rate (CIR) \*  
100  
1 - 100 Mbps

CBS \*  
1024  
10 - 10240 Kbyte

EBS \*  
1024  
10 - 10240 Kbyte

Conform Action \*  
Remark CoS

Remark Value \*  
0

Exceed Action \*  
Drop

Violate Action \*  
Drop

Copy configurations to ports

CANCEL **APPLY**

UI Setting	Description	Valid Range	Default Value
<b>Type</b>	Specify the ingress limit type to use.	Simple Token Bucket / SrTCM	Simple Token Bucket
<b>Ingress Rate (CIR)</b>	Specify the maximum bandwidth allowed for ingress through the port in Mbps.	1 to 1000	100 for Fast Ethernet ports, 1000 for Gigabit Ethernet ports

UI Setting	Description	Valid Range	Default Value
<b>CBS (Committed Burst Size)</b>	Specify the data buffer size in KB for the port that can be used when the data rate exceeds the CIR rate. Data that exceeds the CIR rate will be saved in this buffer, and will be sent when bandwidth is available.	0 to 10240	1024
<b>EBS (Excess Burst Size) (if Type is SrTCM)</b>	Specify the data buffer size in KB for the port when the data rate exceeds the CIR rate. Data that exceeds the CIR rate will be saved in the CBS buffer, and if the CBS buffer is full, data will be stored in the EBS buffer and will be sent when bandwidth is available.	0 to 10240	1024
<b>Conform Action</b>	Select a conform action for the port to take. If <b>Remark CoS</b> or <b>Remark DSCP</b> is selected, an additional input field will appear where a Remark value must be specified.	Do Nothing / Remark CoS / Remark DSCP	Do Nothing
<b>Exceed Action (if Type is SrTCM)</b>	Select an action to take if the amount of data exceeds both the CBS and EBS buffers. <ul style="list-style-type: none"> <li><b>Drop:</b> Packets marked as yellow will be dropped.</li> <li><b>Remark CoS:</b> Specify a CoS Remark value to use if a packet is marked as yellow. This is only available if <b>Remark CoS</b> is selected for the <b>Conform Action</b>.</li> <li><b>Remark DSCP:</b> Specify a DSCP Remark value to use if a packet is marked as yellow. This is only available if <b>Remark DSCP</b> is selected for the <b>Conform Action</b>.</li> </ul>	Drop / Remark CoS / Remark DSCP	Drop
<b>Violate Action</b>	Select an action to take if a packet violates CIR and CBS. <ul style="list-style-type: none"> <li>Drop: Packets marked as violated will be dropped.</li> <li><b>Remark CoS:</b> Specify a CoS Remark value to use if a packet is marked as violated. This is only available if <b>Remark CoS</b> is selected for the <b>Conform Action</b>.</li> <li><b>Remark DSCP:</b> Specify a DSCP Remark value to use if a packet is marked as violated. This is only available if <b>Remark DSCP</b> is selected for the <b>Conform Action</b>.</li> </ul>	Drop / Remark CoS / Remark DSCP	Drop
<b>Copy configurations to ports</b>	Select the ports you want to copy this configuration to.	Drop-down list of ports	N/A

## Port Shutdown

### Menu Path: Layer 2 Switching > QoS > Ingress Rate Limit - Port Shutdown

This page lets you enable the port shutdown feature and configure its settings for each port.

### Port Shutdown Settings

Port Shutdown \*  
Disabled ▾






Release Interval \*  
60  
0 - 10080 min.

APPLY

UI Setting	Description	Valid Range	Default Value
<b>Port Shutdown</b>	Enable or disable the port shutdown feature for the device.  <b>Note</b> After enabling this, you will still need to configure port shutdown for each port you want to use the feature with.	Enabled / Disabled	Disabled
<b>Release Interval</b>	Specify how long in minutes to wait before a shut down port is enabled again. 0 means if this port is shut down, it will remain shut down until manually enabled.	0 to 10080	60




## Port Shutdown List

Q Search			
	Port	Port Shutdown	Threshold (Mbps)
	1	Disabled	100
	2	Disabled	100
	3	Disabled	100
	4	Disabled	100
	5	Disabled	100

UI Setting	Description
<b>Port</b>	Shows the port number for the entry.
<b>Port Shutdown</b>	Shows if port shutdown is enabled or disabled for the port.
<b>Threshold (Mbps)</b>	Shows the threshold in Mbps required to trigger port shutdown for the port.

### Port Shutdown - Edit Port Settings

#### Menu Path: Layer 2 Switching > QoS > Ingress Rate Limit - Port Shutdown

Clicking the **Edit** () icon for an port on the **Layer 2 Switching > QoS > Ingress Rate Limit - Port Shutdown** page will open this dialog box. This dialog lets you configure the threshold to trigger port shutdown.

Click **APPLY** to save your changes.

UI Setting	Description	Valid Range	Default Value
<b>Port Shutdown</b>	Enable or disable port shutdown for this port.	Enabled / Disabled	Disabled
<b>Threshold</b>	Specify the threshold (Mbps) required to trigger a port shutdown.	Fast Ethernet ports: 1 to 100  Gigabit Ethernet ports: 1 to 1000	Fast Ethernet ports: 100  Gigabit Ethernet ports: 1000
<b>Copy configurations to ports</b>	Select the ports you want to copy this configuration to.	Drop-down list of ports	N/A

## About Scheduler

The Scheduler functions as an arbiter within the switching forwarding paths, prioritizing traffic flows based on user-defined criteria. This mechanism enhances data transmission efficiency and ensures that critical packets are transmitted with priority. Moxa devices support two scheduling algorithms: Strict Priority and Weighted Round Robin.

- **Weighted Round Robin:** The Weighted Round Robin type allows users to give priority to specific packets in the higher weighted queue to ensure those packets will be sent first. Moxa switches now have 8 queues, and the weights from highest to lowest are 8:8:4:4:2:2:1:1.
- **Strict:** The Strict Priority type allows users to determine to transmit packets in the highest priority queue first, while packets with lower priority will be transmitted later. This guarantees that traffic with the highest level of priority for data transmission will go first.

Moxa network devices are equipped with multiple traffic queues that enable packet prioritization. This allows higher-priority traffic to pass through the network devices without being delayed by lower-priority traffic. As each packet enters the network devices, it undergoes ingress processing, including classification and marking/re-marking, before being placed into the appropriate egress queue. The network device then forwards packets based on their assigned queue.

### **Scenario: Configuring 3 Devices with Strict Priority**

In this scenario, we will configure three attached devices on the network device with strict priority.

Specifically, we will focus on how packets are managed as they leave (egress) the network device on a particular port. In this case, the setup involves three devices:

- **Device A:** Connected to port 1 on the network device.
- **Device B:** Connected to port 2 on the network device.
- **Device C:** Connected to port 3 on the network device.

### **Objective**

The goal is to configure a "Strict Priority" scheduler on port 3 of the switch. This scheduler will control how packets are prioritized when they exit the switch from this port (which is connected to Device C).

### **Key Components**

#### **1. DSCP (Differentiated Services Code Point) Value:**

- This is a field in the IP header that indicates the level of priority a packet should have.
- In this scenario, packets from Device A have a DSCP value of 0x48, which signifies they should be treated with higher priority.

#### **2. Egress Queues:**

- Network switches typically have multiple egress queues per port. Each queue can be assigned different levels of priority.
- In this case, queue 7 is configured as a high-priority queue, while queue 1 is a lower-priority queue.

## Configuration Details

- **Device A (port 1)** is sending packets with a DSCP value of 0x48. These packets are mapped to egress queue 7 on port 3. Queue 7 is given a higher priority.
- **Device B (port 2)** is sending normal packets without any special DSCP value, so these packets are mapped to egress queue 1 on port 3. Queue 1 has a lower priority.

## "Strict Priority" Scheduler

- **Strict Priority Scheduling** is a mechanism used to determine how packets are sent out when multiple queues have packets waiting to be transmitted.
- In a strict priority setup, the switch will always service higher-priority queues first. This means that as long as there are packets in queue 7 (the high-priority queue), they will be sent out before any packets in queue 1 (the lower-priority queue) are even considered.

## Expected Behavior

- When **Device A and Device B** both send packets to **Device C** at the same time:
  - Packets from **Device A** (with DSCP 0x48) will be placed in the high-priority egress queue 7 and will be transmitted first.
  - Packets from **Device B** will be placed in the low-priority egress queue 1. These packets will only be transmitted once queue 7 is empty.
- As a result, packets from **Device A** will reach **Device C** quickly, without being delayed by the packets from **Device B**.

## Summary

By configuring the scheduler with "Strict Priority" on port 3, we're ensuring that high-priority traffic (from Device A) is not delayed by lower-priority traffic (from Device B). This setup is crucial in scenarios where certain types of data, such as real-time communications or critical control signals, must be delivered promptly without delay.

## Example: Configuring A Sample Environment for Strict Priority Scheduler (RKS-G4000\_Series)


The QoS scheduler example relies on this configuration.

1. Sign in to the device using administrator credentials.
2. Go to **Layer 2 Switching > VLAN > Settings**, and then click  **[Add]**.

The Create VLAN screen appears.

3. In **VLAN**, type 10, and then click **Create**.

The specified VLAN appears in the list.


4. In the table on the second half of the page, find **1/1** and click  **[Edit]**.

The Edit Port Settings screen appears.

5. Specify **Mode** as **Access**, and then specify a **PVID** of **10**.
6. Under **Copy configurations to ports**, choose ports **1/2** and **1/3**, and then click **Apply** to save changes.
7. Go to **Layer 2 Switching > QoS > Classification**, and under **DSCP Mapping**, locate **DSCP 48** and verify that it is set to **6**.

If the value is different, click  **[Edit]**, set **CoS Priority** to **6**, and then click **Apply**.

8. Click **CoS Mapping** at the top of the screen, locate **CoS 6**, and verify that **Queue** is set to **7**.

If the value is different, click  **[Edit]**, set **Queue** to **7**, and then click **Apply**.

The device on Port **1/3** needs to be configured to set its outgoing packets with a QoS DSCP value of 0x48.

### **Example: Configuring A Sample Environment for Strict Priority Scheduler (TN\_Series)**


The QoS scheduler example relies on this configuration.

1. Sign in to the device using administrator credentials.
2. Go to **Layer 2 Switching > VLAN > Settings**, and then click  **[Add]**.

The Create VLAN screen appears.

3. In **VLAN**, type 10, and then click **Create**.

The specified VLAN appears in the list.

4. In the table on the second half of the page, find **1** and click  **[Edit]**.

The Edit Port Settings screen appears.


5. Specify **Mode** as **Access**, and then specify a **PVID** of **10**.

6. Under **Copy configurations to ports**, choose ports **2** and **3**, and then click **Apply** to save changes.

7. Go to **Layer 2 Switching > QoS > Classification**, and under **DSCP Mapping**, locate **DSCP** 48 and verify that it is set to **6**.

If the value is different, click  **[Edit]**, set **CoS Priority** to **6**, and then click **Apply**.

8. Click **CoS Mapping** at the top of the screen, locate **CoS 6**, and verify that **Queue** is set to **7**.

If the value is different, click  **[Edit]**, set **Queue** to **7**, and then click **Apply**.

The device on Port **3** needs to be configured to set its outgoing packets with a QoS DSCP value of 0x48.

### **Example: Configuring Scheduler for Strict Priority**


Strict Priority switching ensures that higher priority packets always preempt loc

This example assumes the following configuration, outlined in the preceding section:

- VLAN of 10
- Ports **1/1**, **1/2**, and **1/3** in **Access** mode assigned to **PVID 10**
- **DSCP** 48 set to **6**
- **CoS 6** with a **Queue** of **7**

Additionally, the device on Port **1/3** needs to be configured to set its outgoing packets with a QoS DSCP value of 0x48.

If your environment does not match the above configuration, the example may not function properly.

1. Sign in to the devices using administrator credentials.
2. Go to **Layer 2 Switching > QoS > Scheduler**.
3. Locate Port **1/3**, and then click  **[Edit]**.

The Edit Port Settings screen appears.

4. Make sure **Type** is set to **Strict Priority**, and then click **Apply**.

### **Example: Configuring Scheduler for Strict Priority (TN Series)**


Strict Priority switching ensures that higher priority packets always preempt loc

This example assumes the following configuration, outlined in the preceding section:

- VLAN of 10
- Ports **1, 2, and 3** in **Access** mode assigned to **PVID 10**
- **DSCP 48** set to **6**
- **CoS 6** with a **Queue** of **7**

Additionally, the device on Port **3** needs to be configured to set its outgoing packets with a QoS DSCP value of 0x48.

If your environment does not match the above configuration, the example may not function properly.

1. Sign in to the devices using administrator credentials.
2. Go to **Layer 2 Switching > QoS > Scheduler**.
3. Locate Port **3**, and then click  **[Edit]**.

The Edit Port Settings screen appears.

4. Make sure **Type** is set to **Strict Priority**, and then click **Apply**.

## **Scheduler**

### **Menu Path: Layer 2 Switching > QoS > Scheduler**

This page lets you configure your device's QoS scheduler on a per-port basis.


## Scheduler List

Q Search		
Port	Type	
 1	SP	
 2	SP	
 3	SP	
 4	SP	
 5	SP	

UI Setting	Description
<b>Port</b>	Shows the port number for the entry.
<b>Type</b>	Shows the scheduling algorithm selected for the port.

## Scheduler - Edit Port Settings


### Menu Path: Layer 2 Switching > QoS > Scheduler

Clicking the **Edit** () icon for a port on the **Layer 2 Switching > QoS > Scheduler** page will open this dialog box. This dialog lets you select the scheduling algorithm for the port.

Click **APPLY** to save your changes.

### Edit Port 1 Settings

Type \*  
Strict Priority

Copy configurations to ports  



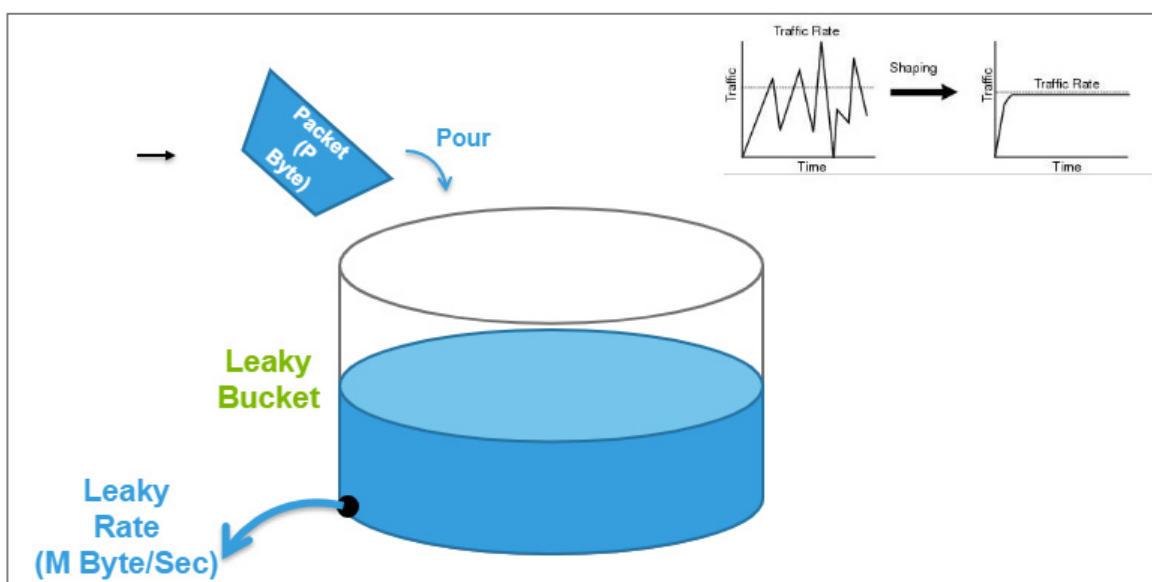
UI Setting	Description	Valid Range	Default Value
<b>Type</b>	Select the scheduler algorithm to use for the port. <ul style="list-style-type: none"> <li><b>Strict Priority:</b> Strict priority will be used.</li> <li><b>Weighted Round Robin:</b> Queued packets will be forwarded based on their associated weight.</li> </ul>	Strict Priority / Weighted Round Robin	Strict Priority
<b>Copy configurations to ports</b>	Select the ports you want to copy this configuration to.	Drop-down list of ports	N/A

## Configuring Egress Shaper

A shaper for egress traffic buffers or queues excess traffic to hold packets and shape traffic flow when source data rates are higher than expected.

### About Egress Shaper

The Egress Shaper uses a meter algorithm known as a leaky bucket. Like its physical counterpart, the leaky bucket collects incoming traffic up to a maximum capacity. Data stored in the bucket is released at a steady rate. When the bucket is empty, the flow stops.



If incoming packets would exceed the capacity the bucket, those packets would be non-conforming, and are not added to the bucket (dropped). Data will be added to the bucket as space becomes available for conforming packets. To setup Egress Shaper on a specific port, you will need to provide CIR (Committed Information Rate) and CBS (Committed Burst Rate) values.


### Configuring Rate Limits for Outgoing Traffic

You can use egress rate limits to ensure steady flow of traffic to ports you specify. In this scenario, we have 3 devices:





- Device A, connected to the switch at Port 1
- Device B, connected to the switch at Port 2
- Device C, connected to the switch at Port 3

When both Device A and Device B send packets simultaneously to Device C, and there are no rate limits set on ports 1 and 2, Configuring the Committed Information Rate (CIR) to 5 Mbps on port 3 ensures that the outgoing packets maintain a steady packet rate to reach Device C as expected.

#### Before you begin:

- Change the configuration mode to **Advanced** mode by selecting the mode in the upper right corner of the UI.
  - Create a new **VLAN ID** with a value of **10**
  - Configure Port 1 with a **PVID** of 10 and with **Access mode** enabled
  - Configure Port 2 with a **PVID** of 10 and with **Access mode** enabled
  - Configure Port 3 with a **PVID** of 10 and with **Access mode** enabled
1. Sign in to the device using administrator credentials.
  2. Go to **Layer 2 Switching > QoS > Egress Shaper**.
  3. Click  **[Edit]** corresponding to **Port 3**.  
**Result:** The **Edit Port Settings** dialogue appears.
  4. In the **CIR** field, specify 5 Mbps, and then click **Apply**.  
**Result:** The new Egress Rate (CIR) will appear in the table.






## Egress Shaper

	Port	Egress Rate (CIR)	CBS
	1	100	1024
	2	100	1024
	3	5	1024
	4	100	1024

### Egress Shaper

**Menu Path:** Layer 2 Switching > QoS > Egress Shaper

This page lets you configure QoS egress shaper settings on a per-port basis.

	Port	Egress Rate (CIR)	CBS
	1	100	1024
	2	100	1024
	3	100	1024
	4	100	1024
	5	100	1024

UI Setting	Description
<b>Port</b>	Shows the port number the entry is for.
<b>Egress Rate (CIR)</b>	Shows the egress Committed Information Rate (CIR) value for the port.

UI Setting	Description
<b>CBS</b>	Shows the egress Committed Burst Size (CBS) value for the port.

## Egress Shaper - Edit Port Settings

### Menu Path: Layer 2 Switching > QoS > Egress Shaper

Clicking the **Edit** (✎) icon for a port on the **Layer 2 Switching > QoS > Egress Shaper** page will open this dialog box. This dialog lets you configure the egress shaping settings for the port.

Click **APPLY** to save your changes.

UI Setting	Description	Valid Range	Default Value
<b>CIR (Committed Information Rate)</b>	Specify the committed data transmission rate.	Fast Ethernet ports: 1 to 100 Gigabit Ethernet ports: 1 to 1000	Fast Ethernet ports: 100 Gigabit Ethernet ports: 1000
<b>CBS (Committed Burst Size)</b>	Specify the maximum amount of data in KB that is allowed to be transmitted in a burst, even if it would cause the CIR rate to be exceeded.	10 to 10240	1024
<b>Copy configurations to ports</b>	Select the ports you want to copy this configuration to.	Drop-down list of ports	N/A

# Multicast

**Multicast** is a one-to-many communication method that sends data to a specific group of receivers. Those who wish to receive multicast packets must register for the multicast service; unregistered recipients will not receive the packets. Multicast is an "on-demand" service typically used for audio and video applications. For example, IP cameras (commonly used in CCTV systems) may need to transmit video streams to three different security guard rooms in a building simultaneously. Multicast is also used for protocol exchanges, as L3 protocols (VRRP, OSPF, RIP, etc) communicate with each other using multicast.

## Benefits of Multicast:

- **Efficient bandwidth utilization:** Multicast reduces network congestion by sending data to only interested recipients.
- **Reduced server load:** Multicast servers only need to send data once, rather than multiple times for individual recipients.
- **Scalability:** Multicast can effectively handle large groups of receivers without affecting network performance.

Overall, multicast is a valuable tool for efficient and scalable one-to-many communication, particularly in applications involving audio, video, and protocol exchanges.

## Multicast In Depth

As mentioned, multicast is a network communication method designed for efficient one-to-many data transmission. Imagine you have a presentation you want to deliver to a specific group of people in a large conference hall. Instead of emailing it to everyone individually, multicast allows you to send it to a single "group" that only the intended recipients can access.

Here's a breakdown of how it works:

- **Groups and Membership:**
  - Devices interested in receiving the same data stream form a multicast group identified by a unique multicast address.

- Devices join or leave the group dynamically using protocols like IGMP (Internet Group Management Protocol).
- **Source and Data:**
  - A single source device transmits the data (e.g., a video stream, a software update).
  - The data is encapsulated with the specific multicast address of the target group.
- **Network Routing:**
  - Network switches and routers play a crucial role in directing the data.
  - They recognize the multicast address and replicate the data packet only for the ports connected to devices that are members of the target group.
  - Devices not in the group will not receive the data, reducing unnecessary network traffic.

There are three primary methods for controlling multicast traffic on a switch:

- **Static multicast** is for configuring the multicast forwarding entries in the switch in a manual or predetermined manner. (e.g., forward 01:00:5E:05:06:07 to ports 1, 2, and 3). This method suits static networks where you want to control all the multicast flow. Another scenario is that the end device cannot communicate with IGMP protocol.
- **GMRP** allows bridges and the devices at the edge of the network to perform dynamic group membership information registration with the MAC bridges connected to the same LAN section. This method lets bridges communicate with each other to register the static multicast table dynamically.
- **IGMP snooping** allows a device to listen in on the IGMP conversation between hosts and routers. By listening to these conversations, the device maintains an association mapping table between port(s) and multicast groups. This method suits dynamic networks where end devices use IGMP to register the multicast group.

In summary, here are key considerations when selecting a multicast traffic control method:

- For static networks with predetermined multicast destinations, **static multicast** offers a simple solution.

- If you have a network with multiple bridges and static multicast tables on edge devices, **GMRP** can help maintain consistency.
- In dynamic networks where end devices use IGMP, **IGMP snooping** provides efficient management of multicast traffic.

## Multicast

### Menu Path: Layer 2 Switching > Multicast

This section lets you configure the Multicast settings.

This section includes these pages:

- IGMP Snooping
- GMRP
- Static Multicast

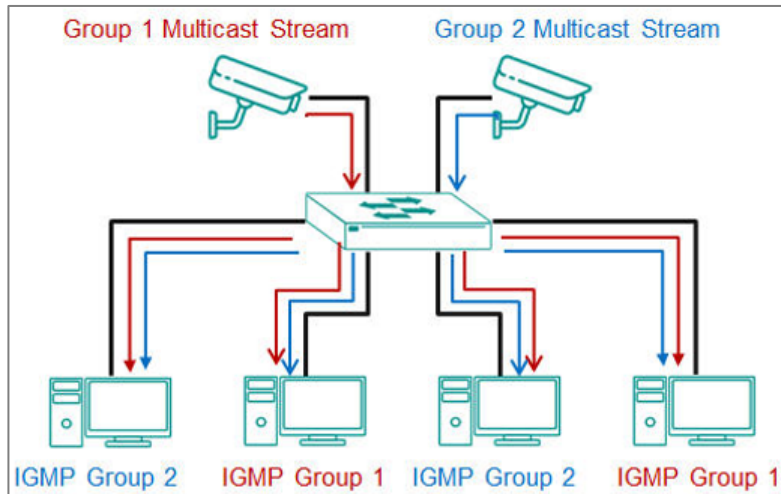
### About IGMP Snooping

IGMP snooping allows switches to reduce the amount of unwanted multicast traffic on a network by maintaining maps of multicast group members, ensuring that multicast packets are only delivered to devices that have explicitly asked to receive them. Internet Group Management Protocol (IGMP) is a network protocol that hosts nearby routers on networks to construct multicast group memberships. IGMP snooping allows a network switch to listen in on the IGMP conversation between hosts and routers. By listening to these conversations, the switch maintains an association mapping table between port(s) and multicast group.

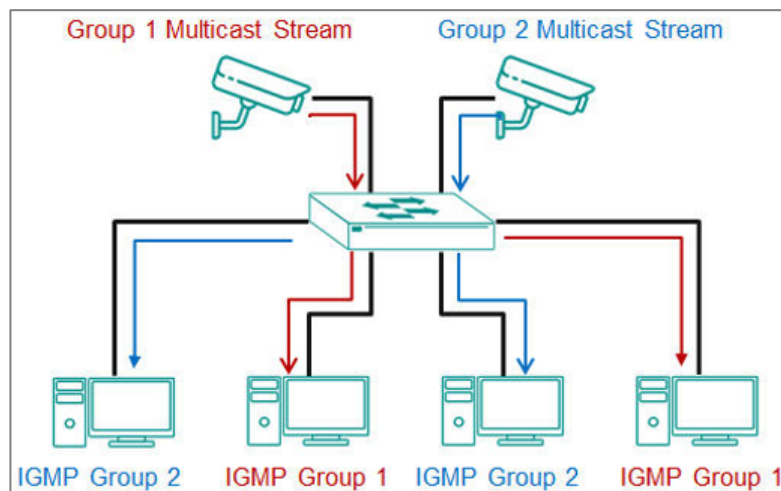
### How IGMP Snooping Works

Without IGMP snooping, a switch will flood multicast traffic to all other non-ingress ports within a broadcast domain (or VLAN). This can cause unnecessary loading for host devices by requiring them to process packets they have not solicited. IGMP snooping can help prevent host devices on a local network from receiving traffic for a multicast group they have not explicitly joined. It provides switches with a mechanism to forward multicast traffic to specific ports that receive IGMP hosts, resulting in more efficient network bandwidth utilization.

### Without IGMP Snooping:



### With IGMP Snooping:



### Enabling IGMP Snooping

IGMP Snooping must be enabled before it can be configured on specific interfaces.

To enable IGMP snooping, do the following:

1. Sign in to the device using administrator credentials.
2. Go to **Layer 2 Switching > Multicast > IGMP Snooping** and click **General**.
3. Set **IGMP Snooping** to **Enabled**.
4. Click **Apply**.

IGMP snooping is now enabled. Existing IGMP snooping configurations will now be active.



## Configuring IGMP Snooping

IGMP snooping is configured at the VLAN level.

- VLAN IDs must be created and assigned before IGMP snooping can be configured.
- IGMP Snooping must be enabled before it can be configured on specific interfaces.

To configure IGMP snooping, do the following:

1. Sign in to the device using administrator credentials.
2. Go to **Layer 2 Switching > Multicast > IGMP Snooping**, and click **VLAN Settings**.

The **IGMP Snooping** list of **VLAN IDs** appears.

3. Click  **[Edit]** corresponding to the VLANs on which to configure IGMP snooping.

**Note:** If you do not see the VLANs you expect, make sure they are correctly assigned.

The Edit VLAN Settings screen appears.

4. Configure all of the following:

Option	Value
<b>IGMP Snooping</b>	<b>Enabled</b>
<b>Version</b>	Choose a version corresponding to device support and feature needs.
<b>Query Interval</b>	125
<b>Static Router Port</b>	This is optional.
<b>Config Role</b>	<b>Querier</b>

5. Click **Apply**.

### About IGMP Versions

IGMP protocols regulate the communication mechanism between querier and listener.

For IGMP-related settings, ensure that you have chosen the correct protocol version.

Consult the table below for guidelines on choosing a version.

IGMP Version	Features	Reference
v1	<p>Features:</p> <ul style="list-style-type: none"> <li>• <b>Multicast Group Membership:</b> Host devices can join multicast groups, but there is no explicit leave message. The host will simply stop responding to membership queries.</li> <li>• <b>Membership Query:</b> Network devices periodically send membership queries to determine if any host devices are still interested in receiving multicast traffic.</li> <li>• <b>Membership Report:</b> When a host device wants to join a multicast group, it sends a membership report. If no reports are received for a multicast group, the network device assumes there are no interested hosts and stops forwarding traffic to that group.</li> </ul> <p>Limitations: No Leave Group Message: Hosts cannot explicitly leave a multicast group, which can lead to inefficient use of resources as routers have to rely on timeouts to determine if there are no more members.</p>	RFC-1112
v2	<p>Additional features:</p> <ul style="list-style-type: none"> <li>• <b>Leave Group Message:</b> Host devices can send a leave group message to notify the network device they are no longer interested in a multicast group, improving the efficiency of multicast traffic management.</li> <li>• <b>Group-Specific Queries:</b> Network devices can send group-specific queries to confirm if any members of a particular multicast group still exist, reducing overall network traffic compared to general queries.</li> <li>• <b>Query Election:</b> Introduces a mechanism to elect a single query router on a subnet to avoid redundant queries, thereby optimizing network bandwidth.</li> </ul>	RFC-2236
v3	<p>Additional Features:</p> <ul style="list-style-type: none"> <li>• <b>Source-Specific Multicast (SSM):</b> Supports source filtering, allowing host devices to specify from which sources they receive multicast traffic. This is useful for applications that need to filter out unwanted traffic from certain sources.</li> <li>• <b>Include/Exclude Mode:</b> Host devices can explicitly include or exclude traffic from specified sources, providing more granular control over multicast group membership.</li> <li>• <b>Membership Report Enhancements:</b> The membership report format is enhanced to support the new source filtering capabilities.</li> </ul>	RFC-3376

**Note**

Although most modern devices should support v3, there may be regulatory concerns or legacy deployments to consider.

## IGMP Snooping

### Menu Path: Layer 2 Switching > Multicast > IGMP Snooping

This page lets you configure IGMP snooping for your device.

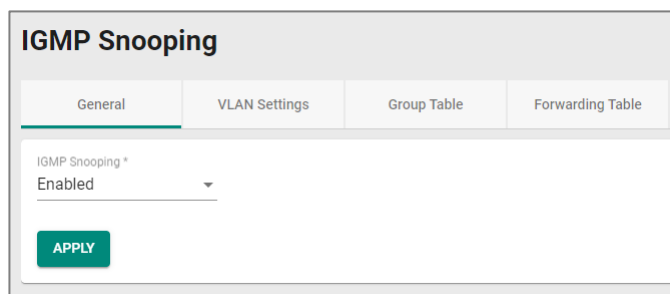
This page includes these tabs:

- General
- VLAN Settings
- Group Table
- Forwarding Table

### IGMP Snooping - General

#### Menu Path: Layer 2 Switching > Multicast > IGMP Snooping - General

This page lets you configure IGMP snooping general settings.




UI Setting	Description	Valid Range	Default Value
<b>IGMP Snooping</b>	Enable or disable IGMP snooping for the device. <b>Note</b> IGMP Snooping cannot be enabled when GMRP is enabled.	Enabled / Disabled	Enabled

## IGMP Snooping - VLAN Settings

### Menu Path: Layer 2 Switching > Multicast > IGMP Snooping - VLAN Settings

This page lets you configure IGMP snooping VLAN settings.

General	VLAN Settings	Group Table	Forwarding Table				
↻							
VLAN ID	Enable	Version	Query Interval	Config Role	Active Role	Static Router Port	Dynamic Router Port
 1	Disabled	2	125	Querier	Non-Querier	--	--
Max. 256							

UI Setting	Description
<b>VLAN ID</b>	Shows the ID of the VLAN ID the entry is for.
<b>Enable</b>	Shows whether IGMP snooping is enabled for the VLAN.
<b>Version</b>	Shows the IGMP version of the packets the VLAN will listen to and send queries for.
<b>Query Interval</b>	Shows the query interval for the Querier function globally for the VLAN, if the Querier is enabled.
<b>Config Role</b>	Shows the config role of the VLAN.
<b>Active Role</b>	Shows the active role of the VLAN.
<b>Static Router Port</b>	Shows the static router port for the VLAN. This is the port that connects to the upper level router (or IGMP querier), or to the upper level router of downstream multicast streams. All received IGMP signaling packets and multicast streams will be forwarded to the static router ports.
<b>Dynamic Router Port</b>	Shows the dynamic router port for the VLAN.

## IGMP Snooping - Edit VLAN Settings

### Menu Path: Layer 2 Switching > Multicast > IGMP Snooping - VLAN Settings

Clicking the **Edit** (✎) icon for a VLAN on the **Layer 2 Switching > Multicast > IGMP Snooping - VLAN Settings** page will open this dialog box. This dialog lets you edit the IGMP snooping settings for the VLAN.

Click **APPLY** to save your changes.

**Edit VLAN 1 Settings**

IGMP Snooping \*  
Disabled

Version \*  
2

Query Interval \*  
125  
20 - 600 sec.

Static Router Port

Config Role \*  
Querier

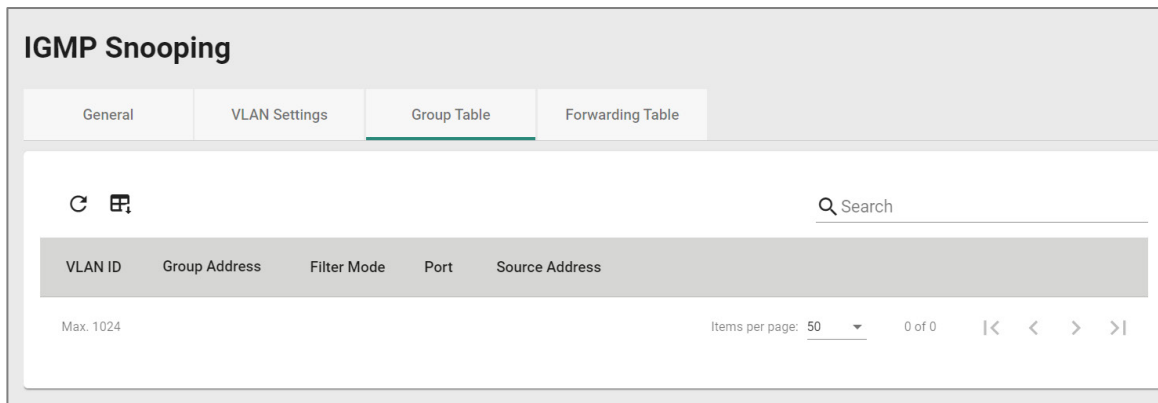
CANCEL APPLY

UI Setting	Description	Valid Range	Default Value
<b>IGMP Snooping</b>	Enable or disable IGMP snooping for the VLAN.	Enabled / Disabled	Disabled
<b>Version</b>	Specify the IGMP version of the packets to listen to and send queries for.	1 / 2 / 3	2
<b>Query Interval</b>	Specify the query interval for the VLAN, if the Querier is enabled.	20 to 600 sec.	125 sec.
<b>Static Router Port</b>	Select a static router port for the VLAN. This is the port that connects to the upper level router (or IGMP querier), or to the upper level router of downstream multicast streams. All received IGMP signaling packets and multicast streams will be forwarded to the static router ports.	Drop-down list of ports	N/A
<b>Config Role</b>	Select the config role for the VLAN.	Querier / Non-Querier	Querier

## Group Table

### Menu Path: Layer 2 Switching > Multicast > IGMP Snooping - Group Table

This page lets you view the IGMP snooping group table.

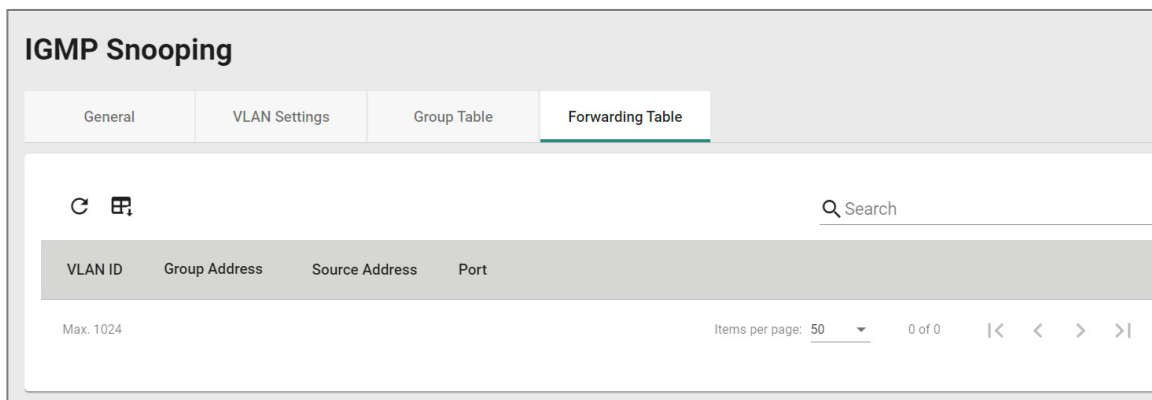


Item	Description
<b>VLAN</b>	Shows the ID of the VLAN the entry is for.
<b>Group Address</b>	Shows the registered multicast group address for the VLAN.
<b>Filter Mode</b>	Shows the filter mode for the VLAN. This is only applicable for IGMPv3. <ul style="list-style-type: none"><li>• <b>Include:</b> Source-specific multicast address group</li><li>• <b>Exclude:</b> Source-specific exclusive multicast address group</li></ul>
<b>Port</b>	Shows the forwarding port for the VLAN.
<b>Source Address</b>	Shows the source address for the VLAN. This is only applicable for IGMPv3.

## IGMP Snooping - Forwarding Table

### Menu Path: Layer 2 Switching > Multicast > IGMP Snooping - Forwarding Table

This page lets you view the IGMP snooping forwarding table.



Item	Description
<b>VLAN</b>	Shows the ID of the VLAN the entry is for.
<b>Group Address</b>	Shows the associated multicast group address for streaming data for the VLAN.
<b>Source Address</b>	Shows the source address for streaming data for the VLAN.
<b>Port</b>	Shows the forwarding port of the VLAN.

## About GMRP


GMRP stands for GARP Multicast Registration Protocol, which is a Generic Attribute Registration Protocol (GARP) application that can be used to prevent multicast from data flooding.

Both GMRP and GARP are defined by IEEE 802.1P, and widely used as a standard protocol in various industrial-related applications. GMRP allows bridges and the devices at the edge of the network to perform a dynamic group membership information registration with the MAC bridges connected to the same LAN section. The information can be transmitted among all bridges in the Bridge LAN that is implemented with extended filtering features. To operate GMRP, the GARP service must be established first.

GARP stands for **Generic Attribute Registration Protocol**, which is a communication protocol defined by IEEE 802.1, offering a generic framework for bridges to register and de-register an attribute value. In a LAN structure, two applications can be applied: **GARP VLAN Registration Protocol (GVRP)** is used to register VLAN trunking between multilayer switches, and **GARP Multicast Registration Protocol (GMRP)** for providing a constrained multicast flooding facility.

L2 switches exchange GMRP packets with each other to know the multicast entries on other switches so that it can also register the multicast entry on its own table. After exchanging the information, the multicast traffic will only be forwarded to the corresponding ports.

### Configuring GMRP

1. Sign in to the device using administrator credentials.
2. Go to **Layer 2 Switching > Multicast > GMRP**.
3. Set **GMRP** to **Enabled**, and then click **Apply**.
4. Locate the port on which you want to enable GMRP, and then click the corresponding  **[Edit]** button.

The Edit Port Settings screen appears.

5. Set **GMRP** to **Enabled**, and then click **Apply** to save your settings.

GMRP is now enabled.

### GMRP

#### Menu Path: [Layer 2 Switching > Multicast > GMRP](#)

This page lets you configure the GMRP settings of your device.



## GMRP Settings

GMRP \*










Disabled ▼

---

**APPLY**

UI Setting	Description	Valid Range	Default Value
<b>GMRP</b>	Enable or disable GMRP for the device.  <b>Note</b> GMRP cannot be enabled when IGMP Snooping is enabled.	Enabled / Disabled	Disabled

## GMRP Port List


Q Search			
Port	Enable	Group Restrict	
 1	Enabled	Disabled	
 2	Enabled	Disabled	
 3	Enabled	Disabled	
 4	Enabled	Disabled	
 5	Enabled	Disabled	
 6	Enabled	Disabled	
 7	Enabled	Disabled	
 8	Enabled	Disabled	
 9	Enabled	Disabled	

1 - 23 of 23

UI Setting	Description
<b>Port</b>	Shows the port number the entry is for.
<b>Enable</b>	Shows whether GMRP is enabled for the port.
<b>Group Restrict</b>	Shows whether group restrict is enabled for the port.

### GMRP - Edit Port Settings

#### Menu Path: Layer 2 Switching > Multicast > GMRP

Clicking the **Edit** () icon for a port on the **Layer 2 Switching > Multicast > GMRP** page will open this dialog box. This dialog lets you edit the GMRP settings for the port.

Click **APPLY** to save your changes.

### Edit Port 1/1 Settings

GMRP \*  
Disabled ▼

Group Restrict \*  
Disabled ▼

Copy configurations to ports  ▼ i

CANCEL
APPLY

UI Setting	Description	Valid Range	Default Value
<b>GMRP</b>	Enable or disable GMRP for the port.	Enabled / Disabled	Disabled
<b>Group Restrict</b>	Enable or disable group restrict for the port.	Enabled / Disabled	Disabled
<b>Copy configurations to ports</b>	Select the ports you want to copy this configuration to.	Drop-down list of ports	N/A

## About Static Multicast

Static multicast is for configuring the multicast forwarding entries in the switch in a manual or predetermined manner.

In multicast networking, data packets are sent from one sender to multiple receivers efficiently, rather than sending individual packets to each receiver separately, as in unicast communication.

Network administrators manually configure the multicast forwarding entries in the device's multicast forwarding table. This involves specifying the multicast group addresses and the corresponding outbound interfaces or ports through which multicast traffic should be forwarded.

Benefits:

1. **Predictable Behavior:** Static multicast provides predictable behavior, as the forwarding paths for multicast traffic are predetermined by the administrator. This can be advantageous in certain network environments where stability and control are prioritized over flexibility and adaptability.
2. **Resource Efficiency:** Since static multicast entries are manually configured and do not involve the overhead of dynamic routing protocols, they can be more resource-efficient in terms of processing power and network bandwidth, especially in small-scale deployments with relatively stable multicast group memberships.

## How Static Multicast works

If the user wants to restrict some of the multicast groups to be forwarded to specific ports for devices that don't support IGMP, users can use static multicast setting.

Users can manually register the multicast forwarding entries, including multicast MAC address and forwarding/forbidden port on the table, and the switch will forward the multicast traffic following the table rather than flooding.

## Static Multicast



### Menu Path: Layer 2 Switching > Multicast > Static Multicast

This page lets you view and manage your device's static multicast table.

#### Limitations

You can create up to 512 static multicast entries.

### Static Multicast Table

	VLAN ID	MAC Address	Port	Forbidden Port
<input type="checkbox"/>	1	01:00:5E:00:00:01	3	---

Max. 1024
Items per page: 50
1 - 1 of 1

UI Setting	Description
<b>VLAN ID</b>	Shows the ID of the VLAN used for the multicast group entry.
<b>MAC Address</b>	Shows the MAC address for the multicast group entry.
<b>Port</b>	Shows the egress ports that multicast streams will forward to for the multicast group entry.
<b>Forbidden Port</b>	Show the forbidden ports that packets will not be forwarded to for the multicast group entry.

## Add a Static Multicast Entry

### Menu Path: Layer 2 Switching > Multicast > Static Multicast

Clicking the **Add (+)** icon on the **Layer 2 Switching > Multicast > Static Multicast** page will open this dialog box. This dialog lets you add a static multicast entry.

Click **CREATE** to save your changes and add the new entry.

### Add a Static Multicast Entry

VLAN ID \* ▼

---

MAC Address \*

---

Port \* ▼

---

Forbidden Port ▼

---

CANCEL
CREATE

UI Setting	Description	Valid Range	Default Value
<b>VLAN ID</b>	Select a VLAN ID for the multicast entry.	Drop-down list of VLAN IDs	N/A

UI Setting	Description	Valid Range	Default Value
<b>MAC Address</b>	Specify the MAC address for the multicast entry.	Valid multicast MAC address	N/A
<b>Port</b>	Select the ports to use as egress ports for multicast streams to be forwarded to.	Drop-down list of ports	N/A
<b>Forbidden Port</b>	Select which ports are forbidden so packets cannot be forwarded to them.	Drop-down list of ports	N/A

# Network Interface

## Menu Path: Network Interface

This page lets you manage the network interfaces of your device.

This page includes these tabs:

- Settings
- Status

## Network Interface - User Privileges

Privileges to settings are granted to the different authority levels as follows. Refer to [System > Account Management > User Accounts](#) for more information on user accounts.

Settings	Admin	Supervisor	User
Network Interface	R/W	R/W	R

## Network Interface - Settings

### Menu Path: Network Interface - Settings

This page lets you manage your device's network interfaces.




#### 🔒 Limitations

You can create up to 4 loopback interfaces.

### Limitations

You can create up to 256 VLAN interfaces.

## Loopback Interface Table

Loopback Interface							
	Search						
<input type="checkbox"/>	Name	Interface	Loopback ID	Alias	IP Address	Netmask	
<input type="checkbox"/> 	loopback1	Enabled	1	1	255.223.12.11	255.255.255.255	

Max. 4 1 - 1 of 1

UI Setting	Description
<b>Name</b>	Shows the name of the loopback interface the entry is for.
<b>Interface</b>	Shows whether the loopback interface is enabled.
<b>Loopback ID</b>	Shows the ID for the loopback interface.
<b>Alias</b>	Shows the alias for the loopback interface.
<b>IP Address</b>	Shows the IP address for the loopback interface.
<b>Netmask</b>	Shows the netmask for the loopback interface.

## Create Loopback Interface Settings

### Menu Path: Network Interface - Settings

Clicking the **Add (+)** icon in the **Loopback Interface** table on the **Network Interface - Settings** page will open this dialog box. This dialog lets you create a loopback interface.

Click **CREATE** to save your changes and add the new loopback interface.



## Create Loopback Interface Settings

### Create Loopback Interface Settings

Loopback Interface \*

Loopback ID \*


Alias


IP Address \*      Netmask

UI Setting	Description	Valid Range	Default Value
<b>Loopback Interface</b>	Enable or disable the loopback interface.	Enabled / Disabled	Enabled
<b>Loopback ID</b>	Specify the ID for the loopback interface.	1 to 10 characters	N/A
<b>Alias</b>	Specify an alias for the loopback interface.	0 to 64 characters	N/A
<b>IP Address</b>	Specify the IP address for the loopback interface.	Valid IP Address	N/A
<b>Netmask</b>	Shows the netmask for the loopback interface. This is fixed to 255.255.255.255 and cannot be changed.	N/A	N/A

## VLAN Interface Table

VLAN Interface




<input type="checkbox"/>	Name	Interface	VLAN ID	Alias	IP Address	Netmask
<input type="checkbox"/> 	vlan1	Enabled	1		192.168.127.251	255.255.255.0

Max. 256 Items per page: 50 1 - 1 of 1 |< < > >|

UI Setting	Description
<b>Name</b>	Shows the name of the VLAN interface the entry is for.
<b>Interface</b>	Shows whether the VLAN interface is enabled.
<b>VLAN ID</b>	Shows the ID for the VLAN interface.
<b>Alias</b>	Shows the alias for the VLAN interface.
<b>IP Address</b>	Shows the IP address for the VLAN interface.
<b>Netmask</b>	Shows the netmask for the VLAN interface.

## Create VLAN Interface Settings

### Menu Path: Network Interface - Settings

Clicking the **Add** () icon in the **VLAN Interface** table on the **Network Interface - Settings** page will open this dialog box. This dialog lets you create a VLAN interface.

Click **CREATE** to save your changes and add the new VLAN interface.

## Create VLAN Interface Settings

### Create VLAN Interface Settings

VLAN Interface \*  
Enabled

VLAN ID \* i  
1 - 4094

Alias  
0 / 64

IP Address \*      Netmask \* ▼

[CANCEL](#) [CREATE](#)

UI Setting	Description	Valid Range	Default Value
<b>VLAN Interface</b>	Enable or disable the VLAN interface.	Enabled / Disabled	Enabled
<b>VLAN ID</b>	Specify the ID for the VLAN interface.	1 to 4094	N/A
<b>Alias</b>	Specify an alias for the VLAN interface.	0 to 64	N/A
<b>IP Address</b>	Specify the IP address for the VLAN interface.	Valid IP Address	N/A
<b>Netmask</b>	Select a netmask for the VLAN interface.	Drop-down list of netmasks	N/A



## Network Interface - Status


### Menu Path: Network Interface - Status

This page lets you see the status of your network interfaces.

## Loopback Interface List

**Loopback Interface**

 Search



Name	Admin Status	Operation Status	Loopback ID	Alias	IP Address	Netmask
loopback1	Enabled	Up	1	1	255.223.12.11	255.255.255.255


1 - 1 of 1

UI Setting	Description
<b>Name</b>	Shows the name of the loopback interface the entry is for.
<b>Admin Status</b>	Show whether the loopback interface is enabled.
<b>Operation Status</b>	Shows the current operating status of the loopback interface.
<b>Lookback ID</b>	Shows the ID of the loopback interface.
<b>Alias</b>	Shows the alias for the loopback interface.
<b>IP Address</b>	Shows the IP address for the loopback interface.
<b>Netmask</b>	Shows the netmask for the loopback interface.

## VLAN Interface List

**VLAN Interface**

 Search

Name	Admin Status	Operation Status	VLAN ID	Alias	IP Address	Netmask
vlan1	Enabled	Up	1		192.168.127.251	255.255.255.0

1 - 1 of 1

UI Setting	Description
<b>Name</b>	Shows the name of the VLAN interface the entry is for.
<b>Admin Status</b>	Shows whether the VLAN interface is enabled.
<b>Operation Status</b>	Shows the operating status of the VLAN interface.
<b>VLAN ID</b>	Shows the ID for the VLAN interface.
<b>Alias</b>	Shows the alias for the VLAN interface.
<b>IP Address</b>	Shows the IP address for the VLAN interface.
<b>Netmask</b>	Shows the netmask for the VLAN interface.

# Redundancy

## Menu Path: Redundancy

This section lets you configure the redundancy settings for your device.

This section includes these pages:

- Layer 2 Redundancy
- Layer 3 Redundancy
- Tracking

## Redundancy - User Privileges

Privileges to settings are granted to the different authority levels as follows. Refer to [System > Account Management > User Accounts](#) for more information on user accounts.

Settings	Admin	Supervisor	User
<b>Layer 2 Redundancy</b>			
<b>Spanning Tree</b>	R/W	R/W	R
<b>Turbo Ring v2</b>	R/W	R/W	R
<b>Turbo Chain</b>	R/W	R/W	R
<b>MRP</b>	R/W	R/W	R
<b>Multiple Dual Homing</b>	R/W	R/W	R
<b>Multiple Network Coupling</b>	R/W	R/W	R
<b>Layer 3 Redundancy</b>			
<b>VRRP</b>	R/W	R/W	R
<b>Tracking</b>	R/W	R/W	R

# Layer 2 Redundancy

## Menu Path: Redundancy > Layer 2 Redundancy

This section lets you manage the Layer 2 redundancy features of your device.

This section includes these pages:

- Spanning Tree
- Turbo Ring V2
- Turbo Chain
- MRP
- Multiple Dual Homing
- Multiple Network Coupling

## About Spanning Tree

The Spanning Tree Protocol (STP) was designed to help construct a loop-free logical topology on an Ethernet network and provide an automatic means of avoiding any network loops. This is particularly important for networks that have a complicated architecture, since unintended loops in the network can cause broadcast storms. Moxa switches' STP feature is disabled by default. To be completely effective, you must enable STP/RSTP on every Moxa switch connected to your network.

STP (802.1D) is a bridge-based system that is used to implement parallel paths for network traffic. STP uses a loop-detection process to:

- Locate and then disable less efficient paths (e.g., paths that have lower bandwidth).
- Enable one of the less efficient paths if a more efficient path fails.

Rapid Spanning Tree Protocol (RSTP) is an IEEE 802.1w network protocol that enhances the speed and stability of the Spanning Tree Protocol (STP). RSTP promotes high availability and a "loop-free" topology, similar to STP, but more quickly within Ethernet networks. It provides faster convergence and is backward compatible with STP. While STP takes 30-50 seconds to converge, RSTP can achieve sub-second convergence.

For applications that require redundancy, but require use of only open-standard protocols and no proprietary protocols, RSTP is a good choice.

## Difference Between STP and RSTP

RSTP is similar to STP but includes additional information in the BPDUs that allow each bridge to confirm that it has taken action to prevent loops from forming when it decides to enable a link to a neighboring bridge. Adjacent bridges connected via point-to-point links will be able to enable a link without waiting to ensure that all other bridges in the network have had time to react to the change. The main benefit of RSTP is that the configuration decision is made locally rather than network-wide, allowing RSTP to carry out automatic configuration and restore a link faster than STP.

STP and RSTP spanning tree protocols operate without regard to a network's VLAN configuration and maintain one common spanning tree throughout a bridged network. Thus, these protocols map one loop-free, logical topology on a given physical topology.

## About BPDU Guard

BDPUs (Bridge Protocol Data Units) are the network communication frames used in the STP (Spanning Tree Protocol). When two switches exchange messages, BDPUs are used to calculate the STP topology, and determine the network communication route. A BPDU filter is often used to screen sending or receiving BPDUs on a specific port of the switch.

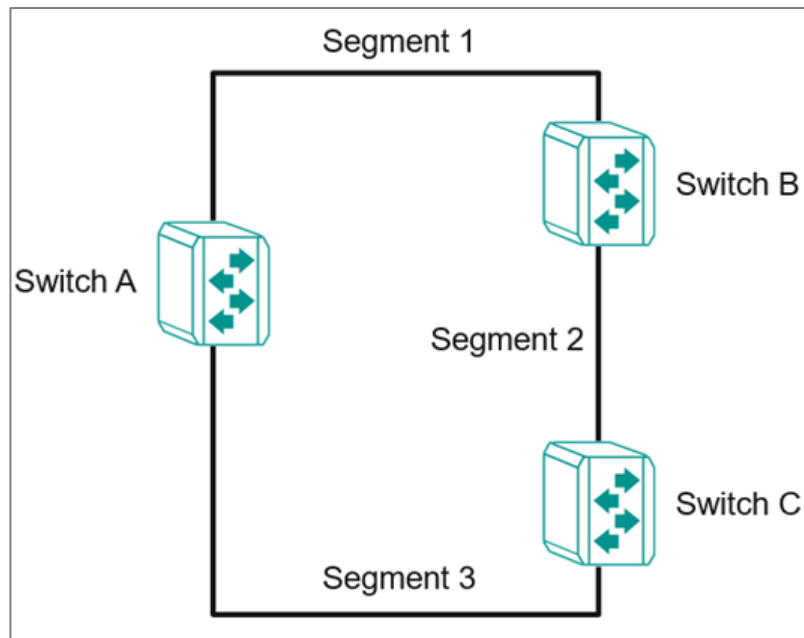
BPDU Guard is a protection mechanism that prevents a port from receiving BPDUs. When an RSTP-enabled port receives BPDUs, it will automatically be in the error-disable state, which means the port will in turn switch to Block state. When STP is enabled, all ports are involved in the STP domain, sending and receiving BPDUs. However, when BPDU Guard is enabled, all ports will not receive or send any BPDUs, as all computers and unmanaged switches do not support STP. When BPDU Guard is enabled, all communications will be treated as error-disabled, and the related ports will be blocked, therefore no more data will be sent or received, protecting the network from a loop chain.

- **Root Guard:** Root Guard prevents a designated port role from changing to root port role on reception of superior information.
- **Loop Guard:** Loop Guard prevents temporary loops in a network caused by **non-designated ports** changing to the spanning-tree **forwarding** state due to a link failure in the topology.
- **BPDU Filter:** BPDU Filter prevents a port from sending and processing BPDUs. A BPDU filter enabled port cannot transmit any BPDUs and drop all received BPDU either.

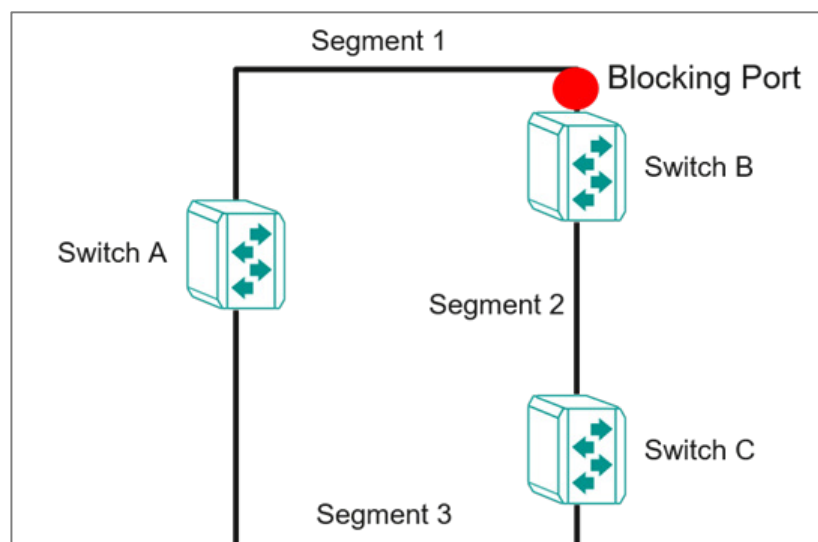


## About STP Operations

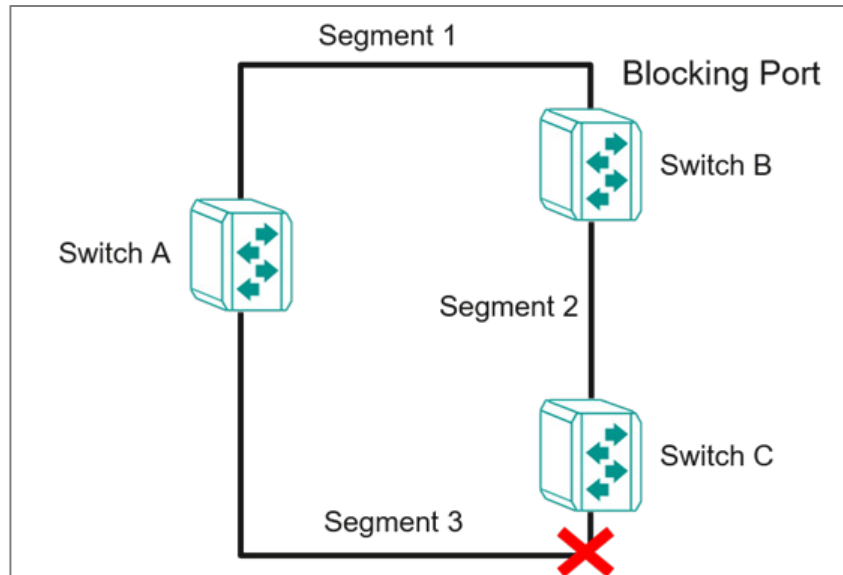
The figure below shows a network made up of three LANs separated by three bridges. Each segment uses at most two paths to communicate with the other segments. Since this configuration can give rise to loops, the network will overload if STP is not enabled.



If STP is enabled, it will detect duplicate paths or block one of the paths from forwarding traffic. In the following example, STP determined that traffic from segment 2 to segment 1 flows through switches C and A since this path is in a forwarding state and is processing BPDUs. However, switch B on segment 1 is in a blocking state.



What happens if a link failure is detected? As shown in the figure below, the STP will change the blocking state to a forwarding state so that traffic from segment 2 flows through switch B to segment 1 through a redundant path.



STP will determine which path between each segment is most efficient, and then assign a specific reference point on the network. When the most efficient path has been identified, the other paths are blocked. In the previous three figures, STP first determined that the path through switch C was the most efficient, and as a result, blocked the path through switch B. After the failure of switch C, STP re-evaluated the situation and opened the path through switch B.

## About RSTP

Rapid Spanning Tree Protocol (RSTP) is an enhancement of the original Spanning Tree Protocol (STP) designed to speed up network convergence and improve overall network performance. RSTP ensures there is only one active path between devices in a network, with backup paths ready to activate if the primary path fails.

Each port is assigned a cost that indicates the efficiency of its link. Typically, this cost is determined by the link's bandwidth, with less efficient links assigned a higher cost.

The RSTP path cost default was originally calculated after detecting the bandwidth as follows.

Link Speed	RSTP/MSTP cost
100 Mbit/s	200,000
1 Gbit/s	20,000
10 Gbit/s	2,000

This can be overwritten from the UI.

### Key Features of RSTP

- **Faster Convergence:** RSTP reduces the time required to detect and respond to network topology changes compared to STP. It eliminates the lengthy listening and learning states of STP, allowing for quicker transitions to active states.
- **Localized Decision-Making:** Unlike STP, where decisions are made network-wide, RSTP enables switches to make local configuration decisions. This allows for faster automatic configuration and quicker restoration of network links.
- **Simplified Port Roles:** RSTP uses only three primary port roles—Root Port, Designated Port, and Alternate Port—streamlining the network’s operation and improving convergence speed.
- **Proposal/Agreement Mechanism:** RSTP introduces the Proposal/Agreement process to quickly determine designated ports during topology changes, further accelerating convergence.

### How RSTP Works

RSTP operates in the following sequence:

1. **Root Bridge Selection:** The switch with the lowest bridge priority or MAC address is designated as the root bridge, forming the base of the spanning tree.
2. **Root Port Selection:** Non-root switches select their root port, which provides the best path to the root bridge based on path cost.
3. **Designated Ports Assignment:** Each network segment designates a port to forward traffic, ensuring optimal paths are used.
4. **Blocking State:** Non-designated or non-root ports remain in a blocking state, preventing loops.

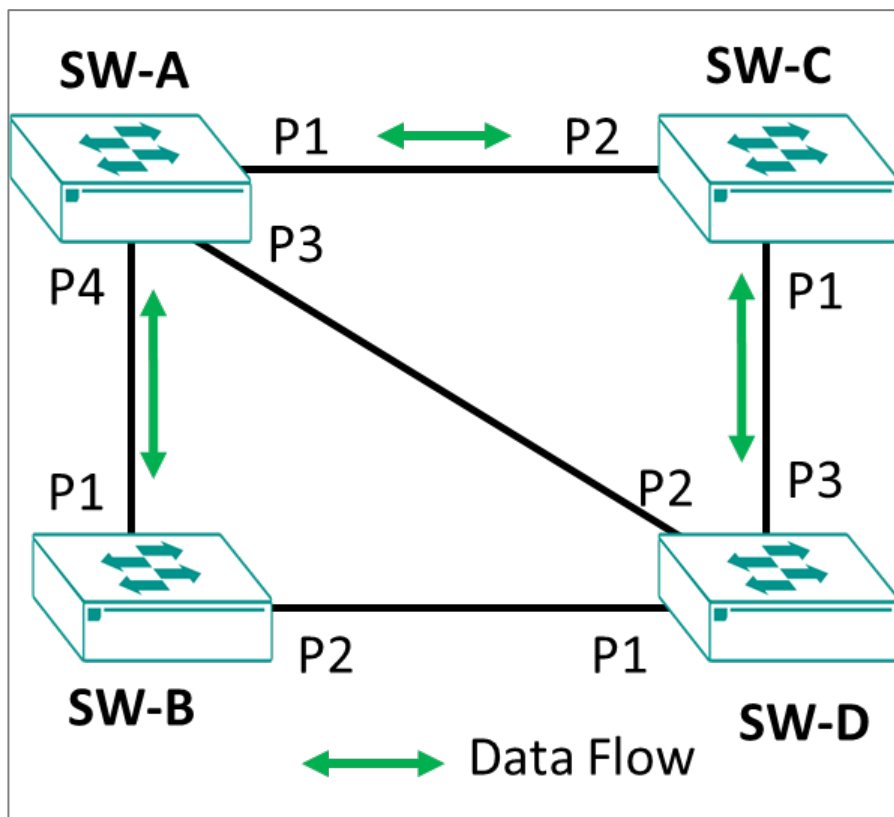
## Benefits of RSTP

- **Improved Network Stability:** RSTP's fast convergence mechanisms reduce the risk of network outages by adapting quickly to changes in the network topology.
- **Backward Compatibility:** RSTP is fully compatible with STP, allowing a smooth transition in mixed networks where some devices still use the older protocol.

Overall, RSTP offers significant improvements over STP, making networks more resilient and responsive to changes, thereby enhancing overall reliability and performance.

## Scenario: Configuring 4 Devices with RSTP

A user wants to configure 4 network devices in an RSTP topology.



Ordinarily, data will flow from SW-A directly to SW-B and SW-C. SW-D data will transit SW-C. However, if something happens that breaks links, data flow can be rerouted without administrator intervention. Follow the subsequent examples to configure each switch.

### Example: Configuring RSTP on SW-A

1. Sign in to the device using administrator credentials.
2. Go to **Redundancy** > **Layer 2 Redundancy** > **Spanning Tree**, and then click **General**.
3. Under **STP Mode**, select **STP/RSTP** from the drop-down list.


If this option was previously **Disabled**, numerous new features will appear.

4. Under **Compatibility**, select **RSTP**.
5. Set **Bridge Priority** to 28672.

This must be lower than other switches on the network to establish SW-A as the root of the topology.


6. Click **Apply** to save your changes.

The list of ports becomes available.

7. Find Port **1/1** on the list of ports, and then click the corresponding  **[Edit]**.


The Edit Port Settings screen appears.

8. Under **Enable**, choose **Enabled** from the drop-down menu.
9. Click **Apply** to save your changes.

10. Find Port **1/3** on the list of ports, and then click the corresponding  **[Edit]**.


The Edit Port Settings screen appears.

11. Under **Enable**, choose **Enabled** from the drop-down menu.
12. Click **Apply** to save your changes.

13. Find Port **1/3** on the list of ports, and then click the corresponding  **[Edit]**.

The Edit Port Settings screen appears.

14. Under **Enable**, choose **Enabled** from the drop-down menu.
15. Click **Apply** to save your changes.

16. Find Port **1/4** on the list of ports, and then click the corresponding  **[Edit]**.

The Edit Port Settings screen appears.

17. Under **Enable**, choose **Enabled** from the drop-down menu.

18. Click **Apply** to save your changes.

SW-A has been configured. You can now move on to configuring SW-B.


### Example: Configuring RSTP on SW-B

1. Sign in to the device using administrator credentials.
2. Go to **Redundancy > Layer 2 Redundancy > Spanning Tree**, and then click **General**.
3. Under **STP Mode**, select **STP/RSTP** from the drop-down list.

If this option was previously **Disabled**, numerous new features will appear.


4. Under **Compatibility**, select **RSTP**.
5. Click **Apply** to save your changes.

The list of ports becomes available.

6. Find Port **1/1** on the list of ports, and then click the corresponding  **[Edit]**.

The Edit Port Settings screen appears.

7. Under **Enable**, choose **Enabled** from the drop-down menu.

8. Find Port **1/2** on the list of ports, and then click the corresponding  **[Edit]**.

The Edit Port Settings screen appears.

9. Under **Enable**, choose **Enabled** from the drop-down menu.
10. Click **Apply** to save your changes.

SW-B has been configured. You can now move on to configuring SW-C.

### Example: Configuring RSTP on SW-C


1. Sign in to the device using administrator credentials.
2. Go to **Redundancy > Layer 2 Redundancy > Spanning Tree**, and then click **General**.

3. Under **STP Mode**, select **STP/RSTP** from the drop-down list.


If this option was previously **Disabled**, numerous new features will appear.

4. Under **Compatibility**, select **RSTP**.
5. Click **Apply** to save your changes.

The list of ports becomes available.

6. Find Port **1/1** on the list of ports, and then click the corresponding  **[Edit]**.

7. Under **Enable**, choose **Enabled** from the drop-down menu.

8. Find Port **1/2** on the list of ports, and then click the corresponding  **[Edit]**.

The Edit Port Settings screen appears.

9. Under **Enable**, choose **Enabled** from the drop-down menu.
10. Click **Apply** to save your changes.

SW-C has been configured. You can now move on to configuring SW-D.

### **Example: Configuring RSTP on SW-D**


SW-D requires specific configuration to ensure that the correct paths are followed.

1. Sign in to the device using administrator credentials.
2. Go to **Redundancy > Layer 2 Redundancy > Spanning Tree**, and then click **General**.
3. Under **STP Mode**, select **STP/RSTP** from the drop-down list.

If this option was previously **Disabled**, numerous new features will appear.

4. Under **Compatibility**, select **RSTP**.
5. Click **Apply** to save your changes.

The list of ports becomes available.


6. Find Port **1/1** on the list of ports, and then click the corresponding  **[Edit]**.

The Edit Port Settings screen appears.

7. Under **Enable**, choose **Enabled** from the drop-down menu.

8. Verify that there is a value in the **Path Cost** field. If there is no value, enter a tentative value of 20,000.

9. Click **Apply** to save your changes.


10. Find Port **1/4** on the list of ports, and then click the corresponding  **[Edit]**.

The Edit Port Settings screen appears.

11. Under **Enable**, choose **Enabled** from the drop-down menu.

12. Verify that there is a value in the **Path Cost** field. If there is no value, enter a tentative value of 20,000.

13. Click **Apply** to save your changes.

14. Find Port **1/4** on the list of ports, and then click the corresponding  **[Edit]**.

15. Under **Enable**, choose **Enabled** from the drop-down menu.

16. Set **Path Cost** to 0.

17. Click **Apply** to save your changes.

With SW-D completed, all devices in the topology are complete.

## Spanning Tree Settings

### Menu Path: Redundancy > Spanning Tree

This page lets you configure the spanning tree settings of your device.

This page includes these tabs:

- General
- Guard
- Status

### Spanning Tree - General

#### Menu Path: Redundancy > Spanning Tree - General

This page lets you configure the STP mode and its related settings.



## Spanning Tree Settings - STP/RSTP

If **STP Mode** is set to **STP/RSTP**, the following settings will appear.

STP Mode *	Compatibility *	Bridge Priority *	
STP/RSTP	RSTP	32768	
		0 - 61440, Multiples of 4096	
Forward Delay Time *	Hello Time *	Max. Age *	Error Recovery Time *
15	2	20	300
4 - 30	sec. 1 - 2	sec. 6 - 40	sec. 30 - 65535
<b>APPLY</b>			

UI Setting	Description	Valid Range	Default Value
<b>STP Mode</b>	Specify the spanning tree protocol (STP) to use.	Disabled / STP/RSTP/ MSTP	Disabled
	<div style="background-color: #f0f0f0; padding: 10px;"> <p><b>Note</b></p> <p>MSTP and GVRP are both VLAN-related functions. When VLAN changes dynamically, MSTP needs to re-converge, which can make the system unstable due to running complex operations. When both MSTP and GVRP are used together, this can result in network instability.</p> <p>Therefore, it is recommended that network administrators avoid enabling both MSTP and GVRP.</p> </div>		
<b>Compatibility</b>	Specify the compatibility mode to use.	STP / RSTP	RSTP
<b>Bridge Priority</b>	Specify the bridge priority number, which must be a multiple of 4096. Lower numbers have higher priority. A device with a higher bridge priority (e.g., a lower value) has a greater chance of being established as the root of the spanning tree topology.	Multiples of 4096 from 0 to 61440	32768
<b>Forward Delay Time</b>	Specify the amount of time in seconds the device waits before checking to see if it should change to a different state.	4 to 30	15
<b>Hello Time</b>	Specify the hello time in seconds. This is the amount of time the root waits between sending hello messages. The root of the spanning tree topology periodically sends out a "hello" message to other devices on the network to check if the topology is healthy.	1 to 2	2
<b>Max. Age</b>	Specify the max age in seconds. If this device is not the root, and it has not received a hello message from the root for longer than the max age time, then this device will reconfigure itself as a root. Once two or more devices on the network are recognized as a root, the devices will renegotiate a new spanning tree topology.	6 to 40	20

UI Setting	Description	Valid Range	Default Value
<b>Error Recovery Time</b>	Specify the error recovery time in seconds. If BPDU guard is triggered on a port, it will automatically recover to the normal state after the error recovery time.	30 to 65535	300

## STP/RSTP - Port Table

If **STP Mode** is set to **STP/RSTP**, this table will appear.

Port	Enable	Edge	Priority	Path Cost	Link Type
1	Enabled	Auto	128	0	Auto
2	Disabled	Auto	128	0	Auto
3	Disabled	Auto	128	0	Auto
4	Disabled	Auto	128	0	Auto
5	Disabled	Auto	128	0	Auto
6	Disabled	Auto	128	0	Auto
7	Disabled	Auto	128	0	Auto
8	Disabled	Auto	128	0	Auto
9	Disabled	Auto	128	0	Auto

1 - 23 of 23

UI Setting	Description
<b>Port</b>	Shows the port number the entry is for.
<b>Enable</b>	Shows whether the spanning tree protocol is enabled for the port.
<b>Edge</b>	Shows the current edge port configuration for the port.
<b>Priority</b>	Show the bridge priority number for the port.
<b>Path Cost</b>	Show the path cost value for the port.
<b>Link Type</b>	Show the link type configuration for the port.

## STP/RSTP Port Table - Edit Port Settings

### Menu Path: Redundancy > Spanning Tree - General

Clicking the **Edit** (✎) icon for an port on the **Redundancy > Spanning Tree - General** page will open this dialog box. This dialog lets you edit the STP/RSTP settings for the port.

Click **APPLY** to save your changes.

UI Setting	Description	Valid Range	Default Value
<b>Enable</b>	Enable or disable spanning tree protocol for the port.	Enabled / Disabled	Disabled
<b>Edge</b>	Select the edge port configuration for the port. <ul style="list-style-type: none"> <li><b>Auto:</b> Auto-detect whether to configure the port as an edge port.</li> <li><b>Yes:</b> The port will be configured as an edge port.</li> <li><b>No:</b> The port will not be configured as an edge port.</li> </ul>	Auto / Yes / No	Auto
<b>Priority</b>	Specify the priority of the port as a multiple of 16. Lower numbers have higher priority. A port with a higher priority (e.g., a lower value) has a greater chance of being a root port.	Multiples of 16 from 0 to 240	128
<b>Path Cost</b>	Specify the path cost value. If this is set to 0, the path cost value will be automatically assigned according to the port speed.	0 to 20000000	0

UI Setting	Description	Valid Range	Default Value
<b>Link Type</b>	Select the link type for the port. <ul style="list-style-type: none"> <li><b>Point-to-point:</b> Use this when the port is operating in full-duplex mode.</li> <li><b>Shared:</b> Use this when the port is operating in half-duplex mode.</li> <li><b>Auto:</b> Auto-detect which mode to use for the port.</li> </ul>	Point-to-point / Shared / Auto	Auto
<b>Copy configurations to ports</b>	Select the ports you want to copy this configuration to.	Drop-down list of ports	N/A

## Spanning Tree Settings - MSTP

If **STP Mode** is set to **MSTP**, the following settings will appear.

STP Mode *	Compatibility *		
MSTP	MSTP		
Forward Delay Time *	Hello Time *	Max. Age *	Error Recovery Time *
15	2	20	300
4 - 30 sec.	1 - 2 sec.	6 - 40 sec.	30 - 65535 sec.
Region Name	Region Revision *	Max. Hops *	
MSTP	0	20	
	4 / 32	0 - 65535	6 - 40
<b>APPLY</b>			

UI Setting	Description	Valid Range	Default Value
<b>STP Mode</b>	Specify the spanning tree protocol (STP) to use.	Disabled / STP/RSTP/ MSTP	Disabled
	<div style="background-color: #f0f0f0; padding: 10px; border: 1px solid #ccc;"> <p><b>Note</b></p> <p>MSTP and GVRP are both VLAN-related functions. When VLAN changes dynamically, MSTP needs to re-converge, which can make the system unstable due to running complex operations. When both MSTP and GVRP are used together, this can result in network instability.</p> <p>Therefore, it is recommended that network administrators avoid enabling both MSTP and GVRP.</p> </div>		
<b>Compatibility</b>	Specify the compatibility mode to use.	RSTP / STP / MSTP	MSTP

UI Setting	Description	Valid Range	Default Value
<b>Forward Delay Time</b>	Specify the amount of time in seconds the device waits before checking to see if it should change to a different state.	4 to 30	15
<b>Hello Time</b>	Specify the hello time in seconds. This is the amount of time the root waits between sending hello messages. The root of the spanning tree topology periodically sends out a "hello" message to other devices on the network to check if the topology is healthy.	1 to 2	2
<b>Max. Age</b>	Specify the max age in seconds. If this device is not the root, and it has not received a hello message from the root for longer than the max age time, then this device will reconfigure itself as a root. Once two or more devices on the network are recognized as a root, the devices will renegotiate a new spanning tree topology.	6 to 40	20
<b>Error Recovery Time</b>	Specify the error recovery time in seconds. If BPDU guard is triggered on a port, it will automatically recover to the normal state after the error recovery time.	30 to 65535	300
<b>Region Name</b>	Specify the MSTP region name.	0 to 32 characters	MSTP
<b>Region Revision</b>	Specify the MSTP region revision.	0 to 65535	0
<b>Max. Hops</b>	Specify the maximum number of hops allowed.	6 to 40	20

## MSTP - Instance List

If **STP Mode** is set to **MSTP**, the following table will appear.

Instance ID	VLAN List	Bridge Priority
<input type="checkbox"/> CIST	Other VLANs	32768

UI Setting	Description
<b>Instance ID</b>	Shows the of the instance the entry is for.

UI Setting	Description
<b>VLAN List</b>	Show the VLAN list configured for the instance.
<b>Bridge Priority</b>	Show the bridge priority value for the instance.

## Instance List - Create Instance

### Menu Path: Redundancy > Spanning Tree - General

Clicking the **Add (+)** icon on the **Redundancy > Spanning Tree - General** page will open this dialog box. This dialog lets you create an MSTP instance.

Click **APPLY** to save your changes.

**Create Instance**

Instance ID \*

VLAN List \*  i

Bridge Priority \*   
0 - 61440, Multiples of 4096

CANCEL
APPLY

UI Setting	Description	Valid Range	Default Value
<b>Instance ID</b>	Select an ID for the instance.	Drop-down list of ID numbers.	N/A
<b>VLAN List</b>	Specify the VLAN IDs to use for the instance. You can enter multiple VLAN IDs by separating them with commas or by using ranges (e.g., 2, 4-8, 10-13).	Valid VLAN IDs	N/A
<b>Bridge Priority</b>	Specify the bridge priority value for the instance as a multiple of 4096. Lower values have higher priority.	Multiples of 4096 from 0 - 61440	N/A

## Instance List - Edit Settings

### Menu Path: Redundancy > Spanning Tree - General

Clicking the **Edit** (✎) icon for an instance on the **Redundancy > Spanning Tree - General** page will open this dialog box. This dialog lets you edit the instance settings.

Click **APPLY** to save your changes.

### Edit CIST Settings

Bridge Priority \*

32768

0 - 61440, Multiples of 4096

CANCEL APPLY

### Edit Instance 1 Settings

VLAN List \*

12 i

Bridge Priority \*

4096

0 - 61440, Multiples of 4096

CANCEL APPLY

UI Setting	Description	Valid Range	Default Value
<b>VLAN List</b>	Specify the VLAN IDs to use for the instance. You can enter multiple VLAN IDs by separating them with commas or by using ranges (e.g., 2, 4-8, 10-13).	N/A	N/A
	<p><span style="font-size: 0.8em;">✎</span> <b>Note</b></p> <p>This setting is not available for the CIST instance.</p>		
<b>Bridge Priority</b>	Specify the bridge priority value for the instance as a multiple of 4096. Lower values have higher priority.	Multiples of 4096 from 0 - 61440	32768 for CIST N/A for other instances

## Spanning Tree - Port Table

If **STP Mode** is set to **MSTP**, the following table will appear. Clicking on the drop-down list at the top left will let you select which instance's port table you want to view.

<input type="checkbox"/>	Port	Enable	Edge	Priority	Path Cost	Link Type
<input type="checkbox"/>	1	Disabled	Auto	128	0	Auto
<input type="checkbox"/>	2	Disabled	Auto	128	0	Auto
<input type="checkbox"/>	3	Disabled	Auto	128	0	Auto
<input type="checkbox"/>	4	Disabled	Auto	128	0	Auto
<input type="checkbox"/>	5	Disabled	Auto	128	0	Auto
<input type="checkbox"/>	6	Disabled	Auto	128	0	Auto
<input type="checkbox"/>	7	Disabled	Auto	128	0	Auto
<input type="checkbox"/>	8	Disabled	Auto	128	0	Auto
<input type="checkbox"/>	9	Disabled	Auto	128	0	Auto

UI Setting	Description
<b>Port</b>	Shows the port number the entry is for.
<b>Enable</b>	Shows whether the spanning tree protocol is enabled for the port.
<b>Edge</b>	Shows the current edge port configuration for the port.
<b>Priority</b>	Show the bridge priority number for the port.
<b>Path Cost</b>	Show the path cost value for the port.
<b>Link Type</b>	Show the link type configuration for the port.



## MSTP Port Table - Edit Port Settings

### Menu Path: Redundancy > Spanning Tree - General

Clicking the **Edit** (✎) icon for an port on the **Redundancy > Spanning Tree - General** page will open this dialog box. This dialog lets you edit the port's settings for the selected instance.

Click **APPLY** to save your changes.

**Edit CIST Port 1 Settings**

Enable \*  
Disabled

Edge \*  
Auto

Priority \*  
128  
0 - 240, Multiples of 16

Path Cost \*  
0  
0 - 200000000

Link Type \*  
Auto

Copy configurations to ports

CANCEL APPLY










UI Setting	Description	Valid Range	Default Value
<b>Enable</b>	Enable or disable spanning tree protocol for the port.	Enabled / Disabled	Disabled
<b>Edge</b>	Select the edge port configuration for the port. <ul style="list-style-type: none"><li>• <b>Auto:</b> Auto-detect whether to configure the port as an edge port.</li><li>• <b>Yes:</b> The port will be configured as an edge port.</li><li>• <b>No:</b> The port will not be configured as an edge port.</li></ul>	Auto / Yes / No	Auto

UI Setting	Description	Valid Range	Default Value
<b>Priority</b>	Specify the priority of the port as a multiple of 16. Lower numbers have higher priority. A port with a higher priority (e.g., a lower value) has a greater chance of being a root port.	Multiples of 16 from 0 to 240	128
<b>Path Cost</b>	Specify the path cost value. If this is set to 0, the path cost value will be automatically assigned according to the port speed.	0 to 20000000	0
<b>Link Type</b>	Select the link type for the port. <ul style="list-style-type: none"> <li><b>Point-to-point:</b> Use this when the port is operating in full-duplex mode.</li> <li><b>Shared:</b> Use this when the port is operating in half-duplex mode.</li> <li><b>Auto:</b> Auto-detect which mode to use for the port.</li> </ul>	Point-to-point / Shared / Auto	Auto
<b>Copy configurations to ports</b>	Select the ports you want to copy this configuration to.	Drop-down list of ports	N/A

## Spanning Tree - Guard

### Menu Path: Redundancy > Spanning Tree - Guard

This page lets you configure BPDU Guard by port.

Q Search					
Port	BPDU Guard	rootGuard	Loop Guard	BPDU Filter	
 1	Disabled	Disabled	Disabled	Disabled	
 2	Disabled	Disabled	Disabled	Disabled	
 3	Disabled	Disabled	Disabled	Disabled	
 4	Disabled	Disabled	Disabled	Disabled	
 5	Disabled	Disabled	Disabled	Disabled	
 6	Disabled	Disabled	Disabled	Disabled	
 7	Disabled	Disabled	Disabled	Disabled	
 8	Disabled	Disabled	Disabled	Disabled	
 9	Disabled	Disabled	Disabled	Disabled	

1 - 23 of 23

UI Setting	Description
<b>Port</b>	Shows the port number the entry is for.
<b>BPDU Guard</b>	Show whether BPDU Guard is enabled for the port.
<b>Root Guard</b>	Show whether Root Guard is enabled for the port.
<b>Loop Guard</b>	Show whether Loop Guard is enabled for the port.
<b>BPDU Filter</b>	Show whether the BPDU Filter is enabled for the port.

## BPDU Guard - Edit Port Settings

### Menu Path: Redundancy > Spanning Tree - Guard

Clicking the **Edit** (✎) icon for a port on the **Redundancy > Spanning Tree - Guard** page will open this dialog box. This dialog lets you edit the BPDU settings for the port.

Click **APPLY** to save your changes.

### Edit Port 1 Settings

BPDU Guard \*

Root Guard \*

Loop Guard \*

BPDU Filter \*

Copy configurations to ports  ⓘ

UI Setting	Description	Valid Range	Default Value
<b>BPDU Guard</b>	Enable/disable BPDU Guard on the port.	Enabled / Disabled	Disabled

UI Setting	Description	Valid Range	Default Value
<b>Root Guard</b>	Enable/disable Root Guard on the port.	Enabled / Disabled	Disabled
<b>Loop Guard</b>	Enable/disable Loop Guard on the port.	Enabled / Disabled	Disabled
<b>BDPU Filter</b>	Enable/disable BPDU Filter on the port.	Enabled / Disabled	Disabled
<b>Copy configurations to ports</b>	Select the ports you want to copy this configuration to.	Drop-down list of ports	N/A

## Spanning Tree - Status

### Menu Path: Redundancy > Spanning Tree - Status

This page lets you view the current spanning tree status of your device.

### Root Information

If **STP Mode** is set to **STP/RSTP**, this display will appear.

#### Root Information ↻

Bridge ID  
**32768/00:90:e8:b1:01:01**

Root Path Cost  
**0**

Forward Delay Time  
**15 (sec.)**

Hello Time  
**2 (sec.)**

Max. Age  
**20 (sec.)**

UI Setting	Description
<b>Bridge ID</b>	Shows the bridge ID.
<b>Root Path Cost</b>	Shows the root path cost.

UI Setting	Description
<b>Forward Delay Time</b>	Shows the forward delay time in seconds.
<b>Hello Time</b>	Shows the hello time in seconds.
<b>Max. Age</b>	Shows the max. age time in seconds.

## Bridge Information

If **STP Mode** is set to **STP/RSTP**, this display will appear.

### Bridge Information ↻

Bridge ID  
**32768/00:90:E8:B1:01:01**

Running Protocol  
**RSTP**

Forward Delay Time  
**15 (sec.)**

Hello Time  
**2 (sec.)**

Max. Age  
**20 (sec.)**

UI Setting	Description
<b>Bridge ID</b>	Shows the bridge ID.
<b>Running Protocol</b>	Shows the current configured spanning tree protocol.
<b>Forward Delay Time</b>	Shows the forward delay time in seconds.
<b>Hello Time</b>	Shows the hello time in seconds.
<b>Max. Age</b>	Shows the max. age time in seconds.

## Spanning Tree - Port Status

If **STP Mode** is set to **STP/RSTP**, the following table will appear.

↻ 🏠
🔍 Search

Port	Edge	Port Role	Port State	Root Path Cost	Path Cost	Link Type
1	No	Disabled	Discarding	0	20000	Point-to-point
2	No	Disabled	Forwarding	0	200000	Point-to-point
3	No	Disabled	Discarding	0	20000	Point-to-point
4	No	Disabled	Discarding	0	20000	Point-to-point
5	No	Disabled	Discarding	0	20000	Point-to-point
6	No	Disabled	Discarding	0	20000	Point-to-point
7	No	Disabled	Discarding	0	20000	Point-to-point
8	No	Disabled	Discarding	0	20000	Point-to-point
9	No	Disabled	Discarding	0	20000	Point-to-point
10	No	Disabled	Discarding	0	20000	Point-to-point
11	No	Disabled	Discarding	0	20000	Point-to-point
12	No	Disabled	Discarding	0	20000	Point-to-point
13	No	Disabled	Discarding	0	20000	Point-to-point


1 – 16 of 16

UI Setting	Description
<b>Port</b>	Shows the port number the entry is for.
<b>Edge</b>	Shows whether this port is connected to an edge device.
<b>Port Role</b>	Shows the role for the port. <ul style="list-style-type: none"> <li><b>Root:</b> The port is connected directly or indirectly to the root device.</li> <li><b>Designated:</b> The port is designated if it can send the best BPDU on the segment to which it is connected.</li> <li><b>Alternate:</b> The alternate port receives more useful BPDU from another bridge and is a blocked port.</li> <li><b>Backup:</b> The backup port receives more useful BPDU from the same bridge and is a blocked port.</li> <li><b>Disabled:</b> The port is disabled.</li> </ul>

UI Setting	Description
<b>Port State</b>	Show the port state. <ul style="list-style-type: none"> <li>• <b>Forwarding</b>: Traffic can be forwarded through this port.</li> <li>• <b>Blocked</b>: Traffic will be blocked.</li> <li>• <b>Disabled</b>: The port is disabled.</li> </ul>
<b>Root Path Cost</b>	Shows the total path cost to the root bridge for the port.
<b>Path Cost</b>	Shows the path cost for the port.
<b>Link Type</b>	Show the link type for the port. <ul style="list-style-type: none"> <li>• <b>Edge Port</b>: The port is connected to an edge device.</li> <li>• <b>Point-to-point</b>: The port is connected to another bridge and is full duplex.</li> <li>• <b>Shared</b>: The port is connected to another bridge and is half duplex.</li> </ul>

## General Information

If **STP Mode** is set to **MSTP**, this display will appear.

General Information 			
Running Protocol	Forward Delay Time	Hello Time	Max. Age
MSTP	15 (sec.)	2 (sec.)	20 (sec.)

UI Setting	Description
<b>Running Protocol</b>	Shows the current configured spanning tree protocol.
<b>Forward Delay Time</b>	Shows the forward delay time in seconds.
<b>Hello Time</b>	Shows the hello time in seconds.
<b>Max. Age</b>	Shows the max. age time in seconds.

## Spanning Tree - Port Status

If **STP Mode** is set to **MSTP**, the following table will appear.

You can use the drop-down list at the top-left to select which instance's status you want to view.

Information of CIST ▾ ⌵

Bridge ID: 32768/00:90:e8:b1:01:01    Regional Root ID: 32768/00:90:e8:b1:01:01    CIST Root ID: 32768/00:90:e8:b1:01:01    CIST Path Cost: 0

Port Status Q Search

Port	Edge	Port Role	Port State	Root Path Cost	Path Cost	Link Type	BPDU Inconsistency	Root Inconsistency	Loop Inconsistency
1	No	Disabled	Discarding	0	20000	Point-to-point	No	No	No
2	No	Disabled	Forwarding	0	200000	Point-to-point	No	No	No
3	No	Disabled	Discarding	0	20000	Point-to-point	No	No	No
4	No	Disabled	Discarding	0	20000	Point-to-point	No	No	No
5	No	Disabled	Discarding	0	20000	Point-to-point	No	No	No
6	No	Disabled	Discarding	0	20000	Point-to-point	No	No	No
7	No	Disabled	Discarding	0	20000	Point-to-point	No	No	No
8	No	Disabled	Discarding	0	20000	Point-to-point	No	No	No

## Information of Instance

When viewing the CIST instance, this information will appear:

UI Setting	Description
<b>Bridge ID</b>	Shows the bridge ID for the CIST instance.
<b>Regional Root ID</b>	Shows the regional root ID for the CIST instance.
<b>CIST Root ID</b>	Shows the bridge ID for the CIST instance.
<b>CIST Path Cost</b>	Shows the bridge ID for the CIST instance.

When viewing an instance other than the CIST instance, this information will appear:

UI Setting	Description
<b>Bridge ID</b>	Shows the bridge ID for the instance.
<b>VLAN List</b>	Shows the VLAN IDs for the instance.
<b>Designated Root ID</b>	Shows the designated root ID for the instance.
<b>Root Path Cost</b>	Shows the root path cost for the instance.



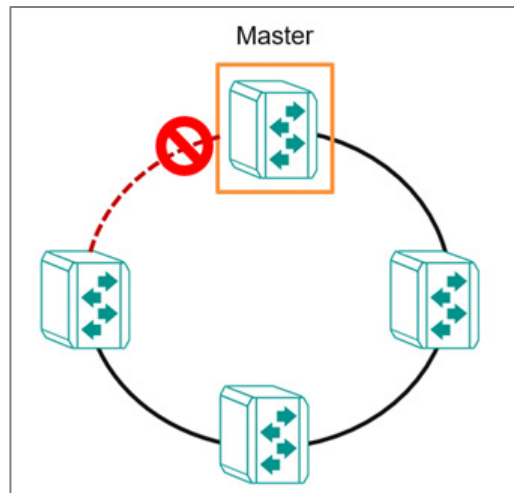
## Port Status

UI Setting	Description
<b>Port</b>	Shows the port number the entry is for.
<b>Edge</b>	Shows whether this port is connected to an edge device.
<b>Port Role</b>	Shows the role for the port. <ul style="list-style-type: none"><li>• <b>Root:</b> The port is connected directly or indirectly to the root device.</li><li>• <b>Designated:</b> The port is designated if it can send the best BPDU on the segment to which it is connected.</li><li>• <b>Alternate:</b> The alternate port receives more useful BPDU from another bridge and is a blocked port.</li><li>• <b>Backup:</b> The backup port receives more useful BPDU from the same bridge and is a blocked port.</li><li>• <b>Disabled:</b> MSTP is disabled for the port.</li></ul>
<b>Port State</b>	Show the port state. <ul style="list-style-type: none"><li>• <b>Forwarding:</b> Traffic can be forwarded through this port.</li><li>• <b>Blocked:</b> Traffic will be blocked.</li><li>• <b>Disabled:</b> The port is disabled.</li></ul>
<b>Root Path Cost</b>	Shows the total path cost to the root bridge for the port.
<b>Path Cost</b>	Shows the path cost for the port.
<b>Link Type</b>	Show the link type for the port. <ul style="list-style-type: none"><li>• <b>Edge Port:</b> The port is connected to an edge device.</li><li>• <b>Point-to-point:</b> The port is connected to another bridge and is full duplex.</li><li>• <b>Shared:</b> The port is connected to another bridge and is half duplex.</li></ul>
<b>BPDU Inconsistency</b>	Shows whether BPDU is received on a port enabled by a BPDU guard.
<b>Root Inconsistency</b>	Shows whether the port is changed to a root port when enabled by a loop guard.
<b>Loop Inconsistency</b>	Shows whether a loop is detected on this port by a loop guard.

## About Turbo Ring v2

Turbo Ring v2 is a high-performance, redundant network topology developed by Moxa for configuring network devices in redundant loops.

In the event of a link failure, the network can automatically reconfigure itself to maintain uninterrupted communication. Recovery times are within 20 ms for Fast Ethernet and 50 ms for Gigabit Ethernet on a network of up to 250 nodes.



Turbo Ring v2 allows connected network devices to elect a "master" switch, which blocks packets from traveling through any of the network's redundant loops and manages the network. If a section breaks, the protocol adjusts the ring so that the disconnected parts of the network establish contact. This enables continuous network operations, even when there is a fault in the network.

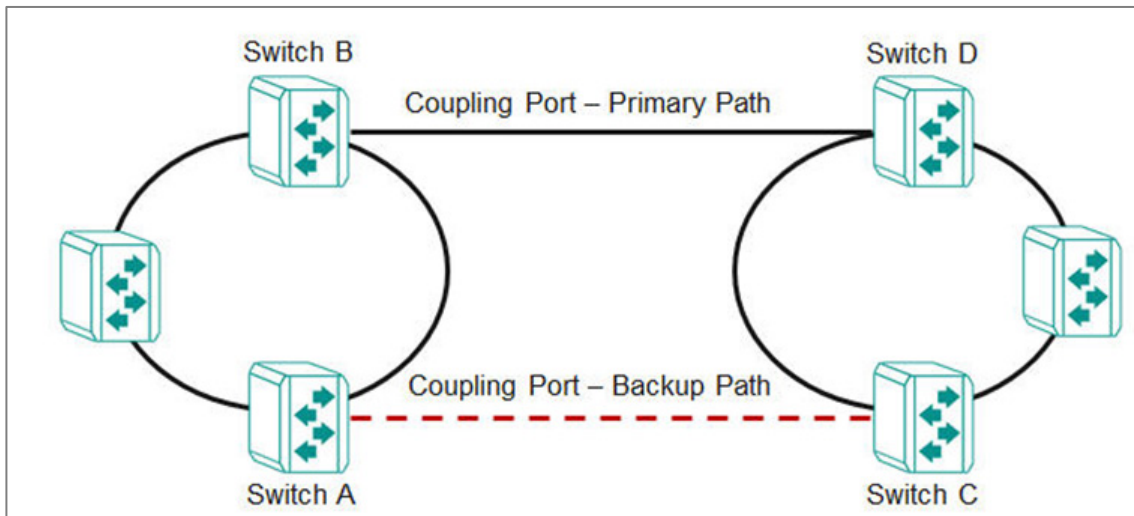
Furthermore, the election mechanism is redundant. If the "master" device itself fails, the network devices detect the failure and automatically elect another. The process occurs quickly, ensuring no interruption.

Turbo Ring v2 supports a backup segment connected to the redundant port (secondary port) on the ring "master". In this case, the backup path is easily identifiable for troubleshooting and replacement.

## About Ring Coupling

Ring Coupling refers to the practice of coupling two rings together.

This may be useful when creating a large redundant ring is inconvenient or impractical, such as for devices in remote areas. Smaller redundant rings can be coupled together for inter-ring communication while still maintaining redundancy of constituent rings and couplings.



Ring coupling uses extra ports on each pair of coupled switches. In this example, that means:

- The (Primary) coupling port on Switch B monitors the main path and connects directly to the port on Switch D.
- The (Backup) coupling port on Switch A monitors the main path and connects directly to the port on Switch C.

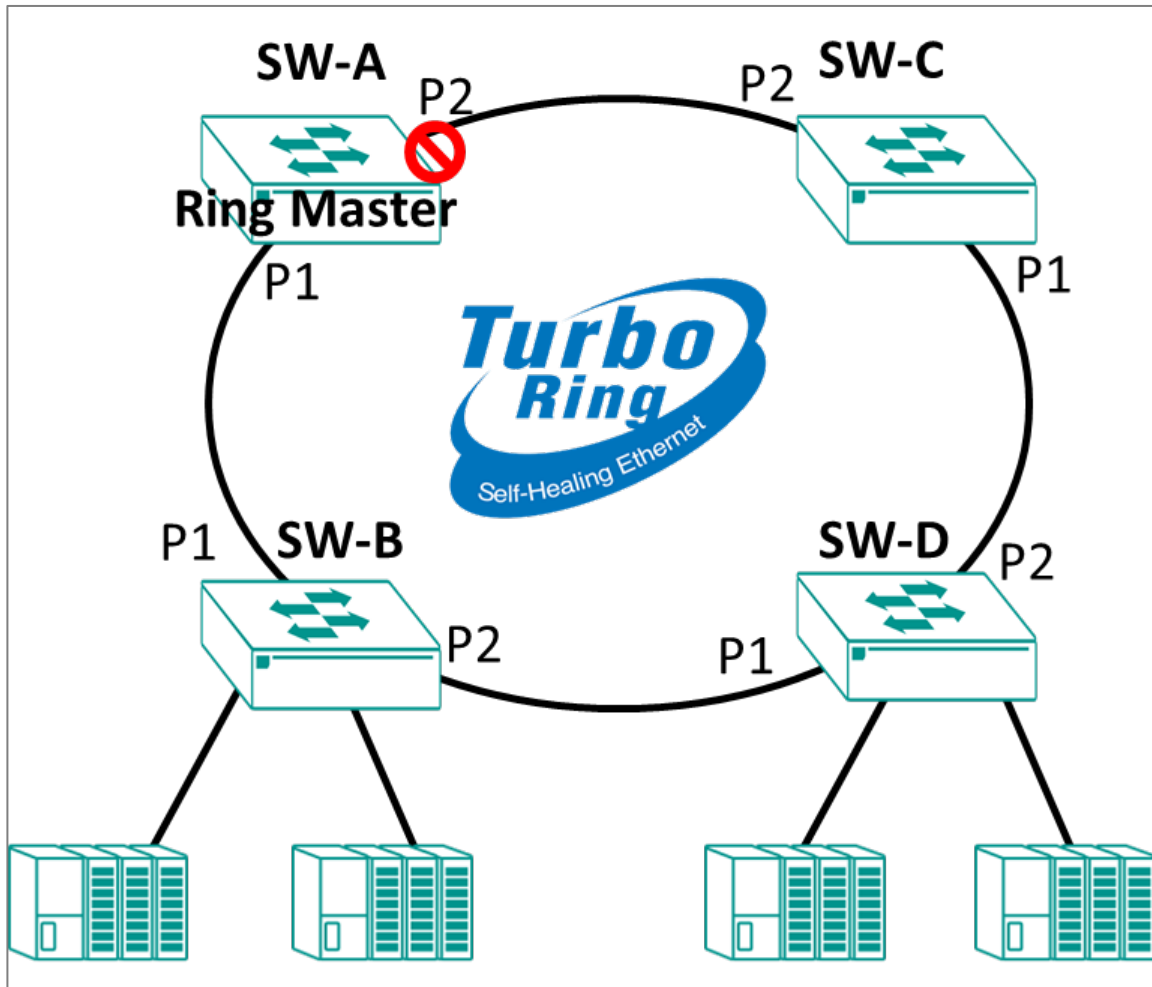
**Note**

Only one coupling (primary + backup) per ring pair.

### Scenario: Using Turbo Ring in a Manufacturing Plant

In this scenario, we describe a factory using a simple ring topology.

A manufacturing plant has a complex network of machines and devices that communicate with each other to keep the production line running smoothly. To ensure that the network remains stable and reliable, the plant needs to use Turbo Ring v2 to create a fault-tolerant network by forming a ring topology.



Set up Turbo Ring v2 to connect multiple networks of machines and devices to create a fault-tolerant network and achieve continuous operations.

Ensure that switches are installed and powered. Wait to connect them until the end.

To configure this scenario, do the following:

1. Configure the settings each network device for Turbo Ring v2.

See the subsequent sections for details about how to configure each device.


2. Connect the network devices in a ring topology, using ports 1 and 2 for ring segments.

If the master network device fails, the other devices in the ring will automatically detect the problem and initiate a new election process to select a new master switch, ensuring that there is no significant interruption in communication.

## Example: Configuring the Master for Turbo Ring v2 in a Manufacturing Plant

Configure the device labeled SW-A for Turbo Ring v2 in our factory example.

Make sure you have NOT connected the ring ports until after you configure Turbo Ring v2 settings. Our examples use ports **1/1** and **1/2** as ring ports.

1. Sign in to the device using administrator credentials.
2. Go to **Redundancy > Layer 2 Redundancy > Turbo Ring V2**, and then click **Settings**.
3. Set **Turbo Ring V2** to **Enabled**.
4. Under Ring Settings, next to **Ring 1**, click  **[Edit]**.

The Ring 1 Settings screen appears.

5. Configure all of the following:

Option	Value
<b>Enabled</b>	<b>Enabled</b>
<b>Master</b>	<b>Enabled</b>
<b>Ring Port 1</b>	<b>1/1</b>
<b>Ring Port 2</b>	<b>1/2</b>

Setting **Master** on multiple devices (or no devices) will have the following effects:

Master Setting	Result
<b>Multiple devices set to Enabled</b>	Ring election based on MAC addresses of <b>Enabled</b> devices
<b>No devices set to Enabled</b>	Ring election based on MAC addresses of all devices
<b>Single device set to Enabled</b>	<b>Enabled</b> device always master, failure of <b>Enabled</b> device results in ring election


6. Click **Apply** to save your changes.

Repeat this step on devices SW-B, SW-C, and SW-D, but with the **Master** setting set to **Disabled**. This process is outlined in the subsequent section.

## Example: Configuring Non-Master Network Devices for Turbo Ring v2 in a Manufacturing Plant

Follow these steps to configure devices SW-B through SW-D in our scenario.

Make sure you have NOT connected the ring ports until after you configure Turbo Ring v2 settings. Our examples use ports **1/1** and **1/2** as ring ports.

1. Sign in to the device using administrator credentials.
2. Go to **Redundancy > Layer 2 Redundancy > Turbo Ring V2**, and then click **Settings**.
3. Set **Turbo Ring V2** to **Enabled**.
4. Under Ring Settings, next to **Ring 1**, click  **[Edit]**.

The Ring 1 Settings screen appears.

5. Configure all of the following:

Option	Value
<b>Enabled</b>	<b>Enabled</b>
<b>Master</b>	<b>Disabled</b>
<b>Ring Port 1</b>	<b>1/1</b>
<b>Ring Port 2</b>	<b>1/2</b>

Setting **Master** on multiple devices (or no devices) will have the following effects:

Master Setting	Result
<b>Multiple devices set to Enabled</b>	Ring election based on MAC addresses of <b>Enabled</b> devices
<b>No devices set to Enabled</b>	Ring election based on MAC addresses of all devices
<b>Single device set to Enabled</b>	<b>Enabled</b> device always master, failure of <b>Enabled</b> device results in ring election

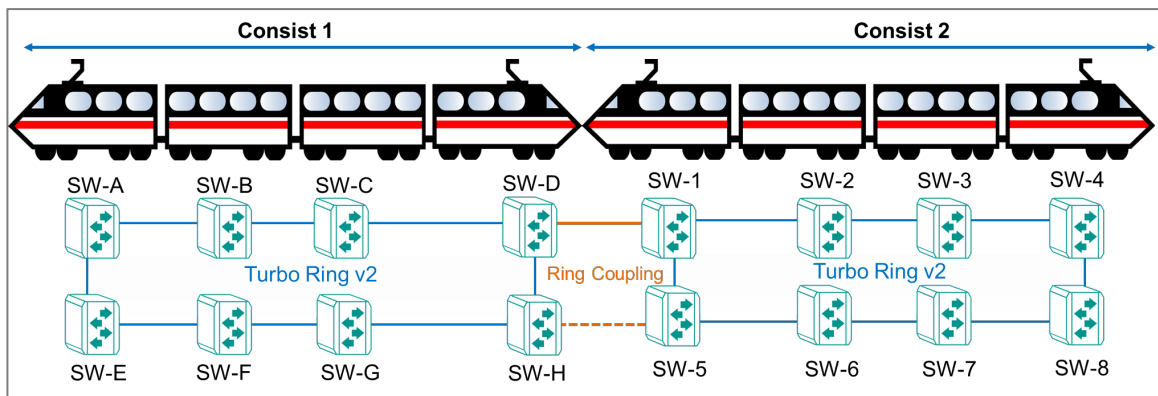
6. Click **Apply** to save your changes.

Once all devices in the ring are configured and enabled, you can connect the ring ports.

## Scenario: Using Turbo Ring in an On-board Train Application

In this scenario, we describe setting up Turbo Ring v2 with ring coupling between train consists.

A railway vehicle manufacturer needs to plan a new on-board network with redundancy and flexible inter-consist communication. The customer plans a ring network with Turbo Ring v2 between multiple vehicles to form one ring per consist. Multiple consists will then use ring coupling for inter-consist communication.



This structure allows for easy administration as consists are coupled and uncoupled.


To configure this scenario, do the following:

1. Configure the settings each network device for Turbo Ring v2.  
See the subsequent sections for details about how to configure each device.
2. Connect the network devices SW-A through SW-H in a ring topology, using ports 1 and 2 for segments of the ring. Do the same for SW-1 through SW-8. Do not connect the ring coupling yet.
3. Configure the Primary Coupling Path path on SW-D.  
See the subsequent sections for details about how to configure ring coupling.
4. Configure the Backup Ring Coupling on SW-H.  
See the subsequent sections for details about how to configure ring coupling.

Once all devices have been configured, you can connect the ring ports and coupling ports.

## Example: Configuring the Master for Turbo Ring v2 in an On-board Rail Application

Make sure you have NOT connected the ring ports until after you configure Turbo Ring v2 settings. Our examples use ports **1/1** and **1/2** as ring ports.

1. Sign in to the device using administrator credentials.
2. Go to **Redundancy > Layer 2 Redundancy > Turbo Ring V2**, and then click **Settings**.
3. Set **Turbo Ring V2** to **Enabled**.
4. Under Ring Settings, next to **Ring 1**, click  **[Edit]**.

The Ring 1 Settings screen appears.

5. Configure all of the following:

Option	Value
<b>Enabled</b>	<b>Enabled</b>
<b>Master</b>	<b>Enabled</b>
<b>Ring Port 1</b>	<b>1/1</b>
<b>Ring Port 2</b>	<b>1/2</b>

Setting **Master** on multiple devices (or no devices) will have the following effects:

Master Setting	Result
<b>Multiple devices set to Enabled</b>	Ring election based on MAC addresses of <b>Enabled</b> devices
<b>No devices set to Enabled</b>	Ring election based on MAC addresses of all devices
<b>Single device set to Enabled</b>	<b>Enabled</b> device always master, failure of <b>Enabled</b> device results in ring election

6. Click **Apply** to save your changes.


Once all devices in the ring are configured and enabled, you can connect the ring ports.

Continue to the next section to see how to configure ring coupling. Do not connect coupling ports until network devices have been configured.



## Example: Configuring non-Master devices for Turbo Ring v2 in an On-board Rail Application

Make sure you have NOT connected the ring ports until after you configure Turbo Ring v2 settings. Our examples use ports **1/1** and **1/2** as ring ports.

1. Sign in to the device using administrator credentials.
2. Go to **Redundancy > Layer 2 Redundancy > Turbo Ring V2**, and then click **Settings**.
3. Set **Turbo Ring V2** to **Enabled**.
4. Under Ring Settings, next to **Ring 1**, click  **[Edit]**.

The Ring 1 Settings screen appears.

5. Configure all of the following:

Option	Value
<b>Enabled</b>	<b>Enabled</b>
<b>Master</b>	<b>Disabled</b>
<b>Ring Port 1</b>	<b>1/1</b>
<b>Ring Port 2</b>	<b>1/2</b>

Setting **Master** on multiple devices (or no devices) will have the following effects:

Master Setting	Result
<b>Multiple devices set to Enabled</b>	Ring election based on MAC addresses of <b>Enabled</b> devices
<b>No devices set to Enabled</b>	Ring election based on MAC addresses of all devices
<b>Single device set to Enabled</b>	<b>Enabled</b> device always master, failure of <b>Enabled</b> device results in ring election

6. Click **Apply** to save your changes.

Once all devices in the ring are configured and enabled, you can connect the ring ports.  
Once all

Continue to the next section to see how to configure ring coupling. Do not connect coupling ports until network devices have been configured.


### Example: Configuring the Primary Ring Coupling Between Consists

Both network devices that make up the ring coupling must be configured as coupling devices.

- Make sure that you have configured both rings in the scenario.
- Do not connect the coupling ports until completing setup on both devices. Our scenario assumes port **1/5** will serve as coupling port.
- Couplers should only be configured on one ring. Our example uses SW-D as the primary and SW-H as the backup. Do not configure SW-1 or SW-5 as couplers.

To configure SW-D as the primary ring coupler:

The procedure on each device is identical. To configure each device, do the following:

1. Sign in to the device using administrator credentials.
2. Go to **Redundancy > Layer 2 Redundancy > Turbo Ring V2**, and then click **Settings**.
3. Under Ring Coupling Settings, click  **[Edit]**.

The Ring Coupling Settings screen appears.

4. Configure all of the following:

Option	Value
<b>Enabled</b>	<b>Enabled</b>
<b>Coupling Mode</b>	<b>Coupling Primary Path</b>
<b>Coupling Port</b>	<b>1/5</b>

5. Click **Apply** to save your changes.

The device has been configured as a primary ring coupling.


Connect the ring coupling ports. Once both devices are connected, you can move on to configuring the backup coupling.

## Example: Configuring the Backup Ring Coupling Between Consists

Both network devices that make up the backup ring coupling must be configured as coupling devices.

- Make sure that you have configured both rings in the scenario.
- Do not connect the coupling ports until completing setup on both devices. Our scenario assumes port **1/5** will serve as coupling port.
- Couplers should only be configured on one ring. Our example uses SW-D as the primary and SW-H as the backup. Do not configure SW-1 or SW-5 as couplers.

To configure SW-H as the backup coupler:

1. Sign in to the device using administrator credentials.
2. Go to **Redundancy > Layer 2 Redundancy > Turbo Ring V2**, and then click **Settings**.
3. Under Ring Coupling Settings, click  **[Edit]**.

The Ring Coupling Settings screen appears.

4. Configure all of the following:

Option	Value
<b>Enabled</b>	<b>Enabled</b>
<b>Coupling Mode</b>	<b>Coupling Backup Path</b>
<b>Coupling Port</b>	<b>1/5</b>

5. Click **Apply** to save your changes.

The device has been configured as a backup ring coupling.

Once the device has been configured, connect the ring coupling ports. Your coupling configuration will be complete.

## Turbo Ring V2

### Menu Path: Redundancy > Turbo Ring V2

This page lets you set up and configure Turbo Ring v2 redundancy for your device.

This page includes these tabs:

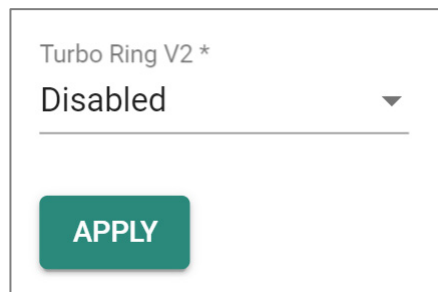
- Settings
- Status

## Turbo Ring V2 - Settings

**Menu Path: Redundancy > Turbo Ring V2 - Settings**

This page lets you configure the Turbo Ring V2 settings.

### Turbo Ring V2 Settings



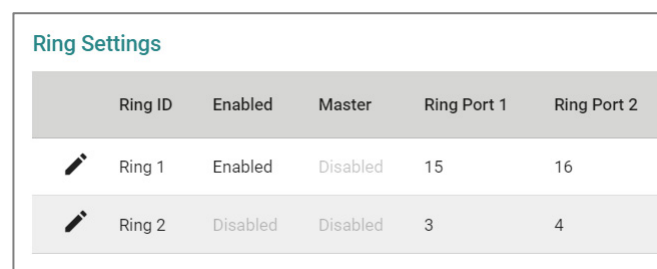
Turbo Ring V2 \*



Disabled

APPLY

UI Setting	Description	Valid Range	Default Value
<b>Turbo Ring V2</b>	Enable or disable Turbo Ring V2 for the device.	Enabled / Disabled	Disabled

### Ring Settings



Ring Settings					
	Ring ID	Enabled	Master	Ring Port 1	Ring Port 2
	Ring 1	Enabled	Disabled	15	16
	Ring 2	Disabled	Disabled	3	4

UI Setting	Description
<b>Ring ID</b>	Shows the ID of the ring the entry is for.
<b>Enabled</b>	Shows whether Turbo Ring V2 is enabled for the ring.
<b>Master</b>	Shows whether the device is designated as the master for the ring.
<b>Ring Port 1</b>	Shows which port will act as ring port 1. If this device is designated as the master for the ring, this will be the primary ring connection.
<b>Ring Port 2</b>	Shows which port will act as ring port 2. If this device is designated as the master for the ring, this will be the backup ring connection and will be blocked normally.

## Edit Ring Settings

### Menu Path: Redundancy > Turbo Ring V2 - Settings

Clicking the **Edit** (✎) icon for a ring on the **Redundancy > Turbo Ring V2 - Settings** page will open this dialog box. This dialog lets you edit the Turbo Ring V2 settings for the ring.

Click **APPLY** to save your changes.

### Ring 1 Settings

Enabled \*  
Enabled ▼

Master \*  
Disabled ▼

Ring Port 1 \*  
15 ▼

Ring Port 2 \*  
16 ▼

CANCEL
APPLY

UI Setting	Description	Valid Range	Default Value
<b>Enabled</b>	Enable or disable Turbo Ring V2 for the ring.	Enabled / Disabled	Disabled
<b>Master</b>	Enable or disable whether the device will be designated as the master for the ring.	Enabled / Disabled	Disabled
<b>Ring Port 1</b>	Specify which port will act as ring port 1. If this device is designated as the master for the ring, this will be the primary ring connection.	Drop-down list of ports	1
<b>Ring Port 2</b>	Specify which port will act as ring port 2. If this device is designated as the master for the ring, this will be the backup ring connection and will be blocked normally.	Drop-down list of ports	2

## Ring Coupling Settings

**Ring Coupling Settings**

Coupling Mode	Enabled	Coupling Port
Primary Path	Disabled	5

UI Setting	Description
<b>Coupling Mode</b>	Shows coupling mode the entry is for.
<b>Enabled</b>	Shows whether ring coupling is enabled or disabled.
<b>Coupling Port</b>	Shows the port used for ring coupling.

## Edit Ring Coupling Settings

### Menu Path: Redundancy > Turbo Ring V2 - Settings

Clicking the **Edit** () icon for an entry on the **Redundancy > Turbo Ring V2 - Settings** page will open this dialog box. This dialog lets you edit the ring coupling settings for the entry.

Click **APPLY** to save your changes.

### Ring Coupling Settings

Enabled \*  
Disabled ▼

Coupling Mode \*  
Coupling Primary Path ▼

Coupling Port \*  
5 ▼

CANCEL
APPLY


UI Setting	Description	Valid Range	Default Value
<b>Enabled</b>	Enable or disable ring coupling for the device.	Enabled / Disabled	Disabled
<b>Coupling Mode</b>	Specify whether this device will be designated as primary or backup path for ring coupling.	Coupling Primary Path / Coupling Backup Path	Coupling Primary Path
<b>Coupling Port</b>	Specify the port to use for ring coupling.	Drop-down list of ports	5

## Turbo Ring V2 - Status

### Menu Path: Redundancy > Turbo Ring V2 - Status

This page lets you view the Turbo Ring V2 ring and ring coupling status.

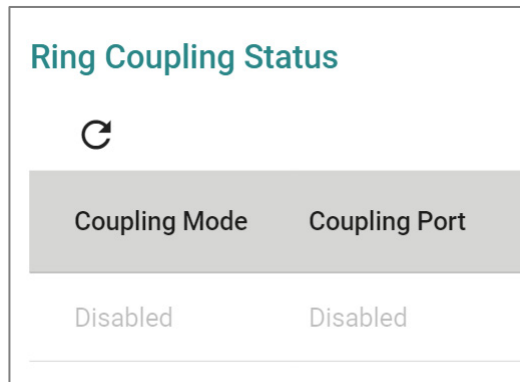
## Ring Status

Ring Status					
					
Ring ID	Master ID	Status ↑	Master	Ring Port 1	Ring Port 2
Ring 1	00:00:00:00:00:00	Disabled	Slave	Disabled	Disabled
Ring 2	00:00:00:00:00:00	Disabled	Slave	Disabled	Disabled

UI Setting	Description
<b>Ring ID</b>	Shows the ID of the ring the entry is for.
<b>Master ID</b>	Shows the MAC address of the ring master.
<b>Status</b>	Shows the status of the ring. <ul style="list-style-type: none"><li>• <b>Healthy:</b> The ring and the ports are working properly.</li><li>• <b>Break:</b> One or more rings have been broken.</li></ul>
<b>Master</b>	Shows whether the device is configured as a master or slave for the ring.
<b>Ring Port 1</b>	Shows which port will act as ring port 1. If this device is designated as the master for the ring, this will be the primary ring connection.
<b>Ring Port 2</b>	Shows which port will act as ring port 2. If this device is designated as the master for the ring, this will be the backup ring connection and will be blocked normally.



## Ring Coupling Status

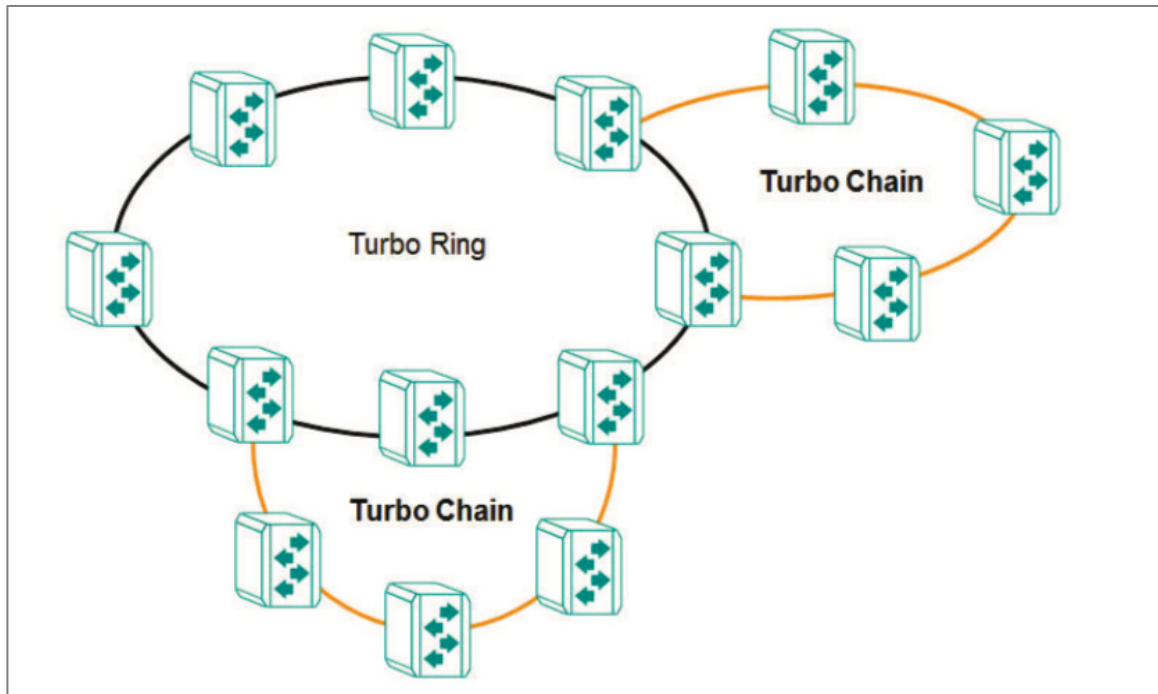


UI Setting	Description
<b>Coupling Mode</b>	Shows whether the device is the primary or backup path for ring coupling.
<b>Coupling Port</b>	Shows the port used for ring coupling.

## About Turbo Chain

Turbo Chain allows flexible expansion on top of an existing topology

This allows for flexible, cost-effective expansions. This allows you to grow existing networks without replacement the main ring while still maintaining reliability and redundancy.

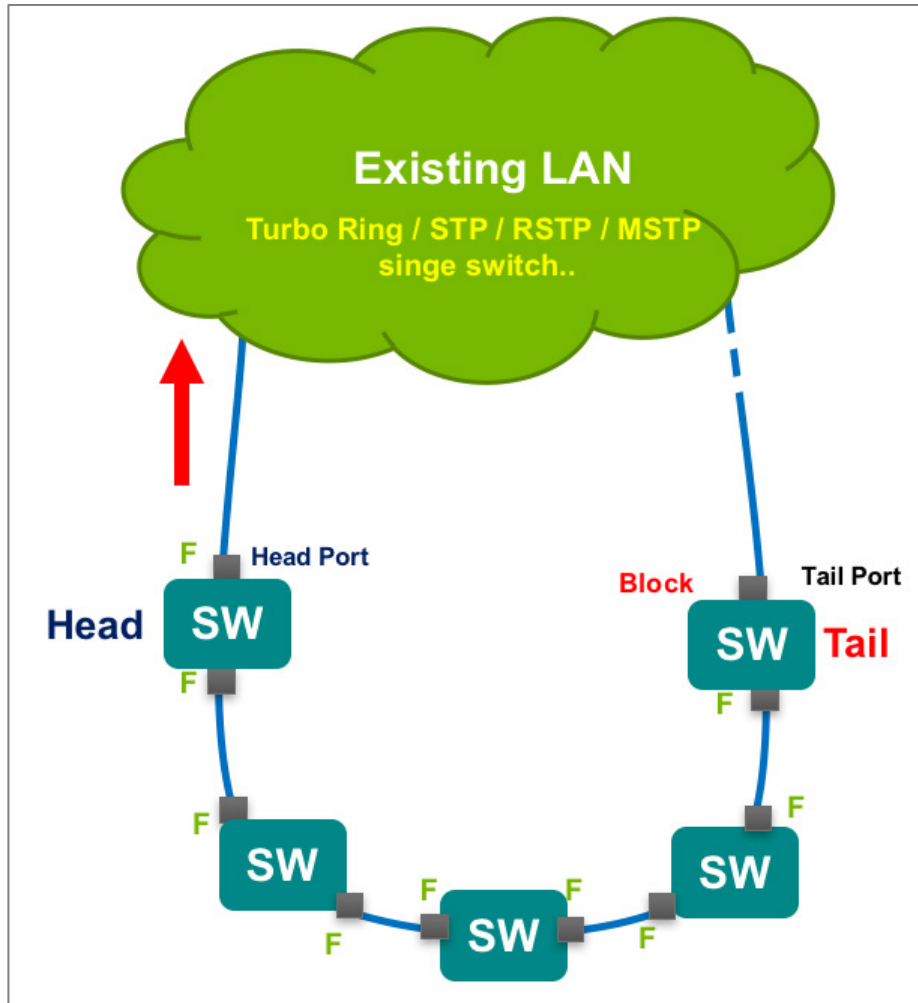


Turbo Chain is a proprietary redundancy technology developed by Moxa, designed for use in widely distributed networks. It enables Ethernet switches to be connected in a daisy-chain configuration, where each switch serves as a backup path for connected devices. Turbo Chain supports system recovery times of under 20 ms for Fast Ethernet and 50 ms for Gigabit Ethernet in member port link environments.

Turbo Chain is suitable for industrial networks with complex topologies, particularly those utilizing multi-ring architectures. It allows the creation of flexible and scalable topologies with rapid media recovery.

In a typical Turbo Chain setup, each Ethernet switch is connected to two others in a daisy-chain configuration. The switches are categorized into three types: Head, Tail, and Member switches. The Head switch connects the chain to the external network, while the Tail switch provides redundancy. If the Head port is disconnected, the Tail port immediately assumes the role of data transfer, ensuring continuous communication.

This technology ensures that in the event of a link or switch failure, Turbo Chain quickly reroutes traffic to an available backup path, minimizing network downtime and maintaining uninterrupted communication.



Turbo Chain is often used in industrial automation, transportation, and surveillance applications where network reliability is critical. It is compatible with other Moxa networking technologies, such as Turbo Ring, and other Redundancy protocols like STP/RSTP, MSTP etc, to provide further redundancy and resilience for industrial networks.

To sum up, here are some of the features of Turbo Chain technology:

1. **Topology:** Turbo Chain uses a daisy-chain topology to connect Ethernet switches in a loop-free configuration.
2. **Redundancy:** Turbo Chain provides a backup path on the tail switch to ensure network availability and reduce downtime in the event of a switch or link failure.
3. **Fast failover:** Turbo Chain has a fast failover mechanism that can detect and activate backup paths in a matter of milliseconds (< 20 ms) to ensure uninterrupted communication between devices.

4. **Compatibility:** Turbo Chain is compatible with other redundancy technologies, such as Turbo Ring and RSTP, to provide even greater redundancy and resilience for industrial networks.

### **Example: Configuring Turbo Chain (RKS-G4000 Series)**

In this example, we will configure network devices for Turbo Chain.

- Determine which devices will be the head, tail, and members of the chain. The head and tail must connect to the main LAN.
- Do not connect any of the chain devices until configuration of all devices is complete.
- Do not use any of the chain ports until configuration is completed. Do not use these ports for administration, as applying the chain configuration to these ports will disconnect you from the web GUI.

You can configure the head, tail, and member devices in any order as long as you do not connect them until after all devices are configured. Choose a device to configure and do the following:

1. Sign in to the device using administrator credentials.
2. Go to **Redundancy > Layer 2 Redundancy > Turbo Chain**, and then click **Settings**.
3. Set **Turbo Chain** to **Enabled**.
4. For chain role, specify one of the following:
  - **Head** - specify only one head of the chain. This will be the primary connection to the rest of the network.
  - **Tail** - specify only one tail of the chain. This device will be the backup connection to the rest of the network.
  - **Member** - specify one or more member devices. Member devices make up the "links" between the head and the tail of the chain. Make sure that there are no loops in the chain.
5. Specify the following Ports based on the **Chain Role**:

Head Chain Role Option	Port Value
<b>Tail Port</b>	<b>2/1</b>
<b>Member Port</b>	<b>2/2</b>

Member Chain Role Option	
<b>Member Port 1</b>	<b>2/1</b>
<b>Member Port 2</b>	<b>2/2</b>

Tail Chain Role Option	
<b>Member Port 1</b>	<b>2/1</b>
<b>Member Port 2</b>	<b>2/2</b>

6. Click **Apply** to save changes.
7. Repeat this procedure to configure all devices in the chain. Once all devices have been configured, connect the devices in the chain.

Once all devices are configured and connected, packets are transmitted through the Head Port to the LAN network. If any Turbo Chain path is disconnected, the Tail Port will be activated so that packet transmission can continue.

## Turbo Chain

### Menu Path: Redundancy > Turbo Chain

This page lets you manage the Turbo Chain feature for your device.

This page includes these tabs:

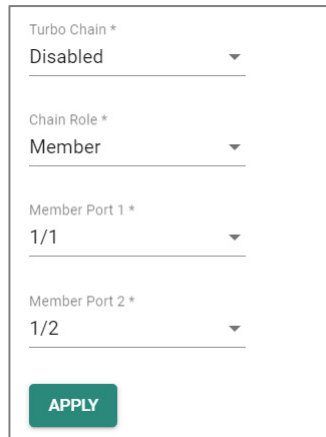
- Settings
- Status

## Turbo Chain - Settings

### Menu Path: Redundancy > Turbo Chain - Settings

This page lets you configure the Turbo Chain settings.

## Turbo Chain Settings



The screenshot shows a configuration form for Turbo Chain settings. It contains four dropdown menus: 'Turbo Chain \*' set to 'Disabled', 'Chain Role \*' set to 'Member', 'Member Port 1 \*' set to '1/1', and 'Member Port 2 \*' set to '1/2'. A green 'APPLY' button is located at the bottom of the form.

UI Setting	Description	Valid Range	Default Value
<b>Turbo Chain</b>	Enable/disable Turbo Chain for your device.	Enabled / Disabled	Disabled
<b>Chain Role</b>	Specify the chain role for your device.	Head / Member / Tail	Member
<b>Member Port 1</b>	Specify the port to use as member port 1.	Drop-down list of ports	1
<b>Member Port 2</b>	Specify the port to use as member port 2.	Drop-down list of ports	2

## Turbo Chain - Status

### Menu Path: Redundancy > Turbo Chain - Status

This page lets you view the Turbo Chain status of your device.

## Turbo Chain Status

Chain Information	
Turbo Chain	Chain Role
Disabled	Member
Member 1 Port Status	Member 2 Port Status
Disabled	Disabled

UI Setting	Description
<b>Turbo Chain</b>	Shows whether Turbo Chain is enabled for your device.
<b>Chain Role</b>	Shows the chain role of your device.
<b>Member Port 1</b>	Shows the status of member port 1.
<b>Member Port 2</b>	Shows the status of member port 2.

## About MRP (Media Redundancy Protocol)

MRP (Media Redundancy Protocol) is a network protocol based on the IEC 62439-2 that allows users to create a redundant ring system. With a recovery time of less than 200 ms, it can support up to 50 devices in each ring.

MRP includes the following roles:

### MRM (Media Redundancy Manager)

MRM, also known as the Ring Manager, is a node in the network topology that manages and monitors the health of the entire ring. There is only one MRM in the network. In the event of a Link Down scenario, the MRM diagnoses the issue and notifies all MRCs (Media Redundancy Clients) to flush their MAC address table and relearn the path. Additionally, the MRM changes the port status of the primary port from blocking to forwarding to restore connectivity.

### MRC (Media Redundancy Client)

MRC, also known as the Ring Client, is a node in the network topology that is monitored by the MRM (Media Redundancy Manager). However, the MRCs do not solely rely on the MRM to detect the health of the ring, they also automatically notify the MRM in the event

of a Link Down or Recovery situation. The MRC flushes its MAC address table and relearns the path when requested by the MRM.

### **MIM (Media Redundancy Interconnection Manager)**

The function of the MIM is to observe and to control the redundant interconnection topology in order to react on interconnection faults. To cover a maximum of applications, two detection methods are provided by this international standard. The MIM can observe the interconnection topology **by RC mode (Ring check mode)**. With RC mode, the MRP interconnection manager can observe the interconnection topology by sending test frames on the interconnection port over the connected rings and receiving them over its ring ports, checking in both directions

### **MIC (Media Redundancy Interconnection Client)**

The other three nodes in the interconnection topology have the role of media redundancy interconnection clients (MIC), in addition to the role of a MRC or MRM. The MIC reacts on received reconfiguration frames from the MIM, it can detect and signal link changes of its interconnection port, and it can issue link change notification messages.

## **Configuring Ring Managers and Clients**

MRP Managers and Clients must be configured before the rings can be used.

- Determine which devices will be the Manager and the Clients. There can only be a single manager.
- Do not connect any of the devices until configuration of all devices is complete.
- Do not use any of the ring ports until configuration is completed. Do not use these ports for administration, as applying the chain configuration to these ports will disconnect you from the web GUI.

Choose a device to configure and do the following:

1. Sign in to the device using administrator credentials.
2. Go to **Redundancy > Layer 2 Redundancy > MRP**, and then click **Settings**.
3. Under Media Redundancy Protocol, choose **Enabled** from the drop-down menu.
4. Specify the following based on the **Role**:



Ring Manager Option	Ring Manager Value
<b>Role</b>	<b>Ring Manager</b>
<b>VLAN ID</b>	Specify the VLAN ID for the ring
<b>Domain UUID</b>	Choose either <b>Default</b> or <b>PROFITNET (Siemens)</b> according to your network configuration
<b>React on Link Change</b>	It is recommended to set this to <b>Enabled</b> . This setting allows the Ring Manager to quickly respond to topology changes, both when a link goes down and when the original topology is restored.
<b>Ring Port 1</b>	Specify the first redundant ring port
<b>Ring Port 2</b>	Specify the second redundant ring port

Ring Client Option	Ring Client Value
<b>Role</b>	<b>Ring Client</b>
<b>VLAN ID</b>	Specify the VLAN ID for the ring
<b>Domain UUID</b>	Choose either <b>Default</b> or <b>PROFITNET (Siemens)</b> according to your network configuration
<b>Ring Port 1</b>	Specify the first redundant ring port
<b>Ring Port 2</b>	Specify the second redundant ring port

5. Click **Apply** to save your changes.

Once all devices are configured, you can connect the ring ports.

## MRP

### Menu Path: Redundancy > MRP

This page lets you configure the MRP parameters of the switch and view the MRP protocol operation status of the switch.

This page includes these tabs:

- Settings

- Status

## MRP - Settings

**Menu Path: Redundancy > MRP - Settings**

This page lets you enable and configure MRP for your device.



### Media Redundancy Protocol

Settings Status

---

Media Redundancy Protocol \*

Enabled ▾

Role *	VLAN ID *	
Ring Client ▾	1	
	1 - 4094	
Domain UUID *	React on Link Change	
Default ▾	Disabled ▾	
	.....	
Ring Port 1 *	Ring Port 2 *	
1/1 ▾	1/2 ▾	

#### Interconnection

Interconnection \*

Enabled ▾



Interconnection Role *	Interconnection Mod...	Interconnection ID *
Interconnection Client ▾	Interconnection Mod... ▾	0
		0 - 65535
Interconnection Port *		
1/3 ▾		

**APPLY**

UI Setting	Description	Valid Range	Default Value
<b>Media Redundancy Protocol</b>	Enable or disable Media Redundancy Protocol (MRP) for the device.	Enabled / Disabled	Disabled
<b>Role</b>	Specify the role for the device. <ul style="list-style-type: none"> <li>• <b>Ring Client:</b> The device will act as a ring client.</li> <li>• <b>Ring Manager:</b> The device will act as a ring manager, and can manage and monitor the ring's health status.</li> </ul>	Ring Client / Ring Manager	Ring Client
<b>VLAN ID</b>	Specify the VLAN ID to use for MRP. <div style="background-color: #f0f0f0; padding: 5px; margin-top: 10px;"> <p><b>Note</b></p> <p>The VLAN ID should align with the ring port settings.</p> </div>	1 to 4094	1
<b>Domain UUID</b>	Select whether to use a default or PROFINET domain UUID.	Default / PROFINET	Default
<b>React on Link Change</b> <b>(If Role is Ring Manager)</b>	Enable or disable reacting on link change. Enable reaction on link change for faster recovery speeds.	Enabled / Disabled	Enabled
<b>Ring Port 1</b>	Specify the port to use as the 1st redundant port. <div style="background-color: #f0f0f0; padding: 5px; margin-top: 10px;"> <p><b>Note</b></p> <p>Only select the port in VLAN Trunk/Hybrid mode.</p> </div>	Drop-down list of ports	N/A
<b>Ring Port 2</b>	Specify the port to use as the 2nd redundant port. <div style="background-color: #f0f0f0; padding: 5px; margin-top: 10px;"> <p><b>Note</b></p> <p>Only select the port in VLAN Trunk/Hybrid mode.</p> </div>	Drop-down list of ports	N/A

## Interconnection

UI Setting	Description	Valid Range	Default Value
<b>Interconnection</b>	Enable or disable MRP interconnection for the device.	Enabled / Disabled	Disabled


UI Setting	Description	Valid Range	Default Value
<b>Interconnection Role</b>	Select the interconnection role for the device.	Interconnection Manager / Interconnection Client	Interconnection Client
<b>Interconnection Mode</b>	Select the interconnection mode to use for the device.  <div style="background-color: #f0f0f0; padding: 5px;"> <p> <b>Note</b></p> <p>The Interconnection Manager and all Interconnection Clients in the same MRP interconnection topology must use the same interconnection mode.</p> </div>	RC Mode	N/A
<b>Interconnection ID</b>	Specify an ID for the interconnection.	0 - 65535	0
<b>Interconnection Port</b>	Select a port to use for the interconnection.  <div style="background-color: #f0f0f0; padding: 5px;"> <p> <b>Note</b></p> <p>Only select the port in VLAN Trunk/Hybrid mode.</p> </div>	Drop-down list of ports	3 or 1/3, depending on the model

## MRP - Status

### Menu Path: Redundancy > MRP - Status

This page lets you view the overall status of the MRP ring and ring ports.

## Ring Status

**Ring Status** 

MRP Ring  
**Enabled**

Role  
**Ring Client**

Ring State  
**Data Exchange Idle**

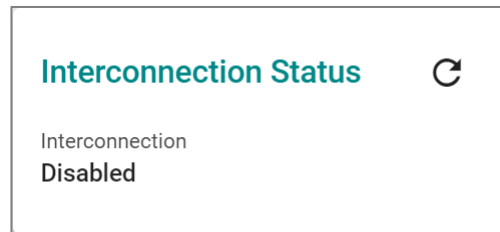
React on Link Change  
**Disabled**

VLAN ID  
**1**

Domain ID  
**FFFFFFFF-FFFF-FFFF-FFFF-FFFFFFFFFFFF**

UI Setting	Description
<b>MRP Ring</b>	Shows whether the MRP ring is enabled.
<b>Role</b>	Shows the role of the device.
<b>Ring State</b>	Shows the current ring state.
<b>React on Link Change</b>	Shows whether reaction on link change is enabled.
<b>VLAN ID</b>	Shows the VLAN ID for the ring.
<b>Domain ID</b>	Shows the domain UUID for the ring.

## Interconnection Status



UI Setting	Description
<b>Interconnection</b>	Shows whether MRP interconnection is enabled.

## MRP Port Status List

Interface	Port	Port Status
Ring Port 1	1	Link Down
Ring Port 2	2	Forwarding

UI Setting	Description
<b>Interface</b>	Shows the interface the entry is for.
<b>Port</b>	Shows the port used for the interface.
<b>Port Status</b>	Shows the port status of the interface.

## About Multiple Dual Homing

Multiple Dual Homing is a layer 2 function that connects two network topologies using a single Ethernet switch, enabling redundancy protocols on each topology. It links either two devices or two rings to two independent connection points, activating a secondary

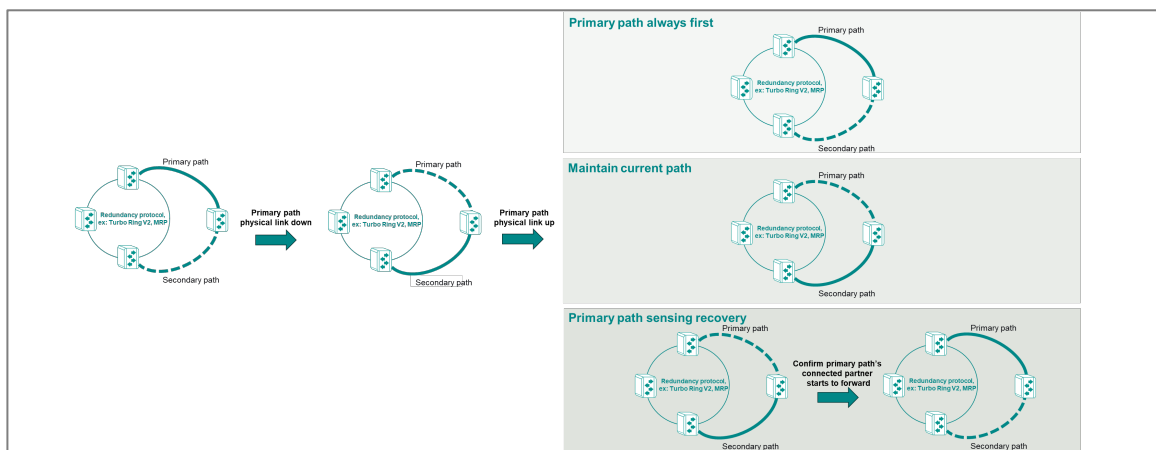
path if the primary path fails. Multiple Dual Homing allows for several dual-homing sessions simultaneously, supporting multiple redundant connections.

## Multiple Dual Homing In Depth

To configure Multiple Dual Homing, you must specify the primary port and secondary (fallback) port for the switch, which correspond to the primary and secondary paths respectively. The primary path serves as the default forwarding path, with the secondary path blocked until the primary goes down.

Multiple dual homing supports three path switching modes:

- **Primary path always first** (default). Automatically switches back to the primary path when it recovers, blocking the secondary path regardless of its status. Recovery time depends on the connected partner's data and physical link timing.
- **Maintain current path**. Maintains the current (secondary) path even if the primary path recovers, until the secondary path disconnects. Reduces the cost of frequent switching.
- **Primary path sensing recovery**. Switches to the primary path once the primary port confirms that the partner device is forwarding, immediately blocking the secondary port. This mode minimizes recovery time.



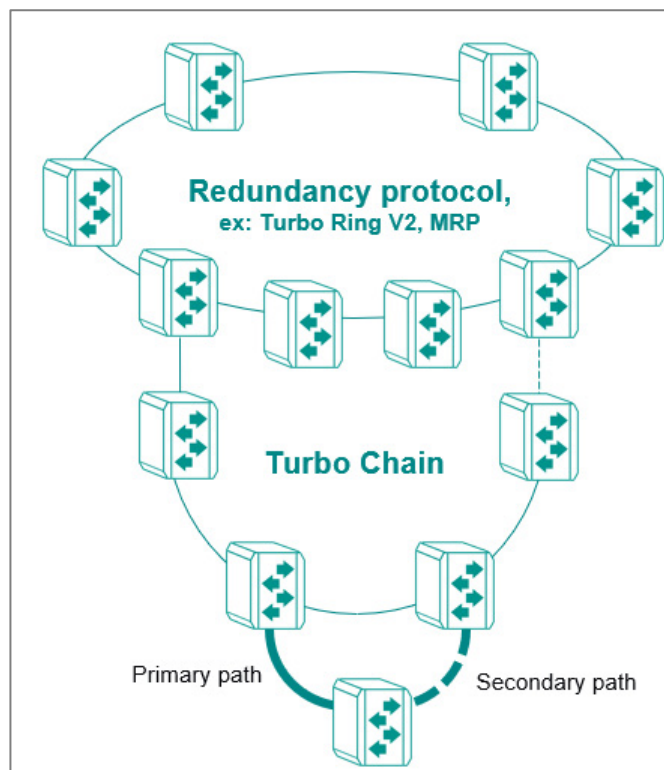
**Note**

It is highly recommended to configure Linkup Delay to avoid rapid oscillation between primary and secondary paths.

When used in conjunction with other Moxa redundancy protocols, such as Turbo Ring v2 and Turbo Chain, Multiple Dual Homing can significantly reduce fault recovery costs.

	Fast Ethernet	Gigabit Copper	SFP
<b>Turbo Ring/Turbo Chain</b>	20 ms	800 ms	50 ms

Multiple Dual Homing can coexist with other redundancy protocols provided these protocols are configured on different ports. Dual Homing and other redundancy protocols are mutually exclusive on any logical port, including trunking ports.





**Note**

Port-Channel ports can be used with Dual-homing, but have the following limitations:

- Port-Channel and member ports can not be deleted while set as a Primary or Secondary port.
- Ports assigned as a Primary or Secondary port cannot be assigned to Port-Channel member ports while Multiple Dual Homing is enabled.

**Note**

Ports with IEEE 802.1X or MAB enabled cannot be specified as Primary or Secondary ports due to the possibility of interruption. Port authorization and redundancy serve different purposes, and should remain on separate ports.


## Configuring Multiple Dual Homing

Do not connect homing ports until setup is complete, otherwise you may risk network looping.

1. Sign in to the device with administrator credentials.
2. Go to **Redundancy > Layer 2 Redundancy > Multiple Dual Homing**, and then choose **Settings**.
3. Under **Settings**, click **Multiple Dual Homing** and choose **Enabled** from the drop-down list.
4. Specify a **Path Switching Mode**:

Option	Description
<b>Primary path always first</b>	Reconnects as soon as physical media is available, with recovery time determined by data link responsiveness.
<b>Maintain current path</b>	After switching paths, device will not switch back unless the secondary becomes unavailable, minimizing recovery time.
<b>Primary path sensing recovery</b>	Reconnects when primary path data link goes back up, reducing recovery time.

4. Click **Apply** to save your changes.

- To edit a Session, under Dual Homing Table Settings, click  **[Edit]** next to the corresponding **Session ID**.

The Edit Session Settings screen appears.

- Specify all of the following, and click **Apply** to save your changes:

Option	Value
<b>Status</b>	<b>Enabled</b>
<b>Primary Port</b>	Specify the Port used as the primary path. This port will be the default link to the network.
<b>Secondary Port</b>	Specify the Port used as the secondary path. This port will be the backup link to the network.

The corresponding **Session ID** updates.


- Repeat this step to configure additional sessions.

Multiple Dual Homing has been configured. You can now connect ports.

It is highly recommended to configure **Linkup Delay** to avoid rapid oscillation between primary and secondary paths.

### Configuring Linkup Delay

Linkup Delay adds a brief pause before establishing a link, which can be useful to avoid oscillation or "flapping" in complex network setups.

- Sign in to the device with administrator credentials.
- Go to **Port > Port Interface > Linkup Delay**.
- Under **Linkup Delay**, select **Enable** from the drop down list, and then click **Apply**.
- Configure Linkup Delay on each port by clicking  **[Edit]** next to the corresponding **Port**, configuring the following, and then clicking **Apply**:

<b>Linkup Delay</b>	<b>Enabled</b>
---------------------	----------------

<b>Delay Time</b>	2 seconds is the default and recommended setting.
<b>Copy configurations to ports</b>	Optionally, duplicate configuration on other ports. For users configuring Multiple Dual Homing, we recommend configuring both primary and backup ports with Linkup Delay.

Linkup Delay settings will be shown in the table.

## Multiple Dual Homing

**Menu Path: Redundancy > Layer 2 Redundancy > Multiple Dual Homing**

This page lets you manage the Multiple Dual Homing feature for your device.

This page includes these tabs:

- Settings
- Status

### Multiple Dual Homing - Settings

**Menu Path: Redundancy > Layer 2 Redundancy > Multiple Dual Homing - Settings**

This page lets you enable and configure Multiple Dual Homing for your device.

## Multiple Dual Homing Settings

### Multiple Dual Homing

Settings
Status

Multiple Dual Homing \*

Enabled ▼





Path Switching Mode \*

Primary path sensing recovery ▼

APPLY

UI Setting	Description	Valid Range	Default Value
<b>Multiple Dual Homing</b>	Enable or disable Multiple Dual Homing for your device.	Enabled/Disabled	Disabled
<b>Path Switching Mode</b>	Select the path switching mode to use for Multiple Dual Homing based on whether or not you want to switch back to the primary path when the primary path recovers.	Primary path always first / Maintain current path / Primary path sensing recovery	Primary path always first

## Multiple Dual Homing Session List

	Session ID	Enabled	Primary Port	Secondary Port
	1	Enabled	1/1	1/2
	2	Disabled	1/3	1/4
	3	Disabled	2/1	2/2
	4	Disabled	2/3	2/4

UI Setting	Description
<b>Session ID</b>	Shows the Multiple Dual Homing session ID the entry is for.
<b>Enabled</b>	Shows whether Multiple Dual Homing is enabled for the session.
<b>Primary Port</b>	Shows the primary port for the session.
<b>Secondary Port</b>	Shows the secondary port for the session.

## Edit Session Settings

### Menu Path: Redundancy > Layer 2 Redundancy > Multiple Dual Homing - Settings

Clicking the **Edit** (✎) icon for a session on the **Redundancy > Layer 2 Redundancy > Multiple Dual Homing - Settings** page will open this dialog box. This dialog lets you edit the Multiple Dual Homing settings for the session.

Click **APPLY** to save your changes.

### Edit Session 1 Settings

Enabled \*

Primary Port \*

Secondary Port \*

UI Setting	Description	Valid Range	Default Value
<b>Status</b>	Enable or disable Multiple Dual Homing for the session.	Enabled / Disabled	Disabled

UI Setting	Description	Valid Range	Default Value
<b>Primary Port</b>	Select the primary port to use for the session.	Drop-down list of ports	Depends on the product model
<b>Secondary Port</b>	Select the secondary port to use for the session.	Drop-down list of ports	Depends on the product model

## Multiple Dual Homing - Status

**Menu Path: Redundancy > Layer 2 Redundancy > Multiple Dual Homing - Status**

This page lets you view the status of Multiple Dual Homing for your device.

### Multiple Dual Homing Session Status List

Session ID	Primary Port	Primary Link Status	Primary Port Status	Secondary Port
1	1/1	Link Down	Link Down	1/2
2	1/3	Link Down	Disabled	1/4
3	2/1	Link Down	Disabled	2/2
4	2/3	Link Down	Disabled	2/4

UI Setting	Description
<b>Session ID</b>	Shows the session ID the entry is for.
<b>Primary Port</b>	Shows the primary port for the session.
<b>Primary Link Status</b>	Shows the current link status of the primary path for the session.
<b>Primary Port Status</b>	Shows the current status of the primary port for the session.

UI Setting	Description
<b>Secondary Port</b>	Shows the secondary port for the session.
<b>Secondary Link Status</b>	Shows the current link status of the secondary path for the session.
<b>Secondary Port Status</b>	Shows the current status of the secondary port for the session.

## About Multiple Network Coupling

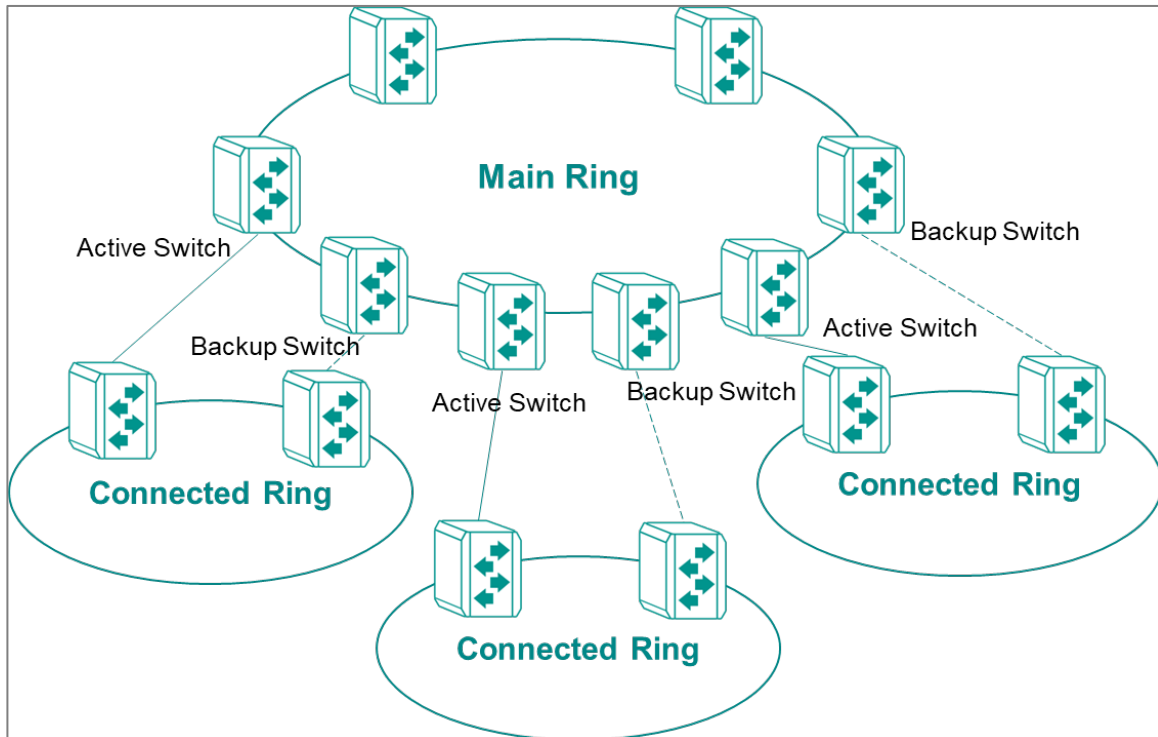
Multiple Network Coupling is a proprietary Moxa feature designed to address various scenarios where heterogeneous redundant networks need to be connected to operate together.

By connecting different redundant protocols, this feature not only provides flexibility for topologies applied in different applications, but also raises the level of overall network availability and stability by making sure the path between different redundant protocols is always unimpeded without looping.

Multiple Network Coupling includes a Main Ring and Connected Rings, and these rings can operate using the same or different redundancy protocols. This feature uses two switches to couple the two rings, and switches in the Main Ring control the coupling links to make sure communication between the two rings is smooth.

### Multiple Network Coupling In Depth

The structure of Multiple Network Coupling includes a Main Ring and Connected Rings.



MX-NOS supports the following redundancy protocols for the Main Ring:

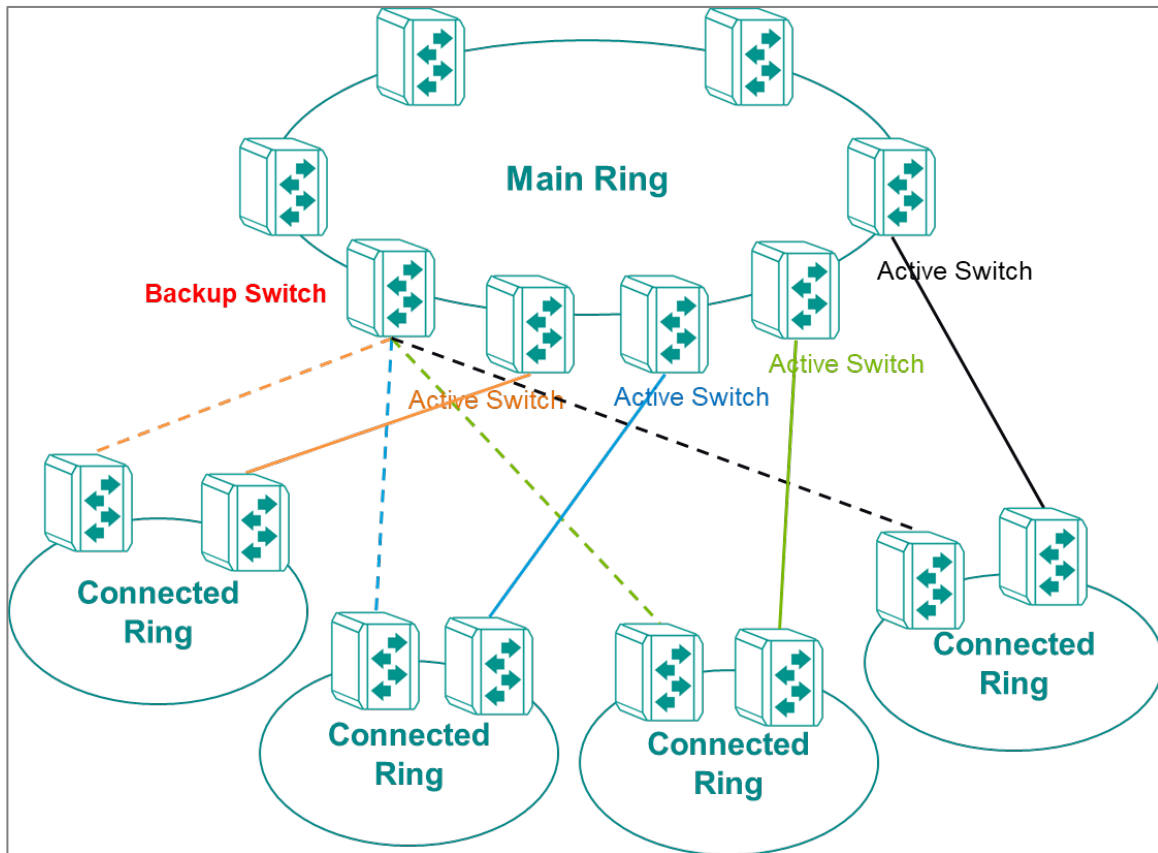
- Turbo Ring v2
- MRP
- HSR

MX-NOS supports the following redundancy protocols for Connected Rings:

- Turbo Ring v2
- MRP
- RSTP

The redundancy protocol on the Main Ring is coupled with the redundancy protocols running on the Connected Rings. Switches in the Main Ring used to couple the Connected Rings are designated as Active Switches or Backup Switches. Active Switches are responsible for the primary path and Backup Switches are responsible for the backup path. The communication protocols designed for the Active Switch and Backup Switch ensure traffic moves smoothly between the rings without looping. The Backup path will take over when the Primary path link is down, and vice versa.





### Multiple Network Coupling Limitations

- The Main Ring can couple with up to 16 Connected Rings.
- A switch in the Main Ring can support up to 4 paths to Connected Rings.
- A Backup Switch can pair with up to 4 Active Switches.
- An Active Switch can only have one Backup Switch.

### About Topologies for Multiple Network Coupling

These are some examples of different Multiple Network Coupling deployments and guidelines for topology planning.

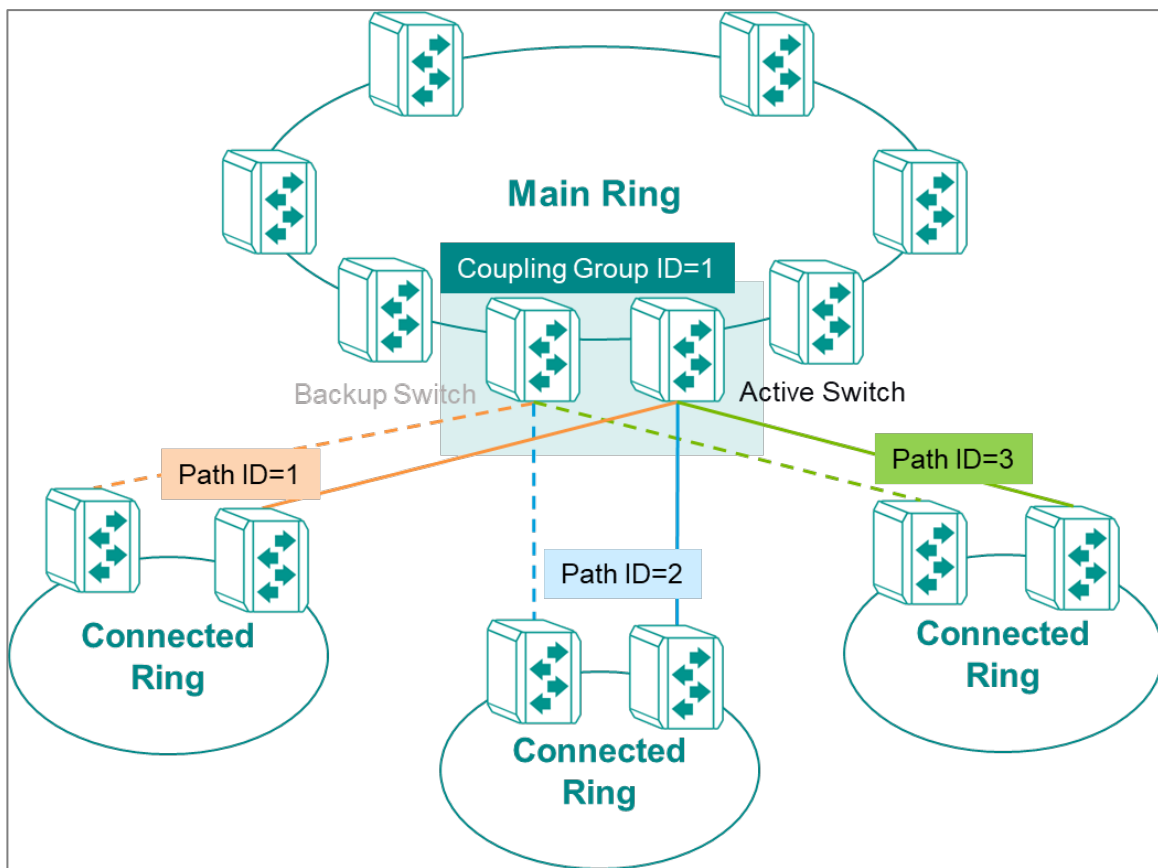
#### Guidelines for Topologies

- Coupling Groups refer to switches on the Main Ring, and the Connected Ring switches attached to them.
  - Each Coupling Group can only have one backup switch.

- Path IDs uniquely identify Connected Rings within the same coupling group.
  - Multiple Connected Rings connected to the same Coupling Group require separate Path IDs.

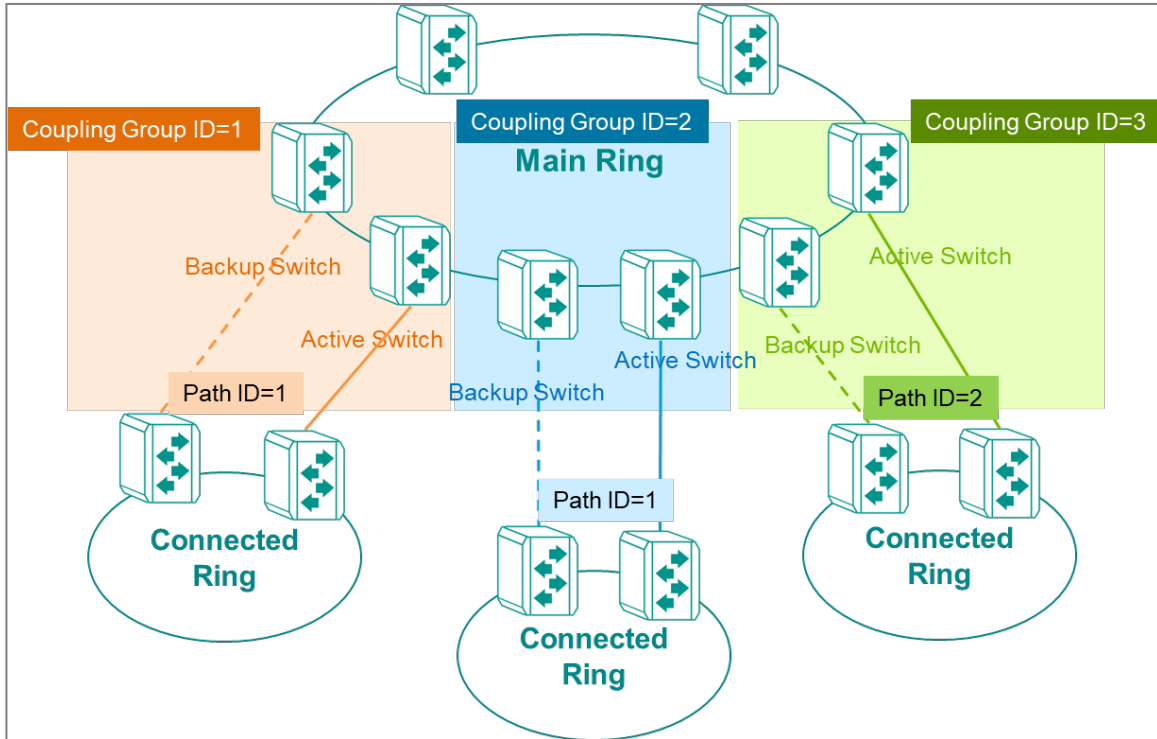
### One Coupling Group, Shared Active and Backup Switches

This topology shares the same Main Ring switches for all Connected Rings. This is a simple, centralized configuration.



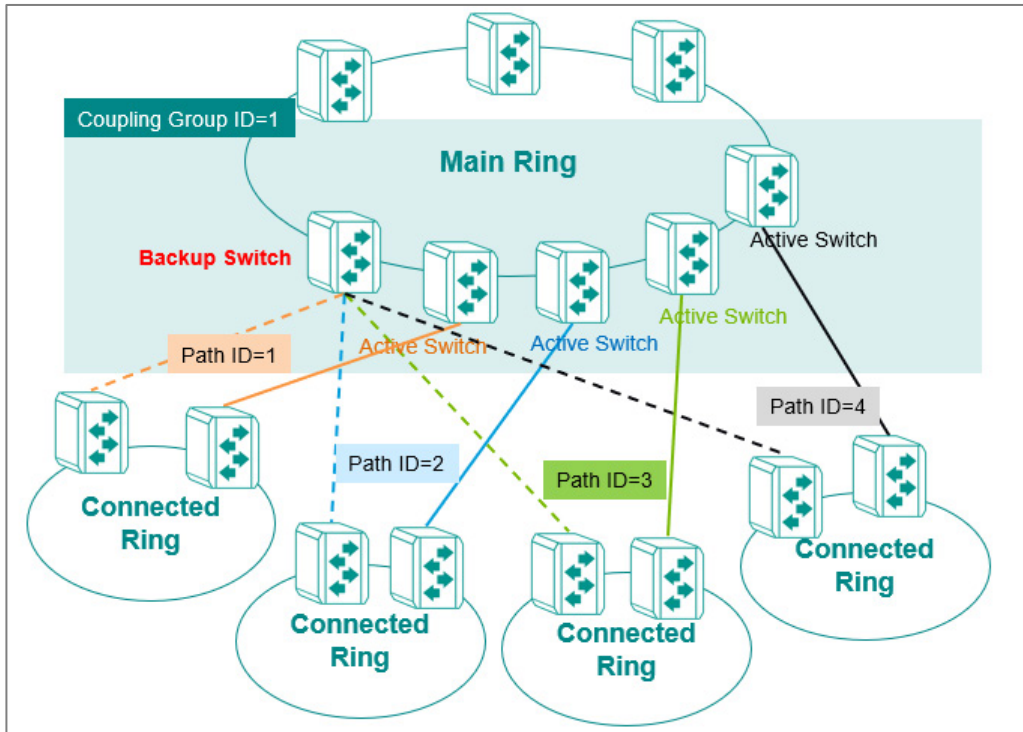
### Three Coupling Groups, Separate Active and Backup Switches

This topology uses separate pairs of Main Ring switches for each Connected Ring, providing maximum redundancy.



### One Coupling Group, Separate Active Switches, Shared Backup Switch

In this hybrid topology, connected rings share a single Backup Switch while maintaining separate Active Switches.



## Configuring Multiple Network Coupling

Multiple Network Coupling generally only needs configuration on Main Ring switches.


- Do not connect Main Ring switches and Connected Ring switches until Multiple Network Coupling is configured.
- Make sure that compatible redundancy protocols have been configured on each ring. As of November 2024, Multiple Network Coupling supports Turbo Ring v2, MRP, and RSTP.

Configure Multiple Network coupling on each "Main Ring" device.

1. Sign in to the device with administrator credentials.
2. Go to **Redundancy > Layer 2 Redundancy > Multiple Network Coupling**, and then click **Settings**.
3. Configure all of the following, and then click **Apply**:

Option	Value
<b>Multiple Network Coupling</b>	<b>Enabled</b>

Option	Value
<b>Coupling switch role</b>	<ul style="list-style-type: none"> <li>• <b>Active:</b> device will serve as the active switch</li> <li>• <b>Backup:</b> device will serve as the backup switch</li> </ul> <p>Only one backup switch supported per connected ring.</p>
<b>Coupling group ID</b>	Specify the coupling group ID from the dropdown list.
<b>Coupling polling interval</b>	<ul style="list-style-type: none"> <li>• <b>80 ms:</b> recommended for up to 16 path IDs.</li> <li>• <b>40 ms:</b> recommended for up to 8 path IDs.</li> </ul>

- To configure Path IDs (corresponding to each Connected Ring), under Coupling Table Settings, click the corresponding  **[Edit]**.  
The Edit Path ID Settings screen appears.
- Configure all of the following, and then click **Apply**:

Option	Value
<b>Status</b>	<b>Enabled</b>
<b>Path ID</b>	Specify the Path ID, corresponding to your Connected Ring
<b>Coupling Port</b>	Specify the port to which your Connected Ring will be connected.

- Repeat this step to configure additional Path IDs and corresponding Connected Rings.

Repeat this procedure for each switch in each coupling group.

For Connected Rings with non-Moxa switches that have RSTP enabled, make sure to enable edge ports on each port connected to the Main Ring.

## Multiple Network Coupling - Status

**Menu Path: Redundancy > Layer 2 Redundancy > Multiple Network Coupling - Status**

This page lets you view the status of Multiple Network Coupling for your device.

## Role Information

**Role Information** ↻

Coupling switch role	Coupling group ID
Disabled	---

UI Setting	Description
<b>Coupling switch role</b>	Shows the coupling switch role of the device.
<b>Coupling group ID</b>	Shows the coupling group ID of the device.


## Coupling Table Status

**Coupling Table Status**

↻

Path ID	Coupling Port	Coupling port state	Partner MAC	Connection Status	Error Status
1	2/1	Link Down	---	Disabled	---
2	2/2	Link Down	---	Disabled	---
3	2/3	Link Down	---	Disabled	---
4	2/4	Link Down	---	Disabled	---

UI Setting	Description
<b>Path ID</b>	Shows the Path ID for the entry.
<b>Coupling Port</b>	Shows the Coupling Port for the entry.
<b>Coupling Port State</b>	Shows the current Coupling Port State for the entry.
<b>Partner MAC</b>	Shows the MAC address of the current partner for the entry, if there is one.

UI Setting	Description
<b>Connection Status</b>	Shows the connection status of the current partner for the entry.
<b>Error Status</b>	Shows Error Status of the entry, if applicable. <ul style="list-style-type: none"> <li>• <b>Multiple active switches:</b> There are duplicate active switches in same path ID and group ID</li> <li>• <b>Multiple backup switches:</b> There are duplicate backup switches in same path ID and group ID, or multiple backup switches for a single active switch.</li> </ul> <div style="background-color: #f0f0f0; padding: 10px; margin-top: 10px;"> <p> <b>Note</b></p> <p>If there is an error, check the configurations for the device and partner device to ensure there are no duplicates.</p> </div>

## Multiple Network Coupling

**Menu Path:** [Redundancy](#) > [Layer 2 Redundancy](#) > [Multiple Network Coupling](#)

This page lets you manage the Multiple Network Coupling feature for your device.

This page includes these tabs:

- Settings
- Status

### Multiple Network Coupling - Settings

**Menu Path:** [Redundancy](#) > [Layer 2 Redundancy](#) > [Multiple Network Coupling - Settings](#)

This page lets you enable and configure Multiple Network Coupling for your device.

## Multiple Network Coupling Settings

**Multiple Network Coupling** \*

Enabled ▼

---

Coupling switch role \*

Backup ▼

---

Coupling polling interval \*

80 ▼ i

ms

**Main Ring Protocol**

Turbo Ring V2 ▼

---

Coupling group ID \*


3 ▼

---

APPLY





UI Setting	Description	Valid Range	Default Value
<b>Multiple Network Coupling</b>	Enable or disable Multiple Network Coupling for your device. This should be enabled if you want the device act as an active switch or backup switch.	Enabled / Disabled	Disabled
<b>Main Ring Protocol</b>	Shows the redundant protocol being used for the Main Ring. This value cannot be changed here. <div style="background-color: #f0f0f0; padding: 10px; margin-top: 10px;"> <p><b>Note</b></p> <p>The redundant protocol you want to enable in the Main Ring must be enabled before enabling Multiple Network Coupling.</p> <p>The redundant protocols supported in the Main Ring include:</p> <ul style="list-style-type: none"> <li>Turbo Ring V2</li> <li>MRP</li> <li>HSR</li> </ul> </div>	N/A	N/A
<b>Coupling switch role</b>	Specify the device's switch role in the Main Ring. <ul style="list-style-type: none"> <li><b>Active:</b> The device will act as the active switch responsible for the primary path.</li> <li><b>Backup:</b> The device will act as the backup switch responsible for the backup path to the Connected Ring.</li> </ul>	Active / Backup	Active
<b>Coupling group ID</b>	Specify the coupling group ID for the switch. <div style="background-color: #f0f0f0; padding: 10px; margin-top: 10px;"> <p><b>Note</b></p> <p>The coupling group ID for the paired active switch and backup switch must be the same.</p> </div>	1 to 16	1



UI Setting	Description	Valid Range	Default Value
<b>Coupling polling interval</b>	Specify the coupling polling interval in milliseconds used to check if the coupling path is forwarding.  <div style="border: 1px solid #ccc; background-color: #f9f9f9; padding: 10px; margin-top: 10px;"> <p> <b>Note</b></p> <p>The maximum number of active/backup switch pairs is 16. We suggest setting the Coupling polling interval to 80 ms if your topology has 16 pairs of active/backup switches to Connected Rings, and 40 ms if you have 8 pairs of active/backup switches.</p> </div>	40, 80	80

## Coupling Table Settings

### Coupling Table Settings

	Status	Path ID	Coupling Port
	Enabled	1	2/1
	Disabled	2	2/2
	Disabled	3	2/3
	Disabled	4	2/4

UI Setting	Description
<b>Status</b>	Shows whether Multiple Network Coupling is enabled for the entry.
<b>Path ID</b>	Shows the path ID for the entry.
<b>Coupling Port</b>	Shows the coupling port for the entry.

## Edit Path ID

### Menu Path: Redundancy > Layer 2 Redundancy > Multiple Network Coupling - Settings

Clicking the **Edit** (✎) for an entry allows you to enable and configure the coupling port for the entry.

### Edit Path ID 1 Settings

Status \*  
Enabled ▼

Path ID \*  
1 ▼

Coupling Port \*  
2/1 ▼

CANCEL APPLY

UI Setting	Description	Valid Range	Default Value
<b>Status</b>	Enable or disable the Path ID for the device.	Enabled / Disabled	Disabled
<b>Path ID</b>	Select the Path ID for the entry.  <div><p><b>Note</b></p><ul style="list-style-type: none"><li>On an active or backup switch, you can configure a maximum of 4 Path ID/Coupling Port pairs.</li><li>Make sure each active/backup switch pair is using the same <b>Path ID</b>.</li></ul></div>	1 to 16	1
<b>Coupling Port</b>	Select the port to use as a coupling port for the Path ID.	Drop-down list of ports	Depends on the product model

# Layer 3 Redundancy

## Layer 3 Redundancy

This section lets you configure the Layer 3 redundancy features of your device.

### About VRRP

Virtual Router Redundancy Protocol (VRRP) is a network protocol enabling multiple switches to collaborate as a group and share a virtual IP address. The main purpose of VRRP is to provide redundancy for the default gateway utilized by hosts on a LAN or VLAN.

In a VRRP setup, a single switch is designated as the "master" while the other switches are "backup" switches. The master switch is responsible for forwarding packets sent to the virtual IP address. On the other hand, the backup switches supervise the master switch and take over its tasks in case of failure. This feature facilitates automatic failover and redundancy, guaranteeing network connectivity even in the event of a switch failure.

To sum up, here are some benefits of VRRP:

1. **Increased Network Reliability:** VRRP enables multiple switches to work together in a group, sharing a virtual IP address. This provides redundancy for the default gateway, ensuring that network connectivity is maintained even if one of the switches fails. This increases the overall reliability of the network and helps prevent downtime.
2. **Automatic Failover:** VRRP facilitates automatic failover, where backup switches take over the tasks of the master switch in case of a failure. This ensures that there is no disruption to network services and users can continue to access resources without any interruption.
3. **Easy Network Management:** VRRP simplifies network management by allowing multiple switches to work together as a group, sharing a virtual IP address. This eliminates the need for complex routing protocols and reduces the risk of misconfigurations.

## VRRP States

In VRRP, switches are assigned different roles and states to ensure seamless failover and improved network availability.

The three primary states of VRRP are:

- **Init State:** This is the initial state when a VRRP switch starts up. The switch initializes its VRRP configuration and has not yet determined whether it should become a Master or a Backup switch. The switch remains in the Init state until it starts receiving VRRP advertisements from other switches in the same VRRP group or until it begins sending advertisements itself.
- **Master State:** In this state, the switch is responsible for forwarding packets sent to the virtual IP address and acts as the default gateway for the devices in the network. The switch with the highest priority (or lowest IP address in case of a tie) becomes the Master switch. The Master switch periodically sends VRRP advertisements to the other switches in the VRRP group to maintain its role. If the Master switch fails, one of the Backup switches will take over the role based on priority.
- **Backup State:** Switches in the Backup state are waiting to take over the Master role if the current Master switch fails. Backup switches listen for VRRP advertisements from the Master and update their timers accordingly. If a Backup switch stops receiving VRRP advertisements from the Master switch for a certain period (typically three times the advertisement interval), it assumes that the Master switch has failed and attempts to transition to the Master state based on its priority.


The VRRP states ensure that the network has a functioning default gateway at all times, providing redundancy and improving network availability in case of device failure. By implementing VRRP, network administrators can achieve increased network reliability, automatic failover, and easier network management.

## VRRP In Depth

VRRP enables several devices to share a virtual IP address and act as a unified virtual router. This feature provides backup capabilities in case one of the devices goes down or becomes unavailable. To accomplish this, VRRP group switches select a master switch based on priority, with the highest priority becoming the master. Each switch in the group

announces its priority, and the master regularly sends out VRRP advertisements to the other switches to update its status.

The virtual IP address is linked with the VRRP group, and the master switch forwards network packets using the virtual IP address as the source address. The backup switches stay inactive, listening to the VRRP messages from the master and are ready to take over if the master fails. The master switch sends advertisement packets to the backup ones to inform them that it is still operational. The advertisement interval is manually configured. If the master switch fails, the backup switch is unable to receive advertisement packets from the master. Once the advertisement down timer expires, backup switch will realize that the master is experiencing issues or has powered down and one of the backup switches with a higher priority takes over as the new master, ensuring there is no disruption in network connectivity.

 **Note**

1. The advertisement down timer is the time during which the Backup switch does not receive three consecutive advertisement packets from the Master.
2. The Backup switch will send GARP and advertisement packets to inform others that backup switch has become the new Master. After the switch update, their MAC tables are updated. (Refer to Figure. 2)
3. The VRRP standard protocol was defined in RFC 3768 and you can see the document on this website.
4. VRRP refers the active switch as the master and all other ones are in the backup state.
5. The virtual MAC address which is mapping to virtual IP is 00-00-5E-00-01-xx. (XX will depends on VRID.)
6. The master switch send the advertisement packet to 224.0.0.18 periodically in 1 second interval by default.

VRRP can also be set up to use preemption, which allows a higher-priority switch to take over as the master even if the current master device is still functional. This can be useful when the higher-priority switch is available again after a period of downtime.

In summary, VRRP is a valuable protocol that provides redundancy in network environments where high availability is critical. It enables multiple devices to act as a single virtual router, ensuring network traffic continues to flow in the event of a device failure.

## VRRP

**Menu Path: Redundancy > Layer 3 Redundancy > VRRP**

This page lets you configure the VRRP settings for your device.

This page includes these tabs:

- Settings
- Status

## VRRP - Settings

**Menu Path: Redundancy > Layer 3 Redundancy > VRRP - Settings**

This page lets you configure the VRRP settings for your device.

### VRRP Settings

VRRP \*  
Disabled ▼ 🔔

---

Version \*  
V2 ▼

---

APPLY

UI Setting	Description	Valid Range	Default Value
<b>VRRP</b>	Enable or disable VRRP for the device.	Enabled / Disabled	Disabled
<b>Version</b>	Select the VRRP version to use.	V2 / V3	V2

### VRRP List

<input type="checkbox"/>	Enable	Interface	VRRID	Priority	Virtual Router IP Address	Advertisement Interval	Preempt Mode	Preempt Delay	Accept Mode	Auth Type	Tracking ID	Decrement
<input type="checkbox"/>	<input checked="" type="checkbox"/>	vlan1	4	2	192.168.127.250	30	Enabled	5	Enabled	None	--	--
<input type="checkbox"/>	<input checked="" type="checkbox"/>	vlan1	3	2	192.168.127.252	30	Enabled	4	Enabled	Simple	--	--


Max: 40

UI Setting	Description
<b>Enable</b>	Shows whether the VRRP interface is enabled.

UI Setting	Description
<b>Interface</b>	Shows which network interface is used for the VRRP interface.
<b>VRID</b>	Shows the virtual router ID for the VRRP interface, which is used to assign the virtual router to a VRRP group.
<b>Priority</b>	Shows the priority of the VRRP interface. Higher numbers indicate higher priority, with 254 being the highest.
<b>Virtual Router IP Address</b>	Shows the IP address of the VRRP interface.
<b>Advertisement Interval (ms)</b>	Shows the advertisement interval for the VRRP interface in milliseconds.
<b>Preempt Mode</b>	Shows the preemption status of the VRRP interface.
<b>Preempt Delay</b>	Shows the preempt delay value of the VRRP interface.
<b>Accept Mode</b>	Shows whether Accept Mode is enabled for the VRRP interface. When enabled, the virtual router designated as the master will allow others to access its own virtual IP address.
<b>Auth Type</b>	Shows the auth type of the VRRP interface, if VRRP V2 is being used.
<b>Tracking ID</b>	Shows the tracking ID of the VRRP interface.
<b>Decrement</b>	Shows the decrement value of the VRRP interface. Within a VRRP interface, the decrement feature dynamically adjusts the priority based on the status of tracked ports. If a tracked port becomes inactive (link down), the VRRP priority is reduced by a predefined decrement value. This ensures that a router with fewer active ports has a lower priority, minimizing the risk of a split brain scenario.

## VRRP - Create Virtual Router

### Menu Path: Redundancy > Layer 3 Redundancy > VRRP - Settings

Clicking the **Add** (  ) icon on the **Redundancy > Layer 3 Redundancy > VRRP - Settings** page will open this dialog box. This dialog lets you create a new virtual router for your device.

Click **CREATE** to save your changes and add the new virtual router.

## 🔒 Limitations

You can create up to 40 virtual routers.

### Create a Virtual Router

Virtual Router \*


Interface \*  VRID \*   
1 - 255

Priority \*   
1 - 254


Virtual Router IP Address \*

Advertisement Interval \*  ms  
30 - 40000

Preempt Mode \*




Auth Type \*  Authentication Key \*    
0 / 8

Accept Mode \*

Tracking ID  

UI Setting	Description	Valid Range	Default Value
<b>Virtual Router</b>	Enable or disable the VRRP interface.	Enabled / Disabled	N/A
<b>Interface</b>	Specify which network interface to use for the VRRP interface.	Drop-down list of interfaces	N/A



UI Setting	Description	Valid Range	Default Value
<b>VRID (Virtual Router ID)</b>	Specify the virtual router ID to use for the VRRP interface. The virtual router ID is used to assign the virtual router to a VRRP group.  <div style="background-color: #f0f0f0; padding: 5px; border: 1px solid #ccc;"> <p> <b>Note</b></p> <p>Devices that operate as master/backup should have the same ID. Each interface supports one virtual router ID.</p> </div>	1 to 255	N/A
<b>Priority</b>	Specify the priority of the VRRP interface. Higher numbers indicate higher priority, with 254 being the highest.  <div style="background-color: #f0f0f0; padding: 5px; border: 1px solid #ccc;"> <p> <b>Note</b></p> <p>If multiple devices have the same priority, the device with the highest IP address will have priority.</p> </div>	1 to 254	N/A
<b>Virtual Router IP Address</b>	Specify the virtual router IP address for the VRRP interface.  <div style="background-color: #f0f0f0; padding: 5px; border: 1px solid #ccc;"> <p> <b>Note</b></p> <p>Devices in the same VRRP group must be in the same subnet.</p> </div>	Valid IP address	N/A
<b>Advertisement Interval</b>	Specify the advertisement interval in milliseconds for the VRRP interface. This determines the interval for the master sending packets to all slave devices to inform them who the master device is.	30 to 40000	N/A
<b>Preempt Mode</b>	Enable or disable preemption for the VRRP interface. When enabled, preemption will decide if the master will retake authority or not after being unavailable.	Enabled / Disabled	N/A
<b>Preempt Delay (if Preempt Mode is Enabled)</b>	Specify the preemption delay in seconds to use for the VRRP interface. The preempt delay is the amount of time the master will wait before retaking authority back in order to prevent the master from acting before the network connection is ready.	0 to 3600	N/A
<b>Auth Type</b>	Select the authentication type to use for the VRRP interface. <ul style="list-style-type: none"> <li>• <b>None:</b> No authentication will be used.</li> <li>• <b>Simple:</b> Simple authentication will be used.</li> </ul>	None / Simple	N/A
<b>Authentication Key</b>	Specify the authentication key to use for the VRRP interface.	0 to 8 characters	N/A

UI Setting	Description	Valid Range	Default Value
<b>Accept Mode</b>	Enable or disable Accept Mode for the VRRP interface. When enabled, the virtual router designated as the master will allow others to access its own virtual IP address.	Enabled / Disabled	N/A
<b>Tracking ID</b>	Select a tracking ID for the virtual router. Click on the select icon and choose a tracking ID.	Link to the Tracking ID List	N/A

## VRRP - Edit Virtual Router

### Menu Path: [Redundancy](#) > [Layer 3 Redundancy](#) > [VRRP - Settings](#)

Clicking the **Edit** (✎) icon for a VRRP interface on the **Redundancy > Layer 3 Redundancy > VRRP - Settings** page will open this dialog box. This dialog lets you edit an existing virtual router.

Click **APPLY** to save your changes.

### Edit This Virtual Router

Virtual Router \*

Interface                      VRID  
                        
1 - 255

Priority \*  
  
1 - 254

Virtual Router IP Address \*

Advertisement Interval \*  
  
30 - 40000                      ms

Preempt Mode \*                      Preempt Delay \*  
                        
0 - 3600                      sec.




Auth Type \*

Accept Mode \*

Tracking ID                     

UI Setting	Description	Valid Range	Default Value
<b>Virtual Router</b>	Enable or disable the VRRP interface.	Enabled / Disabled	N/A
<b>Interface</b>	Specify which network interface to use for the VRRP interface.	Drop-down list of interfaces	N/A

UI Setting	Description	Valid Range	Default Value
<b>VRID (Virtual Router ID)</b>	Specify the virtual router ID to use for the VRRP interface. The virtual router ID is used to assign the virtual router to a VRRP group.  <div style="border: 1px solid #ccc; background-color: #f9f9f9; padding: 5px; margin-top: 10px;"> <p> <b>Note</b></p> <p>Devices that operate as master/backup should have the same ID. Each interface supports one virtual router ID.</p> </div>	1 to 255	N/A
<b>Priority</b>	Specify the priority of the VRRP interface. Higher numbers indicate higher priority, with 254 being the highest.  <div style="border: 1px solid #ccc; background-color: #f9f9f9; padding: 5px; margin-top: 10px;"> <p> <b>Note</b></p> <p>If multiple devices have the same priority, the device with the highest IP address will have priority.</p> </div>	1 to 254	N/A
<b>Virtual Router IP Address</b>	Specify the virtual router IP address for the VRRP interface.  <div style="border: 1px solid #ccc; background-color: #f9f9f9; padding: 5px; margin-top: 10px;"> <p> <b>Note</b></p> <p>Devices in the same VRRP group must be in the same subnet.</p> </div>	Valid IP address	N/A
<b>Advertisement Interval</b>	Specify the advertisement interval in milliseconds for the VRRP interface. This determines the interval for the master sending packets to all slave devices to inform them who the master device is.	30 to 40000	N/A
<b>Preempt Mode</b>	Enable or disable preemption for the VRRP interface. When enabled, preemption will decide if the master will retake authority or not after being unavailable.	Enabled / Disabled	N/A
<b>Preempt Delay (if Preempt Mode is Enabled)</b>	Specify the preemption delay in seconds to use for the VRRP interface. The preempt delay is the amount of time the master will wait before retaking authority back in order to prevent the master from acting before the network connection is ready.	0 to 3600	N/A
<b>Auth Type</b>	Select the authentication type to use for the VRRP interface. <ul style="list-style-type: none"> <li>• <b>None:</b> No authentication will be used.</li> <li>• <b>Simple:</b> Simple authentication will be used.</li> </ul>	None / Simple	N/A
<b>Authentication Key</b>	Specify the authentication key to use for the VRRP interface.	0 to 8 characters	N/A

UI Setting	Description	Valid Range	Default Value
<b>Accept Mode</b>	Enable or disable Accept Mode for the VRRP interface. When enabled, the virtual router designated as the master will allow others to access its own virtual IP address.	Enabled / Disabled	N/A
<b>Tracking ID</b>	Select a tracking ID for the virtual router. Click on the select icon and choose a tracking ID.	Link to the Tracking ID List	N/A

## VRRP - Status

### Menu Path: Redundancy > Layer 3 Redundancy > VRRP - Status

This page lets you see the status of your device's VRRP interfaces.

Interface	VRID	Priority	State	Master Address
0 of 0				

UI Setting	Description
<b>Interface</b>	Shows which network interface is used for the VRRP interface.
<b>VRID</b>	Shows the virtual router ID for the VRRP interface, which is used to assign the virtual router to a VRRP group.
<b>Priority</b>	Shows the priority of the VRRP interface. Higher numbers indicate higher priority.
<b>State</b>	Shows the state of the VRRP interface. <ul style="list-style-type: none"> <li>• <b>Init State:</b> This is the initial state when a virtual router starts up.</li> <li>• <b>Master State:</b> The virtual router is acting as a master, and is responsible for forwarding packets sent to the virtual IP address and acting as the default gateway for the devices in the network.</li> <li>• <b>Backup State:</b> The virtual router is in the backup state, and waiting to take over the master role if the current master fails.</li> </ul>
<b>Master Address</b>	Shows the IP address of the current master for the VRRP interface.

# Tracking

The tracking function allows you to create tracking entries to monitor connectivity status, then trigger actions based on the state of the tracking entry.

## Tracking In Depth

Tracking entries are created to monitor for changes in connectivity, and can be used with other settings to control them based on whether the state of the tracking entry is up or down.

## Types of Tracking Entries

You can create the following types of tracking entries:

- **Interface tracking entry:** These monitor whether an interface or port is up or down.
- **Ping tracking entry:** These monitor whether a specified IP address is responding to ping packets.
- **Logical tracking entry:** These compare the status of other tracking entries by using AND, OR, NAND, or NOR operators.

## Applications for Tracking

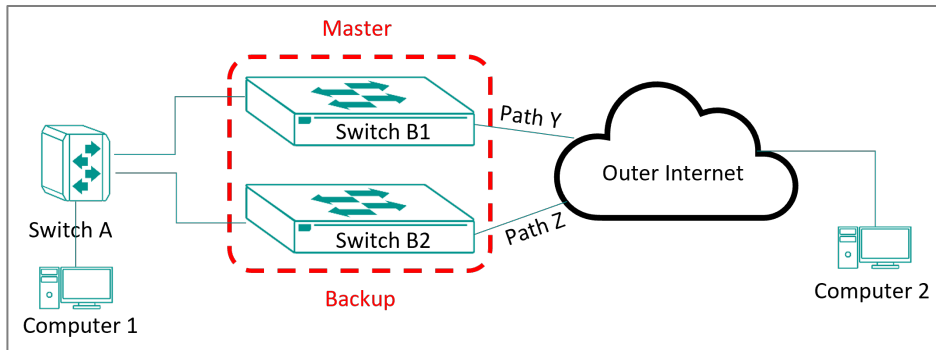
Tracking can be applied in Layer 2 and Layer 3 through various features.

### Layer 3 Tracking

- **VRRP:** Working with VRRP is a common tracking operation, and typically used for L3 switch redundancy. However, VRRP only protects traffic from L3 to L2 and does not track traffic from L3 to outside networks like the Internet. Using Tracking can address this limitation.

As shown in the following figure, VRRP can protect traffic between L2 switches (Switch A) and L3 switches (Switches B1 and B2), but it does not safeguard traffic from the L3 switches to the cloud. In this scenario, we can monitor path Y. If path

Y fails, Tracking can decrease the priority of the Master, triggering the Backup switch to become the new Master, thereby preventing traffic disruption.

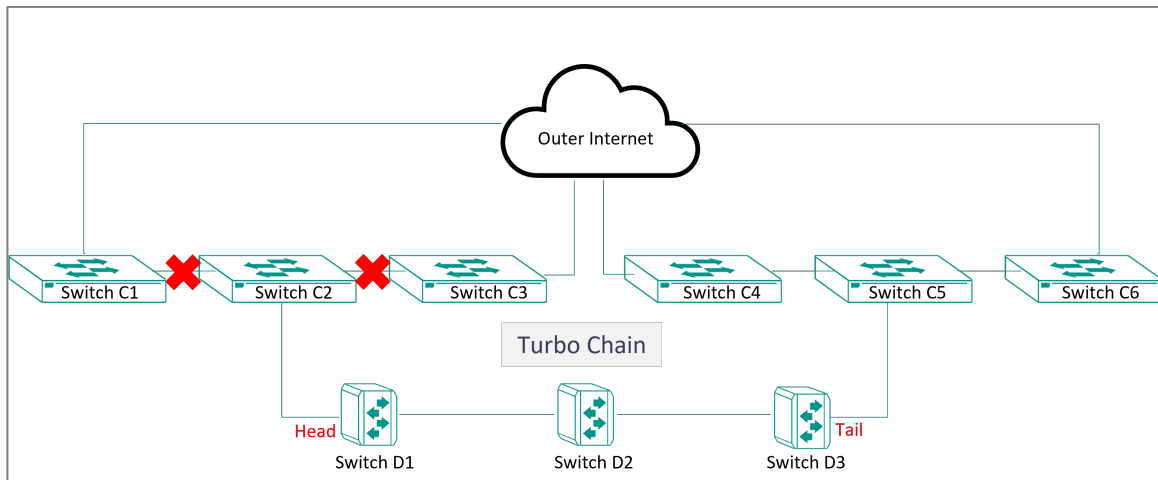


- **Static Route:** When configuring a Static Route, we set an IP address as the next hop to establish a route. However, we may not immediately know if the next hop is still active. In this case, we can use Tracking to monitor the IP address. If the next-hop becomes unavailable, we can delete the static route immediately and enable a backup static route, ensuring that routes to specific subnets remain intact.

## Layer 2 Tracking

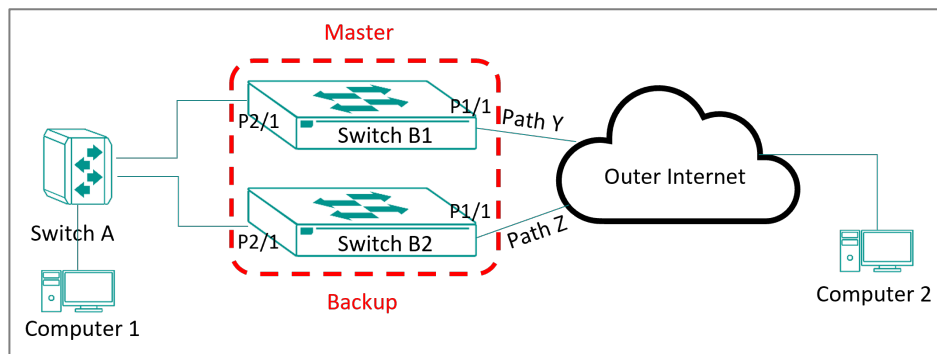
- **Port Setting:** Tracking the status of traffic and enabling or disabling a port is an increasingly important operation.

As shown in the following figure, the Turbo Chain will not detect if both paths of Switch C2 are broken. To address this, we can use Tracking to monitor traffic from Switch C2 to Switch C1 and C3. If both paths are broken, Tracking can disable the port of Switch D1, triggering the Turbo Chain to switch the Head port of Switch D1 from forwarding to blocking, and the Tail port of Switch D3 from blocking to forwarding.



## Controlling a Virtual Router With an Interface Tracking Entry

In this example, Switch B1 is the VRRP Master for a network. We will create an interface tracking rule on Switch B1 to monitor its connection to the outside Internet (Path Y through port 1/1), then use that tracking entry to decrease the VRRP priority of the switch so Switch B2 can take over as the VRRP Master.



### Before you begin:

- On Switch B1, enable VRRP and create a virtual router with 250 as its priority.
- On Switch B2, enable VRRP and create a virtual router with 200 as its priority.

### Enable Tracking

1. Sign in to Switch B1 using administrator credentials.
2. Go to **Redundancy > Tracking**.



3. In the **Settings** tab, select **Enable** for Tracking and click **APPLY**.

### Create the Interface Tracking Entry

1. Sign in to Switch B1 using administrator credentials.
2. Go to **Redundancy > Tracking**.
3. Click the



icon next to **Tracking List of Interface** and select **Interface** to show the interface tracking entries.

4. Click the **Add icon (+)** to create an interface tracking entry.
5. Specify all of the following:

Item	Value
<b>Interface Tracking</b>	Enabled
<b>Tracking ID</b>	1
<b>Interface Type</b>	Port
<b>Port</b>	1/1

6. Click **CREATE**.

### Assign the Tracking ID to the Virtual Router

1. Sign in to Switch B1 using administrator credentials.
2. Go to **Redundancy > Layer 3 Redundancy > VRRP**.
3. Click the **Edit icon (✎)** next to the virtual router to edit it.
4. Click the **Select Tracking ID icon (≡✓)**.
5. Select 1, then click **SELECT**.
6. Enter 100 for the **Decrement** value.
7. Click **APPLY**.

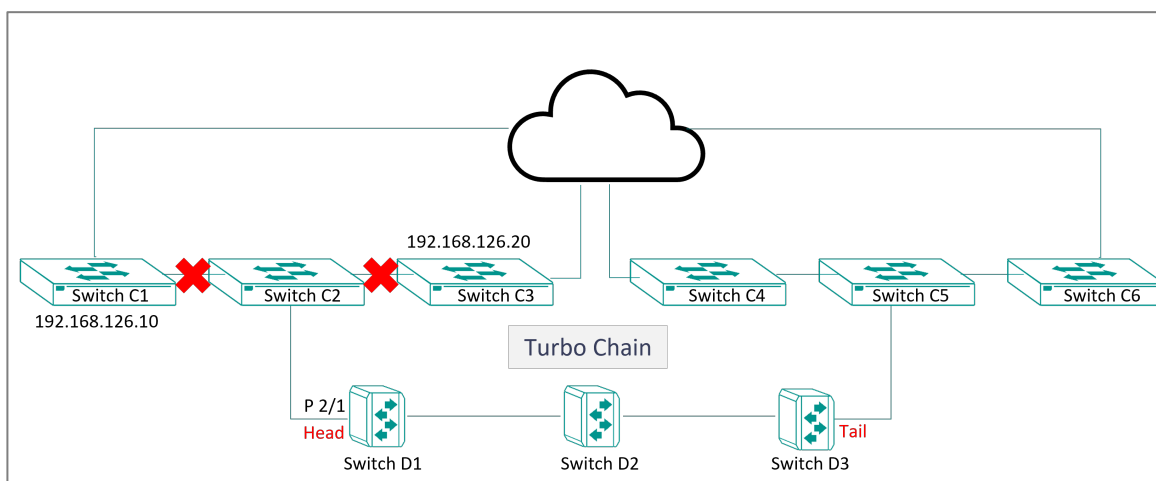
### Results:

We created a mechanism to change the VRRP Master by tracking the state of the

interface connected to the outside Internet. If port status of Port 1/1 on Switch B1 (which is connected to the Internet using Path Y) goes down, the VRRP Priority of the VRRP Master (Switch B1) will decrease by 100 (based on the settings in the example), so that the new VRRP Priority of Switch B1 will be 150. The priority of Switch B2 remains 200, and will make Switch B2 become the new VRRP Master, and Switch B1 will become the VRRP Backup.

## Controlling a Port Through Ping and Logical Tracking Entries

In this example, we will create ping tracking entries on Switch D1 to monitor traffic by pinging two different target IPs. We will then combine these tracking entries by using a logical tracking entry, and use the logical tracking entry to control a port.



### Enable Tracking

1. Sign in to the device using administrator credentials.
2. Go to **Redundancy > Tracking**.
3. In the **Settings** tab, select **Enable** for Tracking and click **APPLY**.

### Create the Ping Tracking Entries

1. Sign in to the device using administrator credentials.
2. Go to **Redundancy > Tracking**.
3. Click the

icon next to **Tracking List of Interface** and select **Ping** to show the ping tracking entries.

4. Click the **Add icon (+)** to create a ping tracking entry.
5. Specify all of the following:

Item	Value
<b>Ping Tracking</b>	Enabled
<b>Tracking ID</b>	2
<b>IP Address</b>	192.168.126.10

6. Click **CREATE**.
7. Repeat the above steps to create the second ping tracking entry, but use these values:

Item	Value
<b>Ping Tracking</b>	Enabled
<b>Tracking ID</b>	3
<b>IP Address</b>	192.168.126.20

### Create the Logical Tracking Entry

1. Sign in to the device using administrator credentials.
2. Go to **Redundancy > Tracking**.
3. Click the



icon next to **Tracking List of Interface** and select **Logical** to show the logical tracking entries.

4. Click the **Add icon (+)** to create a logical tracking entry.
5. Specify all of the following:

Item	Value
<b>Ping Tracking</b>	Enabled
<b>Tracking ID</b>	4
<b>Logical List</b>	<ul style="list-style-type: none"> <li>• 2</li> <li>• 3</li> </ul>
<b>Logical Operator</b>	AND

6. Click **CREATE**.

### Assign the Tracking ID to the Port

1. Sign in to the device using administrator credentials.
2. Go to **Port > Port Interface > Port Settings**.
3. Click the **Edit icon** (✎) for port 2/1.
4. Click the **Select Tracking ID icon** (≡✓).
5. Select 4, then click **SELECT**.
6. Click **APPLY**.

### Results:

We created a mechanism to monitor the traffic status if the path from Switch D1 to Switch C1 and C3 by pinging their IP addresses. If Switches C1 and C3 are both unresponsive (no response from pings to 192.168.126.10 and 192.168.126.20), Tracking ID 4 will change to Down, and Port 2/1 of Switch D1 will be disabled. This will trigger a Turbo Chain topology change and changes the Tail path from blocking to forwarding, allowing Switch D1, D2, and D3 to stay connected to the rest of the network.

## Controlling a Static Route Through an Interface Tracking Entry

This example shows how to create an interface tracking entry to monitor an interface, then use that tracking entry to control a static route.

### Before you begin:

- Create a static route for the interface tracking entry to control

### Enable Tracking

1. Sign in to the device using administrator credentials.
2. Go to **Redundancy > Tracking**.
3. In the **Settings** tab, select **Enable** for Tracking and click **APPLY**.

### Create the Interface Tracking Entry

1. Sign in to the device using administrator credentials.
2. Go to **Redundancy > Tracking**.
3. Click the



icon next to **Tracking List of Interface** and select **Interface** to show the interface tracking entries.

4. Click the **Add icon (+)** to create an interface tracking entry.
5. Specify all of the following:

Item	Value
<b>Interface Tracking</b>	Enabled
<b>Tracking ID</b>	5
<b>Interface Type</b>	Network Interface
<b>Network Interface</b>	Select the interface you want to monitor

6. Click **CREATE**.

### Assign the Tracking ID to the Static Route

1. Sign in to the device using administrator credentials.
2. Go to **Routing > Unicast Route > Static Routing**.
3. Click the **Edit icon (✎)** next to the static route to edit it.
4. Click the **Select Tracking ID icon (≡✓)**.
5. Select 5, then click **SELECT**.
6. Click **APPLY**.

## Results:

The status of the static route will be connected to the status of the vlan1 interface. When the vlan1 interface is up, the static route will be enabled. When the vlan1 interface is down, the static route will be disabled.

## Tracking

### Menu Path: Redundancy > Tracking

This page lets you manage the status tracking feature of your device.

This page includes these tabs:

- Settings
- Status

## Tracking - Settings

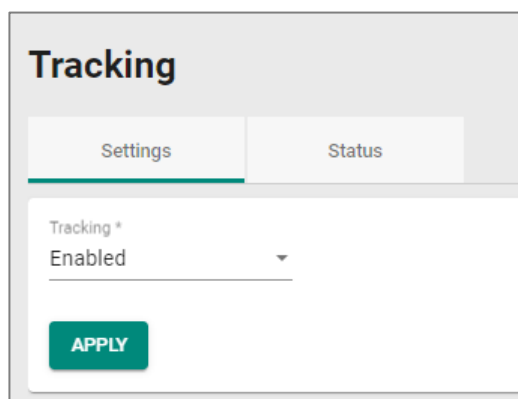
### Menu Path: Redundancy > Tracking - Settings

This tab lets you create and manage status tracking entries.

#### Limitations

You can create up to 16 tracking entries.

## Tracking Settings



The screenshot shows the 'Tracking' configuration page. At the top, there are two tabs: 'Settings' (which is active) and 'Status'. Below the tabs, there is a 'Tracking \*' dropdown menu currently set to 'Enabled'. At the bottom of the settings area, there is a green 'APPLY' button.

UI Setting	Description	Valid Range	Default Value
<b>Tracking</b>	Enable or disable status tracking for the device.	Enabled / Disabled	Disabled

## Tracking List of Interface

If **Tracking List of Interface** is selected from the drop-down menu, this table will appear.

Tracking List of Interface ▾							
+							
<input type="checkbox"/>	Tracking ID	Status	Interface	Down to Up	Up Delay (sec.)	Up to Down	Down Delay (sec.)
<input type="checkbox"/>	1	Enabled	Port 1/1	Enabled	0	Enabled	0
<input type="checkbox"/>	2	Enabled	vlan1	Enabled	10	Enabled	0

UI Setting	Description
<b>Tracking ID</b>	Shows the tracking ID for entry.
<b>Status</b>	Shows whether the entry is enabled.
<b>Interface</b>	Shows the interface monitored by the tracking ID.
<b>Down to Up</b>	Shows whether down to up state change is enabled for the entry. When enabled, the state for the tracking ID will change to Up if the interface status changes from down to up.
<b>Up Delay (sec.)</b>	Shows the delay in seconds the interface status must stay up to be detected as a down to up status change.
<b>Up to Down</b>	Shows whether up to down state change is enabled for the entry. When enabled, the state for the tracking ID will change to Down if the interface status changes from up to down.
<b>Down Delay (sec.)</b>	Shows the delay in seconds the interface status must stay down to be detected as an up to down status change.

## Creating an Interface Tracking Entry

### Menu Path: Redundancy > Tracking - Settings

Clicking the **Add (+)** icon on the **Redundancy > Tracking - Settings** page when **Tracking List of Interface** is selected will open this dialog box. This dialog lets you create a new interface tracking entry.

Click **CREATE** to save your changes and add the new entry.

**Create an Interface Tracking Entry**

Interface Tracking \*  
Disabled

Tracking ID \*

Interface Type \*

State Change (Down to Up) \*      Up Delay \*  
Enabled      0  
0 - 99      sec.

State Change (Up to Down) \*      Down Delay \*  
Enabled      0  
0 - 99      sec.

CANCEL      CREATE

UI Setting	Description	Valid Range	Default Value
<b>Interface Tracking</b>	Enable or disable the interface tracking ID.	Enabled / Disabled	Disabled
<b>Tracking ID</b>	Specify the tracking ID to use for this entry.	Drop-down list of tracking IDs	N/A
<b>Interface Type</b>	Select the interface type to monitor with this entry.	Port / Network Interface	N/A
<b>Port (If Interface Type is Port)</b>	Specify which port to monitor with this entry.	Drop-down list of ports	N/A



UI Setting	Description	Valid Range	Default Value
<b>Network Interface</b> <b>(If Interface Type is Network Interface)</b>	Specify which network interface to monitor with this entry.	Drop-down list of interfaces	N/A
<b>State Change (Down to Up)</b>	<p>Enable or disable down to up state change with this entry.</p> <ul style="list-style-type: none"> <li>• <b>Enabled:</b> The state for the tracking ID will change to Up when the interface status transitions from down to up.</li> <li>• <b>Disabled:</b> The state for the tracking ID will not change when the interface status transitions from down to up.</li> </ul>	Enabled / Disabled	Enabled
<b>Up Delay</b>	Specify how long in seconds the interface status must remain up after detecting a change from down to up in order to trigger a Down to Up state change (if enabled).	0 to 99	0
<b>State Change (Up to Down)</b>	<p>Enable or disable up to down state change with this entry.</p> <ul style="list-style-type: none"> <li>• <b>Enabled:</b> The state for the tracking ID will change to Down when the interface status transitions from up to down.</li> <li>• <b>Disabled:</b> The state for the tracking ID will not change when the interface status transitions from up to down.</li> </ul>	Enabled / Disabled	Enabled
<b>Down Delay</b>	Specify how long in seconds the interface status must remain down after detecting a change from up to down in order to trigger an Up to Down state change (if enabled).	0 to 99	0

## Editing an Interface Tracking Entry

### Menu Path: Redundancy > Tracking - Settings

Clicking the **Edit** (✎) icon for an entry on the **Redundancy > Tracking - Settings** page when **Tracking List of Interface** is selected will open this dialog box. This dialog lets you edit an existing interface tracking entry.

Click **APPLY** to save your changes.

### Edit This Interface Tracking Entry

Interface Tracking \*  
Enabled

Tracking ID \*  
1

Interface Type \*  
Port

Port \*  
1/1

State Change (Down to Up) \*  
Enabled

Up Delay \*  
0  
0 - 99 sec.

State Change (Up to Down) \*  
Enabled

Down Delay \*  
0  
0 - 99 sec.

CANCEL APPLY

UI Setting	Description	Valid Range	Default Value
<b>Interface Tracking</b>	Enable or disable the interface tracking ID.	Enabled / Disabled	Disabled
<b>Tracking ID</b>	Specify the tracking ID to use for this entry.	Drop-down list of tracking IDs	N/A
<b>Interface Type</b>	Select the interface type to monitor with this entry.	Port / Network Interface	N/A
<b>Port (If Interface Type is Port)</b>	Specify which port to monitor with this entry.	Drop-down list of ports	N/A
<b>Network Interface (If Interface Type is Network Interface)</b>	Specify which network interface to monitor with this entry.	Drop-down list of interfaces	N/A
<b>State Change (Down to Up)</b>	Enable or disable down to up state change with this entry. <ul style="list-style-type: none"> <li><b>Enabled:</b> The state for the tracking ID will change to Up when the interface status transitions from down to up.</li> <li><b>Disabled:</b> The state for the tracking ID will not change when the interface status transitions from down to up.</li> </ul>	Enabled / Disabled	Enabled

UI Setting	Description	Valid Range	Default Value
<b>Up Delay</b>	Specify how long in seconds the interface status must remain up after detecting a change from down to up in order to trigger a Down to Up state change (if enabled).	0 to 99	0
<b>State Change (Up to Down)</b>	Enable or disable up to down state change with this entry. <ul style="list-style-type: none"> <li>• <b>Enabled:</b> The state for the tracking ID will change to Down when the interface status transitions from up to down.</li> <li>• <b>Disabled:</b> The state for the tracking ID will not change when the interface status transitions from up to down.</li> </ul>	Enabled / Disabled	Enabled
<b>Down Delay</b>	Specify how long in seconds the interface status must remain down after detecting a change from up to down in order to trigger an Up to Down state change (if enabled).	0 to 99	0

## Deleting an Interface Tracking Entry

### Menu Path: Redundancy > Tracking - Settings

You can delete an entry by using the checkboxes to select the entries you want to delete, then clicking the **Delete** (🗑️) icon.

## Tracking List of Ping

If **Tracking List of Ping** is selected from the drop-down menu, this table will appear.

Tracking List of Ping ▾									
<input type="checkbox"/>	Tracking ID	Status	IP Address	Interval (ms)	Timeout (ms)	Down to Up	Received (packets)	Up to Down	Lost (packets)
<input type="checkbox"/>	3	Enabled	192.168.127.26	1000	1000	Enabled	3	Disabled	3
<input type="checkbox"/>	4	Enabled	192.168.126.10	1000	1000	Enabled	5	Enabled	5

UI Setting	Description
<b>Tracking ID</b>	Shows the ID for the tracking rule.

UI Setting	Description
<b>Status</b>	Shows the status of the tracking rule.
<b>IP Address</b>	Shows the IP Address monitored by the tracking rule.
<b>Interval (ms)</b>	Shows the interval in milliseconds between state checks for the tracking rule.
<b>Timeout (ms)</b>	Shows the timeout in milliseconds to wait for the IP address to respond to a ping packet before detecting a timeout and setting the status to down.
<b>Down to Up</b>	Shows whether down to up state change is enabled for the entry. When enabled, the state for the tracking ID will change to Up if the IP address status changes from down to up.
<b>Received (packets)</b>	Shows the number of ping response packets that must be received before the status of the IP address changes to up.
<b>Up to Down</b>	Shows whether up to down state change is enabled for the entry. When enabled, the state for the tracking ID will change to Down if the IP address status changes from up to down.
<b>Lost (packets)</b>	Shows the number of ping request packets that must be lost before the status of the IP address changes to down.

## Creating a Ping Tracking Entry

### Menu Path: Redundancy > Tracking - Settings

Clicking the **Add (+)** icon on the **Redundancy > Tracking - Settings** page when **Tracking List of Ping** is selected will open this dialog box. This dialog lets you create a new ping tracking entry.

Click **CREATE** to save your changes and add the new entry.

### Create a Ping Tracking Entry

Ping Tracking \*  
 Disabled

Tracking ID \*  
 \_\_\_\_\_

IP Address \*  
 \_\_\_\_\_

Interval \*  
 1000  
 500 - 100000 ms

Timeout \*  
 1000  
 500 - 100000 ms

State Change (Down to Up) \*  
 Enabled

Received \*  
 3  
 1 - 99 packets

State Change (Up to Down) \*  
 Enabled

Lost \*  
 3  
 1 - 99 packets

CANCEL CREATE

UI Setting	Description	Valid Range	Default Value
<b>Ping Tracking</b>	Enable or disable the ping tracking ID.	Enabled / Disabled	Disabled
<b>Tracking ID</b>	Specify the tracking ID to use for this entry.	Drop-down list of Tracking IDs	N/A
<b>IP Address</b>	Specify the IP Address to monitor with this entry.	Valid IP address	
<b>Interval</b>	Specify the interval in milliseconds between state checks for the tracking rule.	500 - 100000	1000
<b>Timeout</b>	Specify the timeout in milliseconds to wait for the IP address to respond to a ping packet before detecting a timeout and detecting the IP address as down.	500 - 100000	1000

UI Setting	Description	Valid Range	Default Value
<b>State Change (Down to Up)</b>	<p>Enable or disable down to up state change with this entry.</p> <ul style="list-style-type: none"> <li>• <b>Enabled:</b> The state for the tracking ID will change to Up when the IP address status transitions from down to up.</li> <li>• <b>Disabled:</b> The state for the tracking ID will not change when the IP address status transitions from down to up.</li> </ul>	Enabled / Disabled	Enabled
<b>Received</b>	Specify the number of ping response packets that must be received before the status of the IP address changes to up.	1 - 99	3
<b>State Change (Up to Down)</b>	<p>Enable or disable up to down state change with this entry.</p> <ul style="list-style-type: none"> <li>• <b>Enabled:</b> The state for the tracking ID will change to Down when the IP address status transitions from up to down.</li> <li>• <b>Disabled:</b> The state for the tracking ID will not change when the IP address status transitions from up to down.</li> </ul>	Enabled / Disabled	Enabled
<b>Lost</b>	Specify the number of ping request packets that must be lost before the status of the IP address changes to down.	1 - 99	3

## Editing a Ping Tracking Entry

### Menu Path: Redundancy > Tracking - Settings

Clicking the **Edit** (✎) icon for an entry on the **Redundancy > Tracking - Settings** page when **Tracking List of Ping** is selected will open this dialog box. This dialog lets you edit an existing ping tracking entry.

Click **APPLY** to save your changes.

### Edit This Ping Tracking Entry

Ping Tracking \*  
Enabled

Tracking ID \*  
3

IP Address \*  
192.168.127.26

Interval \*  
1000  
500 - 100000 ms

Timeout \*  
1000  
500 - 100000 ms

State Change (Down to Up) \*  
Enabled

Received \*  
3  
1 - 99 packets

State Change (Up to Down) \*  
Disabled

Lost \*  
3  
1 - 99 packets


CANCEL APPLY

UI Setting	Description	Valid Range	Default Value
<b>Ping Tracking</b>	Enable or disable the ping tracking ID.	Enabled / Disabled	Disabled
<b>Tracking ID</b>	Specify the tracking ID to use for this entry.	Drop-down list of Tracking IDs	N/A
<b>IP Address</b>	Specify the IP Address to monitor with this entry.	Valid IP address	
<b>Interval</b>	Specify the interval in milliseconds between state checks for the tracking rule.	500 - 100000	1000
<b>Timeout</b>	Specify the timeout in milliseconds to wait for the IP address to respond to a ping packet before detecting a timeout and detecting the IP address as down.	500 - 100000	1000

UI Setting	Description	Valid Range	Default Value
<b>State Change (Down to Up)</b>	<p>Enable or disable down to up state change with this entry.</p> <ul style="list-style-type: none"> <li>• <b>Enabled:</b> The state for the tracking ID will change to Up when the IP address status transitions from down to up.</li> <li>• <b>Disabled:</b> The state for the tracking ID will not change when the IP address status transitions from down to up.</li> </ul>	Enabled / Disabled	Enabled
<b>Received</b>	Specify the number of ping response packets that must be received before the status of the IP address changes to up.	1 - 99	3
<b>State Change (Up to Down)</b>	<p>Enable or disable up to down state change with this entry.</p> <ul style="list-style-type: none"> <li>• <b>Enabled:</b> The state for the tracking ID will change to Down when the IP address status transitions from up to down.</li> <li>• <b>Disabled:</b> The state for the tracking ID will not change when the IP address status transitions from up to down.</li> </ul>	Enabled / Disabled	Enabled
<b>Lost</b>	Specify the number of ping request packets that must be lost before the status of the IP address changes to down.	1 - 99	3

## Deleting a Ping Tracking Entry

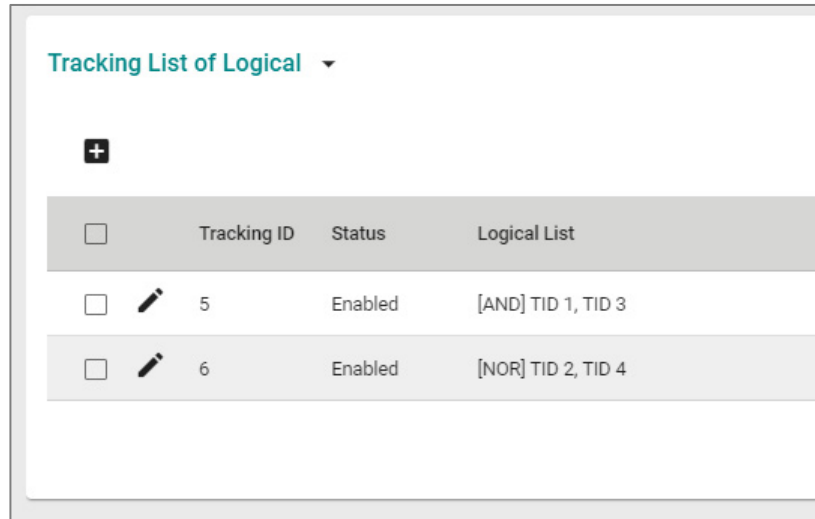
### Menu Path: Redundancy > Tracking - Settings

You can delete an entry by using the checkboxes to select the entries you want to delete, then clicking the **Delete** (  ) icon.

## Tracking List of Logical

If **Tracking List of Logical** is selected from the drop-down menu, this table will appear.





UI Setting	Description
<b>Tracking ID</b>	Shows the ID for the tracking rule.
<b>Status</b>	Shows the status of the tracking rule.
<b>Logical List</b>	Shows the logical rule and the Tracking IDs it contains.

## Creating a Logical Tracking Entry

### Menu Path: Redundancy > Tracking - Settings

Clicking the **Add (+)** icon on the **Redundancy > Tracking - Settings** page when **Tracking List of Logical** is selected will open this dialog box. This dialog lets you create a new logical tracking entry.

Click **CREATE** to save your changes and add the new entry.

### Create a Logical Tracking Entry

Logical Tracking \*  
Disabled ▼

Tracking ID \*  
 ▼

Logical List \*  
 ▼

Logical Operator \*  
AND ▼

CANCEL
CREATE

UI Setting	Description	Valid Range	Default Value
<b>Logical Tracking</b>	Enable or disable the logical tracking ID.	Enabled / Disabled	Disabled
<b>Tracking ID</b>	Specify the tracking ID to use for this entry. <div style="background-color: #f0f0f0; padding: 5px; margin-top: 10px;"> <p><b>Note</b></p> <p>The tracking ID for a logical tracking rule must be higher than the tracking IDs used in the logical list for the rule.</p> </div>	Drop-down list of Tracking IDs	N/A
<b>Logical List</b>	Specify which tracking IDs you want to monitor for this entry. <div style="background-color: #f0f0f0; padding: 5px; margin-top: 10px;"> <p><b>Note</b></p> <p>You need to set up a tracking ID before you can include it in a logical list.</p> </div>	Drop-down list of existing Tracking IDs	N/A

UI Setting	Description	Valid Range	Default Value
<b>Logical Operator</b>	<p>Specify how the state of the logical tracking rule should change based on the state of the tracking IDs in the logical list.</p> <ul style="list-style-type: none"> <li>• <b>AND:</b> When all tracking IDs in the logical list are Up, the state will be Up. Otherwise, the state will be Down.</li> <li>• <b>OR:</b> If any of the tracking IDs in the logical list are Up, the state will be Up. Otherwise, the state will be Down.</li> <li>• <b>NAND:</b> When all tracking IDs in the logical list are Up, the state will be Down. Otherwise, the state will be Up.</li> <li>• <b>NOR:</b> If any of the tracking IDs in the logical list are Up, the state will be Down. Otherwise, the state will be Up.</li> </ul>	AND / OR / NAND / NOR	AND

## Editing a Logical Tracking Entry

### Menu Path: Redundancy > Tracking - Settings

Clicking the **Edit** (✎) icon for an entry on the **Redundancy > Tracking - Settings** page when **Tracking List of Logical** is selected will open this dialog box. This dialog lets you edit an existing logical tracking entry.

Click **APPLY** to save your changes.

### Edit This Logical Tracking Entry



Logical Tracking \*  
Enabled ▼

Tracking ID \*  
5 ▼

Logical List \*  
1, 3 ▼


Logical Operator \*  
AND ▼

CANCEL
APPLY

UI Setting	Description	Valid Range	Default Value
<b>Logical Tracking</b>	Enable or disable the logical tracking ID.	Enabled / Disabled	Disabled
<b>Tracking ID</b>	Specify the tracking ID to use for this entry.  <div style="background-color: #f0f0f0; padding: 5px;"> <p> <b>Note</b></p> <p>The tracking ID for a logical tracking rule must be higher than the tracking IDs used in the logical list for the rule.</p> </div>	Drop-down list of Tracking IDs	N/A
<b>Logical List</b>	Specify which tracking IDs you want to monitor for this entry.  <div style="background-color: #f0f0f0; padding: 5px;"> <p> <b>Note</b></p> <p>You need to set up a tracking ID before you can include it in a logical list.</p> </div>	Drop-down list of existing Tracking IDs	N/A
<b>Logical Operator</b>	Specify how the state of the logical tracking rule should change based on the state of the tracking IDs in the logical list. <ul style="list-style-type: none"> <li>• <b>AND:</b> When all tracking IDs in the logical list are Up, the state will be Up. Otherwise, the state will be Down.</li> <li>• <b>OR:</b> If any of the tracking IDs in the logical list are Up, the state will be Up. Otherwise, the state will be Down.</li> <li>• <b>NAND:</b> When all tracking IDs in the logical list are Up, the state will be Down. Otherwise, the state will be Up.</li> <li>• <b>NOR:</b> If any of the tracking IDs in the logical list are Up, the state will be Down. Otherwise, the state will be Up.</li> </ul>	AND / OR / NAND / NOR	AND

## Deleting a Logical Tracking Entry

### Menu Path: Redundancy > Tracking - Settings

You can delete an entry by using the checkboxes to select the entries you want to delete, then clicking the **Delete** (  ) icon.

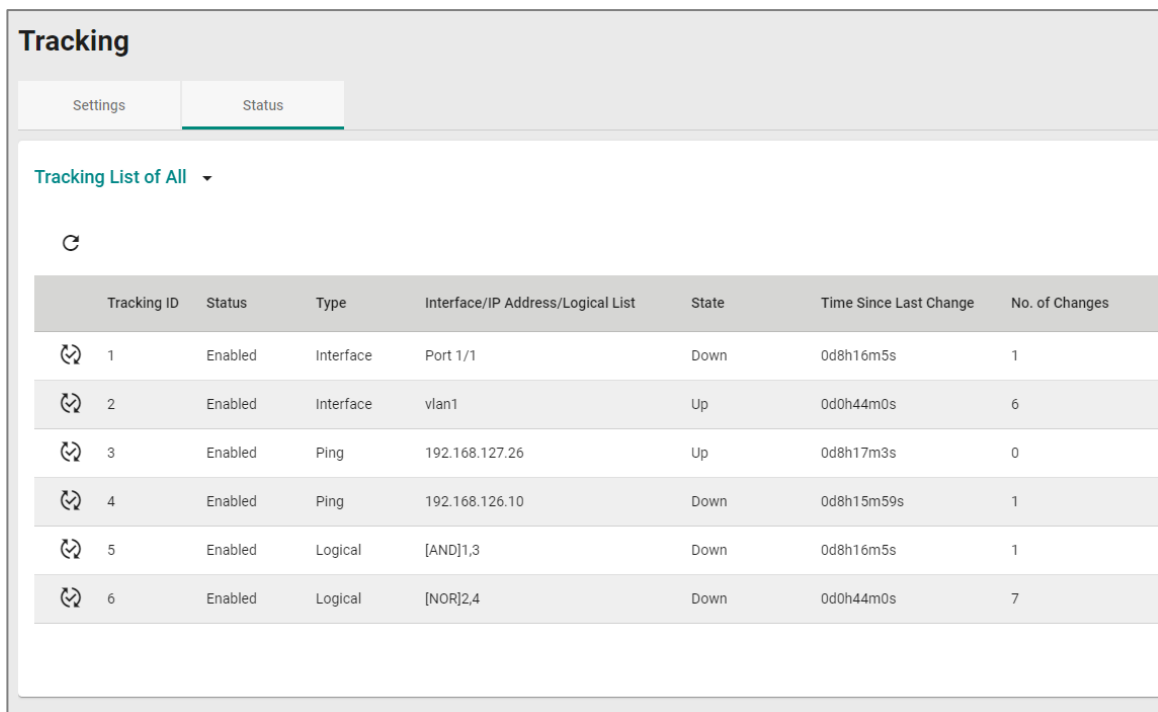
## Tracking - Status

### Menu Path: Redundancy > Tracking - Status

This page lets you see the status of your tracking entries.

### Tracking Status List

You can use the drop-down menu at the top of the table to filter the list to show all tracking entries, or only tracking entries of a specific type.



Tracking ID	Status	Type	Interface/IP Address/Logical List	State	Time Since Last Change	No. of Changes
1	Enabled	Interface	Port 1/1	Down	0d8h16m5s	1
2	Enabled	Interface	vlan1	Up	0d0h44m0s	6
3	Enabled	Ping	192.168.127.26	Up	0d8h17m3s	0
4	Enabled	Ping	192.168.126.10	Down	0d8h15m59s	1
5	Enabled	Logical	[AND]1,3	Down	0d8h16m5s	1
6	Enabled	Logical	[NOR]2,4	Down	0d0h44m0s	7

UI Setting	Description
<b>Tracking ID</b>	Shows the tracking ID for entry.
<b>Status</b>	Shows whether the tracking ID enabled.
<b>Type</b>	Shows the type of the tracking entry.
<b>Interface/ IP Address/Logical List</b>	Shows the interface, IP address, logical list this entry is monitoring, based on the tracking entry's type.
<b>State</b>	Shows the current state of the tracking ID.
<b>Time Since Last Change</b>	Shows the time since the last state change for the tracking ID.

UI Setting	Description
<b>No. of Changes</b>	Shows the number of times the tracking ID has changed state since the device was booted.

# Network Service

## Menu Path: Network Service

This section lets you configure your device's network services.

This section includes these pages:

- DHCP Server
- DHCP Relay Agent
- DNS Server

## Network Service - User Privileges

Privileges to settings are granted to the different authority levels as follows. Refer to [System > Account Management > User Accounts](#) for more information on user accounts.

Settings	Admin	Supervisor	User
DHCP Server	R/W	R/W	R
DHCP Relay Agent	R/W	R/W	R
DNS Server	R/W	R/W	R

## Configuring DHCP Server Functions

Moxa routers and L2 switches support DHCP server functionality, allowing auto-assignment of IP configurations.

### Introduction to DHCP

The Dynamic Host Configuration Protocol (DHCP) automatically provides an Internet Protocol (IP) host with an IP configuration. This can include IP address, subnet mask, DNS Configuration, and default gateway. among others.

This ensures that connected clients do not need manual IP configuration, saving time and increasing flexibility in deployments.

## Overview of DHCP Server Configuration


The integrated DHCP server of the device can operate in one of three modes.

### DHCP Pool

This mode automatically assigns IP addresses to connected devices from a user-configured IP address pool.

### MAC-based IP Assignment (Static IP)

MAC-based IP assignment, also known as static IP assignment, assigns specified IP addresses to MAC addresses of network devices. This ensures that devices maintain the same IP address, regardless of factors like connection order or lease duration. By configuring a DHCP server with table of MAC addresses and corresponding IP addresses, administrators can have more control over IP allocation, and by extension, device management and security.

 **Note**

DHCP Pool and MAC-based IP Assignment can be active at the same time.

### Port-based IP Assignment

Port-based IP assignment allocates IP addresses by the physical port on the device (Port 1, 2 etc.). This allows pre-assignment based on port, ensuring the device connected to each port will always have the same IP address.

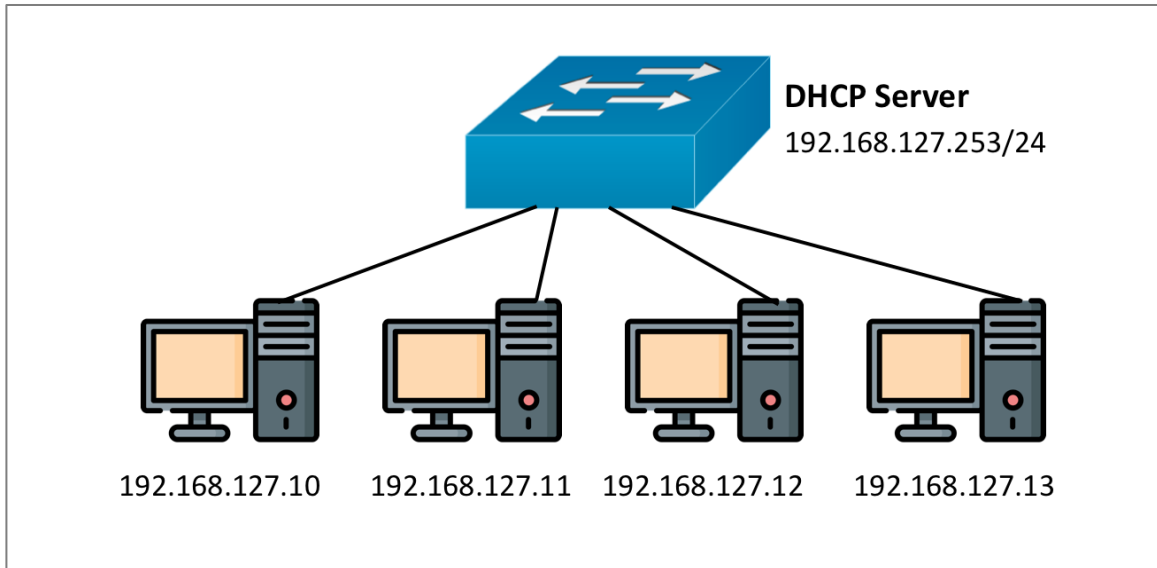
## Configuring Dynamic IP Address Assignment (DHCP Server Pool)


In this example, we configure a sample scenario with a pool of automatically-assigned IP addresses.

This scenario explains how automatically assign IP addresses to four PC clients on a subnet. We configure a switch act as DHCP server to automatically assign addresses, in



In this scenario, the switch acts as a DHCP server for the 192.168.127.xxx IP subnet and PCs are DHCP clients.



1. Sign in to the device using administrator credentials.
2. Go to **System > Network > DHCP Server > General**.
3. Under **Mode**, make sure **DHCP/MAC-based IP Assignment** is selected.
4. Under DHCP Pool Table, click  **[Add]**.

The **Create a DHCP Server Pool** screen appears.


5. Configure all of the following:

Option	Value
<b>Starting IP Address</b>	192.168.127.10
<b>Subnet Mask</b>	<b>24 (255.255.255.0)</b>
<b>Ending IP Address</b>	192.168.127.20
<b>Default Gateway</b>	192.168.127.253
<b>Lease Time</b>	1440
<b>DNS Server IP Address 1</b>	8.8.8.8

Option	Value
<b>DNS Server IP Address 2</b>	8.8.8.4
<b>NTP Server IP Address</b>	8.8.8.10

6. Click **Apply** to save your settings.

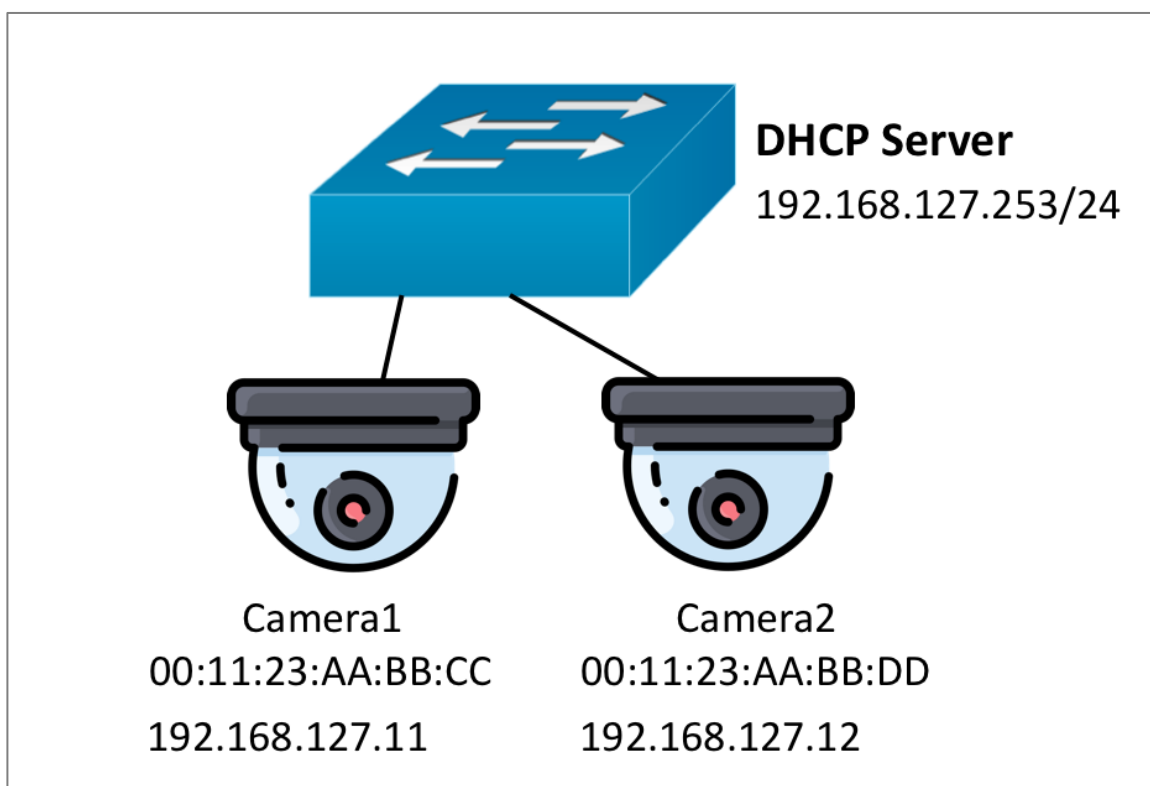
**Note**


You can delete entries by going to System > Network > DHCP Server > General, and then under DHCP, selecting one or more entries by clicking the corresponding checkbox, and then clicking  [Delete].

## Reserving IP Addresses for Specific Devices (MAC-based IP Assignment)

This scenario outlines how to reserve and automatically assign IP addresses for two cameras, ensuring that each camera always receives the same address.

We will configure the switch using MAC-based IP reservation and assignment.



1. Sign in to the device using administrator credentials.
2. Go to **System > Network > DHCP Server > General**.
3. Under **Mode**, choose **DHCP/MAC-based IP Assignment** from the drop-down list, and then click **Apply**.
4. Go to **System > Network Service > DHCP Server > MAC-based IP Assignment**, and then click  **[Add]**.

The Create Entry screen appears.

5. Configure all of the following:

Option	Value
<b>Enable</b>	<b>Enabled</b>
<b>Hostname</b>	Camera1
<b>IP Address</b>	192.168.127.11
<b>Subnet Mask</b>	<b>24 (255.255.255.0)</b>
<b>MAC Address</b>	00:11:23:AA:BB:CC
<b>Default Gateway</b>	192.168.127.253
<b>Lease Time</b>	1440
<b>DNS Server IP Address1</b>	8.8.8.8
<b>DNS Server IP Address1</b>	8.8.8.4
<b>NTP Server IP Address</b>	8.8.8.10


The entry will appear in the table.


6. Repeat this process for the second camera, with the following settings:

Option	Value
<b>Enable</b>	<b>Enabled</b>
<b>Hostname</b>	Camera2

Option	Value
<b>IP Address</b>	192.168.127.12
<b>Subnet Mask</b>	<b>24 (255.255.255.0)</b>
<b>MAC Address</b>	00:11:23:AA:BB:CC
<b>Default Gateway</b>	192.168.127.253
<b>Lease Time</b>	1440
<b>DNS Server IP Address1</b>	8.8.8.8
<b>DNS Server IP Address1</b>	8.8.8.4
<b>NTP Server IP Address</b>	8.8.8.10

The entry will appear in the table.

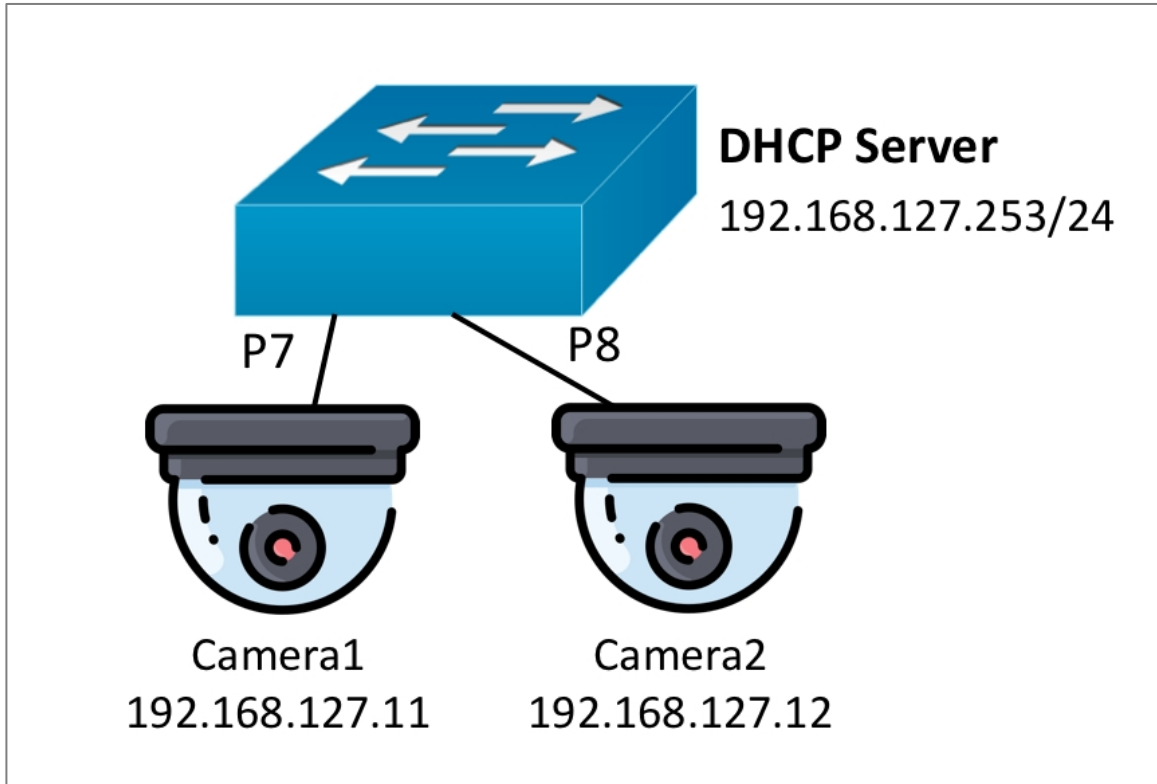
 **Note**


You can delete entries by going to System > Network Service > DHCP Server > MAC-based IP Assignment, selecting one or more entries by clicking the corresponding checkbox, and then clicking  [Delete].

## Configuring Port-based IP Assignment

This scenario assigns IP addresses to cameras based on their port of connection.

We will configure the switch as a DHCP server that uses port index-based IP assignments for each of the cameras. All ports will always assign the same IP addresses.



1. Sign in to the device using administrator credentials.
2. Go to **System > Network > DHCP Server > General**.
3. Under **Mode**, choose **Port-based IP Assignment** from the drop-down list, and then click **Apply**.
4. In the table below **Mode**, click  **[Add]**.
5. Configure all of the following:

Option	Value
<b>Enable</b>	<b>Enabled</b>
<b>Port</b>	<b>7</b>
<b>IP Address</b>	192.168.127.11
<b>Subnet Mask</b>	<b>24 (255.255.255.0)</b>
<b>Default Gateway</b>	192.168.127.253

Option	Value
<b>Lease Time</b>	1440
<b>DNS Server IP Address1</b>	8.8.8.8
<b>DNS Server IP Address1</b>	8.8.8.4
<b>NTP Server IP Address</b>	8.8.8.10
<b>Hostname</b>	Camera1

The entry will appear in the table.

6. Repeat this process for the second camera, with the following settings:

Option	Value
<b>Enable</b>	<b>Enabled</b>
<b>MAC Address</b>	00:11:23:AA:BB:CC
<b>IP Address</b>	192.168.127.12
<b>Subnet Mask</b>	<b>24 (255.255.255.0)</b>
<b>Default Gateway</b>	192.168.127.253
<b>Lease Time</b>	1440
<b>DNS Server IP Address1</b>	8.8.8.8
<b>DNS Server IP Address1</b>	8.8.8.4
<b>NTP Server IP Address</b>	8.8.8.10
<b>Hostname</b>	Camera2

The entry will appear in the table.

## DHCP Server

**Menu Path: Network Service > DHCP Server**

This page lets you configure the DHCP server settings.

This page includes these tabs:

- General
- Lease Table

## DHCP Server - General

**Menu Path: Network Service > DHCP Server - General**

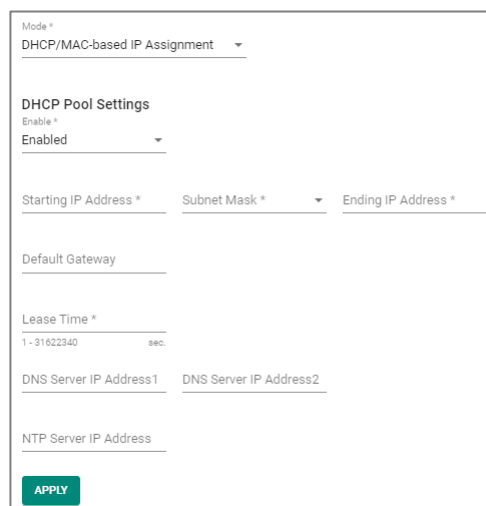
This page lets you configure the DHCP server mode and port settings.

### ⚠ Limitations

You can create up to 256 DHCP/MAC-based IP assignments.

## DHCP Server Settings

If **Mode** is set to **DHCP/MAC-based IP Assignment**, and **DHCP Pool Settings** is **Enabled**, these settings will appear.



The screenshot shows a configuration form for DHCP Pool Settings. At the top, there is a dropdown menu for 'Mode' set to 'DHCP/MAC-based IP Assignment'. Below this is the 'DHCP Pool Settings' section, which includes an 'Enable' dropdown set to 'Enabled'. The form contains several input fields: 'Starting IP Address \*', 'Subnet Mask \*' (with a dropdown arrow), 'Ending IP Address \*', 'Default Gateway', 'Lease Time \*' (with a value of '1 - 31622340 sec.'), 'DNS Server IP Address1', 'DNS Server IP Address2', and 'NTP Server IP Address'. An 'APPLY' button is located at the bottom left of the form.

UI Setting	Description	Valid Range	Default Value
<b>Mode</b>	Select a DHCP server mode.	Disabled / DHCP/MAC-based IP Assignment / Port-based IP Assignment	Disabled
<b>Enable</b>	Enable or disable use of a DHCP pool.	Enabled / Disabled	Disabled
<b>Starting IP Address</b>	Specify the starting IP address of the DHCP IP pool.	Valid unicast IP address	N/A
<b>Subnet Mask</b>	Specify the subnet mask for DHCP clients in the pool.	Valid subnet mask	N/A
<b>Ending IP Address</b>	Specify the ending IP address of the DHCP IP pool.	Valid unicast IP address	N/A
<b>Default Gateway</b>	Specify the default gateway to use for DHCP clients in the pool.	Valid IP address	N/A
<b>Lease Time</b>	Specify how long in seconds a device can keep the assigned IP address before it needs to renew the lease with the DHCP server.	1 to 31622340	N/A
<b>DNS Server IP Address1</b>	Specify the IP address of the first DNS server to use for DHCP clients in the pool.	Valid IP address	N/A
<b>DNS Server IP Address2</b>	Specify the IP address of the second DNS server to use for DHCP clients in the pool.	Valid IP address	N/A
<b>NTP Server IP Address</b>	Specify the IP address of the NTP server to use for DHCP clients in the pool.	Valid IP address	N/A

## DHCP Server List - MAC-based Assignment

If **DHCP Server Mode** is set to **DHCP/MAC-based IP Assignment**, this table will appear.

Enable	Hostname	IP Address	Subnet Mask	Lease Time (sec.)	MAC Address	Default Gateway	DNS Server IP
<input checked="" type="checkbox"/>	Test	19.126.255.5	255.255.192.0	6	00:90:E8:A9:ED:2B		



UI Setting	Description
<b>Enable</b>	Shows whether MAC-based IP assignment is enabled for the MAC address.
<b>Hostname</b>	Shows the hostname to use for clients that connect to the MAC address.
<b>IP Address</b>	Shows the IP address assigned to clients that connect to the MAC address.
<b>Subnet Mask</b>	Shows the subnet mask assigned to clients that connect to the MAC address.
<b>Lease Time (sec.)</b>	Shows the lease time in seconds for IP assignments through the MAC address.
<b>MAC Address</b>	Shows the MAC address of the MAC-based IP assignment.
<b>Default Gateway</b>	Shows the default gateway for clients that connect to the MAC address.
<b>DNS Server IP Address 1</b>	Shows the IP address of the first DNS server to use for clients that connect to the MAC address.
<b>DNS Server IP Address 2</b>	Shows the IP address of the second DNS server to use for clients that connect to the MAC address.
<b>NTP Server IP Address</b>	Shows the NTP server to use for clients that connect to the MAC address.

## MAC-based IP Assignment - Creating a DHCP Server Entry

### Menu Path: Network Service > DHCP Server - General


Clicking the **Add (+)** icon on the **Network Service > DHCP Server - General** page when **DHCP Server Mode** is set to **DHCP/MAC-based IP Assignment** will open this dialog box. This dialog lets you create a new MAC-based IP assignment.

Click **CREATE** to save your changes and add the new account.

### Create Entry

Enable \*  
 Enabled ▼

---

Hostname \*   
0 / 63

---

IP Address \*      Subnet Mask \* ▼

---

MAC Address \*

---

Default Gateway

---

Lease Time \*  
 1 - 31622340      sec.

---

DNS Server IP Address 1      DNS Server IP Address 2

---

NTP Server IP Address

---

CANCEL      CREATE

UI Setting	Description	Valid Range	Default Value
<b>Enable</b>	Enable or disable the MAC-based IP assignment entry.	Enabled / Disabled	Enabled
<b>Hostname</b>	Specify a hostname for the IP assignment.	Drop-down list of ports	N/A
<b>IP Address</b>	Specify the IP address for the IP assignment.	Valid IP address	N/A
<b>Subnet Mask</b>	Select the subnet mask for the IP assignment.	Drop-down list of subnet masks	N/A
<b>MAC Address</b>	Specify the MAC address that this IP assignment will apply to.	Valid MAC address	

UI Setting	Description	Valid Range	Default Value
<b>Default Gateway</b>	Specify the default gateway for the IP assignment.	Valid IP address	N/A
<b>Lease Time</b>	Specify the lease time in seconds for the IP assignment.	1 to 31622340	
<b>DNS Server IP Address1</b>	Specify the IP address of the first DNS server to use for the IP assignment.	Valid IP address	N/A
<b>DNS Server IP Address2</b>	Specify the IP address of the second DNS server to use for the IP assignment.	Valid IP address	N/A
<b>NTP Server IP Address</b>	Specify the NTP server to use for the IP assignment.	Valid IP address	N/A

## DHCP Server List - Port-based Assignment

If **DHCP Server Mode** is set to **Port-based IP Assignment**, this table will appear.

	Port	Enable	IP Address	Subnet Mask	Lease Time (sec.)	Default Gateway	DNS Server IP Address1	DNS Server IP Address2	NTP Server IP Address	Hostname	Domain Name	Log Server IP Address
<input type="checkbox"/>	7	Enabled	192.168.7.252	255.255.255.0	86400	192.168.7.254						

UI Setting	Description
<b>Port</b>	Shows the port number the entry is for.
<b>Enable</b>	Shows whether port-based IP assignment is enabled for the port.
<b>IP Address</b>	Shows the IP address assigned to clients that connect to the port.
<b>Subnet Mask</b>	Shows the subnet mask assigned to clients that connect to the port.
<b>Lease Time (sec.)</b>	Shows the lease time in seconds for IP assignments through the port.
<b>Default Gateway</b>	Shows the default gateway for clients that connect to the port.
<b>DNS Server IP Address 1</b>	Shows the IP address of the first DNS server to use for clients that connect to the port.
<b>DNS Server IP Address 2</b>	Shows the IP address of the second DNS server to use for clients that connect to the port.

UI Setting	Description
<b>NTP Server IP Address</b>	Shows the NTP server to use for clients that connect to the port.
<b>Hostname</b>	Shows the hostname to use for clients that connect to the port.
<b>Domain Name</b>	Shows the domain name to use for clients that connect to the port.
<b>Log Server IP Address</b>	Shows the IP address of the log server to use for clients that connect to the port.

## Port-based Assignment - Creating a DHCP Server Entry

### Menu Path: Network Service > DHCP Server - General

Clicking the **Add (+)** icon on the **Network Service > DHCP Server - General** page will open this dialog box. This dialog lets you create a new port-based IP assignment.

Click **CREATE** to save your changes and add the new account.

**Create Entry**

Enable \*  
Enabled

Port \*

IP Address \*      Subnet Mask \*

Lease Time \*  
1 - 31622340 sec.

Default Gateway

DNS Server IP Address1      DNS Server IP Address2

NTP Server IP Address

Hostname      Domain Name  
0 / 63      0 / 63

Log Server IP Address

CANCEL      **CREATE**

UI Setting	Description	Valid Range	Default Value
<b>Enable</b>	Enable or disable the port-based IP assignment entry.	Enabled / Disabled	Enabled

UI Setting	Description	Valid Range	Default Value
<b>Port</b>	Select which port the DHCP server will assign an IP address for.	Drop-down list of ports	N/A
<b>IP Address</b>	Specify the IP address assigned to clients that connect to the port.	Valid IP address	N/A
<b>Subnet Mask</b>	Select the subnet mask assigned to clients that connect to the port.	Drop-down list of subnet masks	N/A
<b>Lease Time</b>	Specify the lease time in seconds for IP assignments through the port.	1 to 31622340	N/A
<b>Default Gateway</b>	Specify the default gateway for clients that connect to the port.	Valid IP address	N/A
<b>DNS Server IP Address1</b>	Specify the IP address of the first DNS server to use for clients that connect to the port.	Valid IP address	N/A
<b>DNS Server IP Address2</b>	Specify the IP address of the second DNS server to use for clients that connect to the port.	Valid IP address	N/A
<b>NTP Server IP Address</b>	Specify the NTP server to use for clients that connect to the port.	Valid IP address	N/A
<b>Hostname</b>	Specify the hostname to use for clients that connect to the port.	Up to 63 characters	N/A
<b>Domain Name</b>	Specify the domain name to use for clients that connect to the port.	Up to 63 characters	N/A
<b>Log Server IP Address</b>	Specify the IP address of the log server to use for clients that connect to the port.	Valid IP address	N/A

## Lease Table

### Menu Path: [Network Service > DHCP Server - Lease Table](#)

This page lets you view the IP address lease table.

## Lease Table



Hostname	IP Address	MAC Address	Time Left
	192.168.7.252		(static)

UI Setting	Description
<b>Hostname</b>	Shows the hostname of the client.
<b>IP Address</b>	Shows the IP address leased to the client.
<b>MAC Address</b>	Shows the MAC address of the client.
<b>Time left</b>	Shows the amount of time left in seconds on the DHCP lease for the client. <b>(static)</b> means the IP address is statically assigned.

## Configuring DHCP Relay Agent

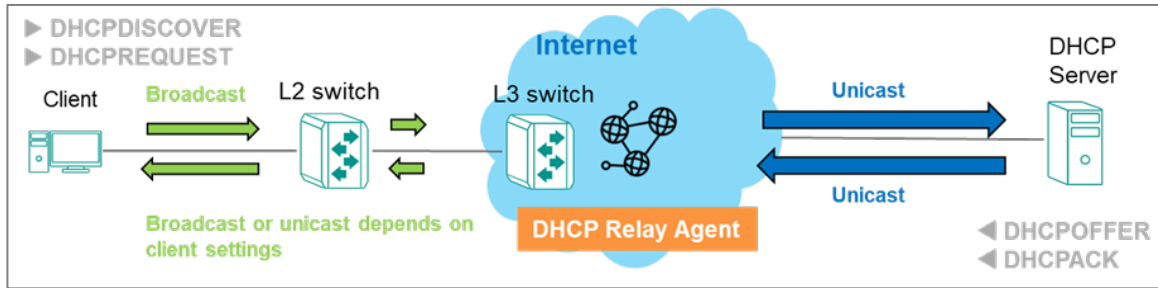
DHCP Relays can help reduce broadcast DHCP requests by relaying DHCP requests between networks.

### About DHCP Relay Agents

DHCP relay agents can provide a bridge for DHCP communication across network segments.

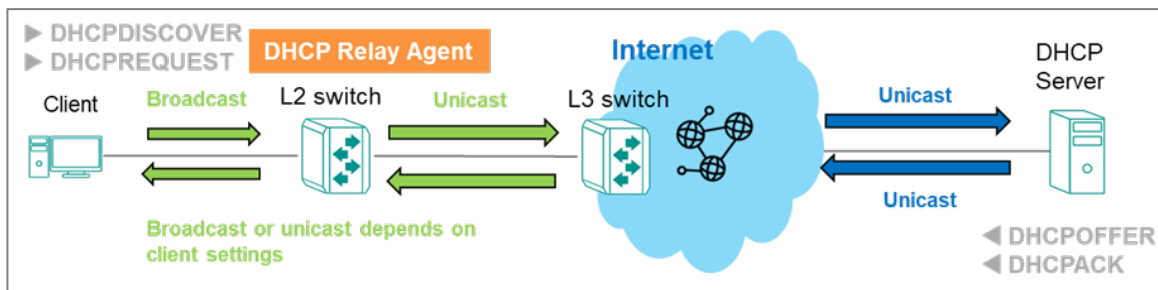
### DHCP Relays on L3 Switches

A DHCP Relay Agent on an L3 switch converts broadcast DHCP packets to unicast packets, and then routes them to the DHCP server.



## DHCP Relays on L2 Switches

On an L2 switch, the switch would convert DHCP broadcast packets to DHCP unicast packets, forward them to an L3 switch, which would then route them the DHCP server.




## Configuring DHCP Relay Agent (RKS-G4000 Series)

You can configure your switch to serve as a DHCP relay agent.

1. Sign in to the device using administrator credentials.
2. Go to **Network Service > DHCP Relay Agent > General**.
3. Under **DHCP Relay Agent**, choose **Enabled** from the drop-down menu.
4. Specify up to 4 addresses in the **DHCP Server Address** field, and then click **Apply** to save changes.


### Note

If DHCP Server Address is left blank, DHCP servers will be unable to reply to packets sent from connected clients.

5. To configure a **Port**, click the corresponding  **[Edit]** button.

6. The **Edit Port** screen appears.
7. Specify all of the following:

Option	Value
<b>Relay</b>	To enable the relay, choose <b>Enabled</b> . To disable the relay while retaining settings, choose <b>Disabled</b> .
<b>Status</b>	To accept incoming DHCP packets from DHCP servers, choose <b>Trusted</b> from the drop-down menu.

 **Note**

You can copy your settings to other ports by selecting them from the drop-down menu.

8. Click **Apply** to save your changes.

## Configuring Option 82

Option 82 provides additional information in relayed packets that can make DHCP server address allocation more effective. If your DHCP server supports it, it can provide additional information that can facilitate context-aware address allocation, as well as more flexible tracking and management.

To configure Option 82:

1. Sign in to the device using administrator credentials.
2. Go to **Network Service > DHCP Relay Agent > General**, and then click **Option 82**.
3. Specify the ID that will be sent to the relay by clicking **Remote ID Type**, and then choosing an option from the drop-down menu.

For the **Other** option, you can specify a static value of up to 64 characters.

4. To enable **Option 82** on a given **Port**, click  **[Edit]** next to the corresponding **Port**.



**Note**

Choose an Port connected to client devices. Do not choose an outbound Port.

The **Edit Port** screen appears.

5. Click **Option 82** and choose **Enable** from the drop-down menu.
6. Click **Apply** to save your settings.

## DHCP Relay Agent

**Menu Path: Network Service > DHCP Relay Agent**

This page lets you manage the DHCP Relay Agent feature of your device.

This page includes these tabs:

- General
- Option 82

### DHCP Relay Agent - General

**Menu Path: Network Service > DHCP Relay Agent - General**

This page lets you enable the DHCP Relay Agent feature and configure its related settings.

### DHCP Relay Agent Settings

**DHCP Relay Agent**

General    Option 82







DHCP Relay Agent \*  
Disabled

1st Server IP Address    2nd Server IP Address    3rd Server IP Address    4th Server IP Address

**APPLY**

UI Setting	Description	Valid Range	Default Value
<b>DHCP Relay Agent</b>	Enable or disable the DHCP Relay Agent feature on your device.	Enabled / Disabled	Disabled
<b>1st/2nd/3rd/4th Server IP Address</b>	Specify the 1st, 2nd, 3rd, and 4th server IP address.	Valid IP address	N/A

### DHCP Relay Agent - Port List

	Port	Relay	Status
	1	Disabled	Trusted
	2	Disabled	Trusted
	3	Disabled	Trusted
	4	Disabled	Trusted
	5	Disabled	Trusted
	6	Disabled	Trusted

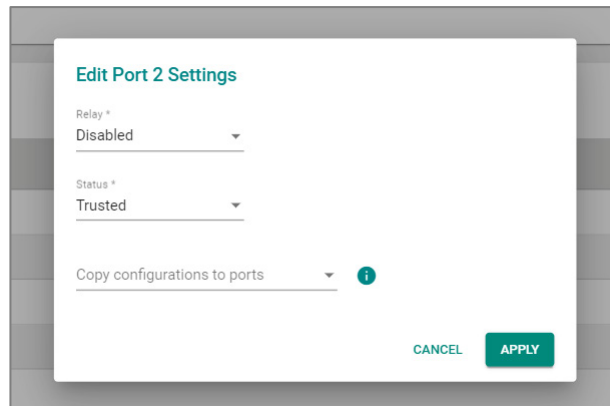
UI Setting	Description
<b>Port</b>	Shows the port number the entry is for.
<b>Relay</b>	Shows whether the relay function is enabled for the port.
<b>Status</b>	Shows the status of the relay on the port.

## DHCP Relay Agent - Edit Port Settings

### Menu Path: Network Service > DHCP Relay Agent - General

Clicking the **Edit** (✎) icon for a port on the **Network Service > DHCP Relay Agent - General** page will open this dialog box. This dialog lets you manage DHCP relay settings for the port.

Click **APPLY** to save your changes.



UI Setting	Description	Valid Range	Default Value
<b>Relay</b>	Enable or disable the relay function for the port.	Enabled / Disabled	Disabled
<b>Status</b>	Specify the relay status for the port. <ul style="list-style-type: none"><li>• <b>Trusted:</b> DHCP packets with Option 82 or with a non-zero giaddr will be accepted.</li><li>• <b>Untrusted:</b> DHCP packets with Option 82 or with a non-zero giaddr will be discarded.</li></ul>	Trusted / Untrusted	Trusted
<b>Copy configurations to ports</b>	Select the ports you want to copy this configuration to.	Drop-down list of ports	N/A

## Option 82

### Menu Path: Network Service > DHCP Relay Agent - Option 82

This page lets you manage Option 82 and its related settings.

## Option 82 Settings

### DHCP Relay Agent

General
Option 82

Remote ID Type \*

IP ▼

Remote ID Value

192.168.127.252

.....

Remote ID Display







C0A87FFC

.....

APPLY

UI Setting	Description	Valid Range	Default Value
<b>Remote ID Type</b>	Specify the remote ID type.	IP / MAC / Client ID / Other	IP
<b>Remote ID Value</b>	<p>If the <b>Remote ID Type</b> is <b>Other</b>, specify the remote ID value to use.</p> <p>For all other types, this shows the remote ID value for the selected remote ID type and cannot be edited.</p>	N/A	Varies depending on different options
<b>Remote ID Display</b>	Shows the remote ID. This field is read-only and cannot be changed.	N/A	Remote ID


## Option 82 - Port List

	Port	Option 82
	1	Disabled
	2	Disabled
	3	Disabled
	4	Disabled
	5	Disabled
	6	Disabled

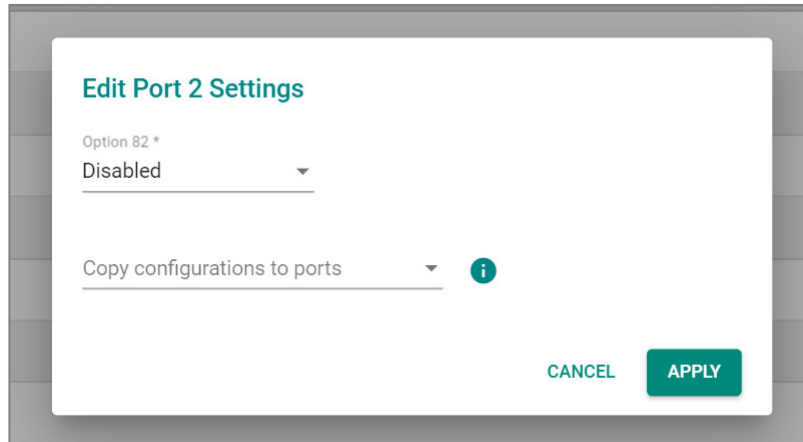
UI Setting	Description
<b>Port</b>	Shows the port number the entry is for.
<b>Option 82</b>	Shows whether Option 82 is enabled for the port.

## Option 82 - Edit Port Settings

### Menu Path: Network Service > DHCP Relay Agent - Option 82

Clicking the **Edit** () icon for an port on the **Network Service > DHCP Relay Agent - Option 82** page will open this dialog box. This dialog lets you enable or disable Option 82 for the port.

Click **APPLY** to save your changes.



UI Setting	Description	Valid Range	Default Value
<b>Option 82</b>	Enable or disable Option 82 for the port.	Enabled / Disabled	Disabled
<b>Copy configurations to ports</b>	Select the ports you want to copy this configuration to.	Drop-down list of ports	N/A

## About DNS

A Domain Name System (DNS) is a hierarchical decentralized naming system for computers, services, or other resources connected to the Internet or a private network. It translates domain names, which are human-readable identifiers for resources, into IP addresses, which are numerical identifiers used to locate and communicate with these resources.

## DNS Settings

**Menu Path:** [Network Service](#) > [DNS Settings](#)

This page lets you specify the DNS servers your device will use. Click **APPLY** to save your changes.

## DNS Settings

### DNS Settings

Primary DNS Server  
\_\_\_\_\_

Secondary DNS Server  
\_\_\_\_\_

**APPLY**

UI Setting	Description	Valid Range	Default Value
<b>Primary DNS Server</b>	Specify the IP address of the primary DNS server used by your network.	Valid IP address	N/A
<b>Secondary DNS Server</b>	Specify the IP address of the secondary DNS server used by your network.  The switch will use the secondary DNS server if the primary DNS server fails to connect.	Valid IP address	N/A

# Routing

## Menu Path: Routing

This section lets you configure the routing settings for your device.

This section includes these pages:

- Unicast Route
- Multicast Route

## Routing - User Privileges

Privileges to settings are granted to the different authority levels as follows. Refer to [System > Account Management > User Accounts](#) for more information on user accounts.

Settings	Admin	Supervisor	User
<b>Unicast Route</b>			
<b>Static Routing</b>	R/W	R/W	R
<b>OSPF Settings</b>	R/W	R/W	R
<b>OSPF Status</b>	R	R	R
<b>Routing Table</b>	R	R	R
<b>Multicast Route</b>			
<b>PIM-DM</b>	R/W	R/W	R
<b>PIM-SM Settings</b>	R/W	R/W	R
<b>PIM-SM Status</b>	R	R	R
<b>Multicast Local Route</b>	R/W	R/W	R
<b>Multicast Routing Table</b>	R	R	R



## About Unicast Routes

A static route is a manually configured network path used to deliver network traffic to a specific destination network or host. Unlike dynamic routes established by routing protocols, static routes are created and managed by a network administrator. They are typically used in small networks or situations where there is a limited number of destinations that need to be reached.

Among these static routes, a special type known as the default route, or 'gateway of last resort', plays a critical role. This default route, often designated as 0.0.0.0/0, represents a catch-all path. When a device doesn't have a specific route for a packet's destination IP address, it will utilize the default route, sending the data along this path. This ensures that all data, regardless of its destination, has a route to follow.

While both default and static routes are manually configured, they serve different purposes. Static routes are used for specific, predefined network paths, while the default route is a catch-all, used when no other path is available for a specific data packet. This allows for increased control over network traffic while ensuring that data can reach otherwise unspecified networks, typically including the public Internet.

Static routes, including default routes, offer several advantages, including:

- More control over network traffic, allowing administrators to direct traffic along specific paths.
- Less overhead and resource usage, as static routes don't require routers to exchange routing information.
- Faster convergence, since there are no routing updates to process.

However, static routes also have some disadvantages:

- May be time-consuming and prone to human error, as administrators must manually configure and update routes.
- Unable to adapt to network changes automatically, requiring manual intervention to update routing tables when network topology changes.
- May not scale well in large networks with numerous destinations and frequent changes.

In summary, static routing is a method for unicast communication in which network paths are manually configured by network administrators. While they offer more control

over network traffic and can improve performance in some cases, static routes can be time-consuming to manage and may not be well-suited for large, dynamic networks.

## Unicast Route

### Menu Path: [Routing](#) > [Unicast Route](#)

This section lets you manage unicast routes for your device.

This section includes these pages:

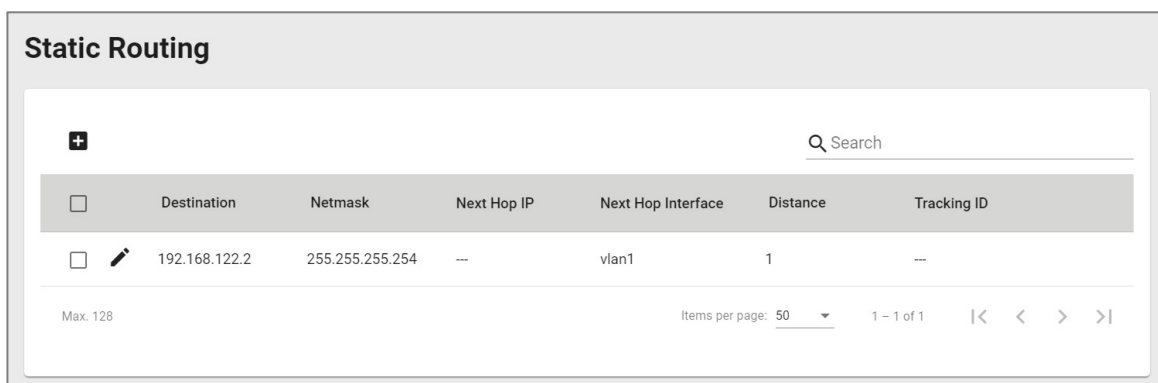
- [Static Routing](#)
- [OSPF](#)
- [Routing Table](#)

## Static Routing

### Menu Path: [Routing](#) > [Unicast Route](#) > [Static Routing](#)

This page lets you manage static routes for your device, which allows you to specify the next hop (or router) that the device will forward data to for a specific subnet. Static routes will be added to the routing table and stored on the device.

### Static Route List



The screenshot shows the 'Static Routing' configuration page. It features a table with columns for Destination, Netmask, Next Hop IP, Next Hop Interface, Distance, and Tracking ID. A single route is listed with Destination 192.168.122.2, Netmask 255.255.255.254, Next Hop IP ---, Next Hop Interface vlan1, and Distance 1. The page also includes a search bar, a '+ Add' button, and pagination controls showing 'Max. 128' items and 'Items per page: 50'.

	Destination	Netmask	Next Hop IP	Next Hop Interface	Distance	Tracking ID
<input type="checkbox"/>	192.168.122.2	255.255.255.254	---	vlan1	1	---

UI Setting	Description
<b>Destination</b>	Shows the destination IP address for the static route.
<b>Netmask</b>	Shows the subnet mask for the destination IP address.

UI Setting	Description
<b>Next Hop IP</b>	Shows the next hop IP on the path to the destination IP address.
<b>Next Hop Interface</b>	Shows the next hop Interface on the path to the destination IP address.
<b>Distance</b>	Shows the distance value used to determine the priority of the static route. Lower values have higher priority.
<b>Tracking ID</b>	Shows the tracking ID selected for the route. When the status of the tracking ID is up, the route will be enabled. When the status of the tracking ID is down, the route will be disabled.

## Create a Static Route

### Menu Path: Routing > Unicast Route > Static Routing

Clicking the **Add (+)** icon on the **Routing > Unicast Route > Static Routing** page will open this dialog box. This dialog lets you create a new static route.

Click **CREATE** to save your changes and add the new account.

### Create a Static Route

Destination \*

Netmask \*

Next Hop Type \* i


Next Hop IP  Next Hop Interface

Distance \*   
1 - 255

Tracking ID  ≡

CANCEL CREATE


UI Setting	Description	Valid Range	Default Value
<b>Destination</b>	Specify the destination IP address for the static route.	Valid IP address	N/A
<b>Netmask</b>	Specify the subnet mask for the destination IP address.	Drop-down list of subnet masks	N/A
<b>Next Hop IP</b>	Specify the next hop on the path to the destination IP.	Valid IP address	N/A
<b>Next Hop Interface</b>	Select a previously created VLAN interface or leave this field blank.	Drop-down list of interfaces	N/A
<b>Distance</b>	Specify the distance value to determine the priority of the static route. Lower values have higher priority.	1 to 255	N/A
<b>Tracking ID</b>	Select a tracking ID for the static route. When the status of the tracking ID is up, the route will be enabled. When the status of the tracking ID is down, the route will be disabled.	List of existing tracking IDs	N/A

 **Note**

You need to create a tracking ID before you can select it. Refer to [Tracking](#) for more information.

## Edit This Static Route

### Menu Path: [Routing](#) > [Unicast Route](#) > [Static Routing](#)

Clicking the **Edit** () icon on the **Routing > Unicast Route > Static Routing** page will open this dialog box. This dialog lets you edit an existing static route.

Click **APPLY** to save your changes.

### Edit This Static Route

Destination \*  
192.168.122.2

Netmask \*  
31 (255.255.255.254) ▾

Next Hop Type \* ⓘ


Next Hop IP \_\_\_\_\_ Next Hop Interface  
vlan1 ▾

Distance \*  
1  
1 - 255

Tracking ID


CANCEL
APPLY


UI Setting	Description	Valid Range	Default Value
<b>Destination</b>	Specify the destination IP address for the static route.	Valid IP address	N/A
<b>Netmask</b>	Specify the subnet mask for the destination IP address.	Drop-down list of subnet masks	N/A
<b>Next Hop IP</b>	Specify the next hop on the path to the destination IP.	Valid IP address	N/A
<b>Next Hop Interface</b>	Select a previously created VLAN interface or leave this field blank.	Drop-down list of interfaces	N/A
<b>Distance</b>	Specify the distance value to determine the priority of the static route. Lower values have higher priority.	1 to 255	N/A

UI Setting	Description	Valid Range	Default Value
<b>Tracking ID</b>	Select a tracking ID for the static route. When the status of the tracking ID is up, the route will be enabled. When the status of the tracking ID is down, the route will be disabled.	List of existing tracking IDs	N/A
<p> <b>Note</b></p> <p>You need to create a tracking ID before you can select it. Refer to <a href="#">Tracking</a> for more information.</p>			

## Delete Static Route

### Menu Path: [Routing](#) > [Unicast Route](#) > [Static Routing](#)

You can delete entries by using the checkboxes to select the entries you want to delete, then clicking the **Delete** () icon.

Static Routes						
	Status	Name	Destination Address	Netmask	Next Hop	Metric
<input checked="" type="checkbox"/>	Disabled	test	192.168.122.1	255.255.255.0	192.168.122.2	1
Max. 512						

## OSPF

### Menu Path: [Routing](#) > [Unicast Route](#) > [OSPF](#)

This section lets you manage OSPF for your device.

This section includes these pages:

- OSPF Settings
- OSPF Status

## OSPF

Open Shortest Path First (OSPF) is a dynamic routing protocol used in Internet Protocol (IP) networks. Specifically, it is a link-state routing protocol in the group of interior gateway protocols, operating within a single autonomous system.

As a link-state routing protocol, OSPF establishes and maintains neighbor relationships in order to exchange routing updates with other routers. The neighbor relationship table is called an adjacency database in OSPF. OSPF forms neighbor relationships only with routers directly connected to it. In order to form a neighbor relationship between two routers, the interfaces used to form the relationship must be in the same area. An interface can only belong to a single area.

With OSPF enabled, the Moxa Layer 3 switch is able to exchange routing information with other L3 switches or routers more efficiently in a large system.

### OSPF Settings

**Menu Path: [Routing](#) > [Unicast Route](#) > [OSPF](#) > [OSPF Settings](#)**

This page lets you configure OSPF for your device.

This page includes these tabs:

- General
- Area
- Interface
- Neighbor
- Aggregation
- Virtual Link

### OSPF Settings - General

**Menu Path: [Routing](#) > [Unicast Route](#) > [OSPF](#) > [OSPF Settings - General](#)**

This page lets you configure OSPF general settings.

## OSPF Settings - General

### OSPF Settings

General
Area
Interface
Neighbor
Aggregation
Virtual Link

OSPF \*  
Disabled ▼

Router ID \*  
0.0.0.0

Current Router ID  
0.0.0.0 ⓘ

RFC 1583 Compatibility \*  
Disabled ▼

SPF Hold Time \*  
5000  
0 - 65535 ms

APPLY

UI Setting	Description	Valid Range	Default Value
<b>OSPF</b>	Enable or disable OSPF for your device.	Enabled / Disabled	Disabled
<b>Router ID</b>	Specify the Router ID of your Moxa router.  <div style="background-color: #f0f0f0; padding: 5px; margin-top: 10px;"> <p><b>Note</b></p> <p>The router ID, which must be established for every OSPF instance, should be written in the dot-decimal format of an IP address (e.g., 1.2.3.4) and does not need to be part of any routable subnet on the network, since it is an IP address.</p> </div>	Router ID	0.0.0.0
<b>Current Router ID (View-only)</b>	Specify the current Router ID of your Moxa router.  <div style="background-color: #f0f0f0; padding: 5px; margin-top: 10px;"> <p><b>Note</b></p> <p>When the Router ID is set to 0.0.0.0, the Current Router ID will automatically use the highest interface IP address.</p> </div>	Current Router ID	0.0.0.0
<b>Compatible RFC 1583 (Available in Advanced Mode)</b>	Enable or disable compatibility with RFC 1583.	Enabled / Disabled	Disabled



UI Setting	Description	Valid Range	Default Value
<b>SPF Hold Time (ms)</b> <b>(Available in Advanced Mode)</b>	Specify the SPF hold time in milliseconds.	0 to 65535	5000

## OSPF Protocol List

Protocol	Redistribute	Type	Metric
Static	Disabled	E2	20
Connected	Disabled	E2	20

UI Setting	Description
<b>Protocol</b>	Shows the OSPF protocol the entry is for.
<b>Redistribute</b>	Shows whether redistribution is enabled for the protocol.
<b>Type</b>	Shows the metric type used for routes to be redistributed.
<b>Metric</b>	Shows the metric value used for routes to be redistributed.

## Editing Redistribute Settings

### Menu Path: [Routing](#) > [Unicast Route](#) > [OSPF](#) > [OSPF Settings - General](#)

Clicking the **Edit** (✎) icon for a protocol on the **Routing > Unicast Route > OSPF > OSPF Settings - General** page will open this dialog box. This dialog lets you edit the redistribute settings for the protocol.

Click **APPLY** to save your changes.

**Note**

The name of the dialog will change depending on whether you are editing settings for a static or connected protocol.

### Edit Redistribute Static

Redistribute \*  
Disabled

Type \*  
E2

Metric \*  
20  
1 - 16777214

CANCEL APPLY

### Edit Redistribute Connected

Redistribute \*  
Disabled

Type \*  
E2

Metric \*  
20  
1 - 16777214

CANCEL APPLY

UI Setting	Description	Valid Range	Default Value
<b>Redistribute</b>	Enable or disable redistribution for the protocol.	Enabled / Disabled	Enabled

UI Setting	Description	Valid Range	Default Value
<b>Type</b> (Only in Advanced Mode)	Select the metric type applied to the routes to be redistributed.	E1/ E2	E2
<b>Metric</b> (Only in Advanced Mode)	Specify the metric value for the routes to be redistributed into OSPF.	1 to 16777214	20

## OSPF Settings - Area

**Menu Path: Routing > Unicast Route > OSPF > OSPF Settings - Area**

This page lets you configure OSPF area settings.

### Limitations

You can create up to 64 OSPF areas.

Area ID	Area Type	Summary
0.0.0.0	Normal	No Summary

Max. 64      Items per page: 50      1 - 1 of 1

UI Setting	Description
<b>Area ID</b>	Shows the area ID for the area.
<b>Area Type</b>	Shows the type of the area.
<b>Summary</b>	Shows the summary of the area.

## Creating an OSPF Area

**Menu Path: Routing > Unicast Route > OSPF > OSPF Settings - Area**

Clicking the **Add (+)** icon on the **Routing > Unicast Route > OSPF > OSPF Settings - Area** page will open this dialog box. This dialog lets you add a new OSPF area.

Click **CREATE** to save your changes.



The 'Create Area' dialog box contains three input fields: 'Area ID' (text input), 'Area Type' (dropdown menu), and 'Summary' (dropdown menu with an information icon). At the bottom right, there are two buttons: 'CANCEL' and 'CREATE'.

UI Setting	Description	Valid Range	Default Value
<b>Area ID</b>	Specify the area ID for the new area.	0.0.0.0 to 255.255.255.255	0.0.0.0
<b>Area Type</b>	Select the area type to use.	Normal / Stub / NSSA	N/A
<b>Summary</b>	Select whether to include a summary for the area or not.	Summary / No Summary	N/A

## Editing an OSPF Area

**Menu Path: Routing > Unicast Route > OSPF > OSPF Settings - Area**

Clicking the **Edit (✎)** icon for an OSPF area on the **Routing > Unicast Route > OSPF > OSPF Settings - Area** page will open this dialog box. This dialog lets you edit the settings of the OSPF area.

Click **APPLY** to save your changes.

### Edit This Area

Area ID  
0.0.0.0  
.....

Area Type \*  
Normal ▼

Summary \*  
No Summary ▼ i

CANCEL
APPLY

UI Setting	Description	Valid Range	Default Value
<b>Area ID (View-only)</b>	Shows the area ID. This value cannot be changed.	N/A	N/A
<b>Area Type</b>	Select the area type to use.	Normal / Stub / NSSA	N/A
<b>Summary</b>	Select whether to include a summary for the area or not.	Summary / No Summary	N/A

## Deleting an Area

### Menu Path: [Routing](#) > [Unicast Route](#) > [OSPF](#) > [OSPF Settings - Area](#)

You can delete an area by using the checkboxes to select the ones you want to delete, then clicking the **Delete** (🗑️) icon.

## OSPF Settings - Interface

### Menu Path: [Routing](#) > [Unicast Route](#) > [OSPF](#) > [OSPF Settings - Interface](#)

This page lets you configure OSPF interface settings.

## OSPF Interface List

Interface Name	Interface Alias	IP Address	OSPF	Area ID	Hello Interval (sec.)	Dead Interval (sec.)	Priority	Cost	Network Type	Auth Type	Key ID	Passive Interface
vlan1		192.168.127.253	Disabled	0.0.0.0	10	40	1	1	Broadcast	--	--	Disabled

Items per page: 50 1 - 1 of 1 |< < > >|

UI Setting	Description
<b>Interface Name</b>	Shows the name of the interface this entry is for.
<b>Interface Alias</b>	Shows the alias for the interface.
<b>IP Address</b>	Shows the IP address for the interface.
<b>OSPF</b>	Shows whether OSPF is enabled for the interface.
<b>Area ID</b>	Shows the area ID for the interface.
<b>Hello Interval (sec.)</b>	Shows the hello packet send interval in seconds for the interface.
<b>Dead Interval (sec.)</b>	Shows the dead interval in seconds for the interface.
<b>Priority</b>	Shows the L3 priority for the interface.
<b>Cost</b>	Shows the cost for the interface. Lower values mean higher priority.
<b>Network Type (Only in Advanced Mode)</b>	Shows the network type assigned to the interface to determine how hello packets will be sent.
<b>Auth Type</b>	Shows the OSPF authentication type used for the interface.
<b>Key ID</b>	Shows the OSPF authentication key ID used for the interface.
<b>Passive Mode (Only in Advanced Mode)</b>	Shows whether passive mode is enabled for the interface.

## Editing an OSPF Interface

**Menu Path: Routing > Unicast Route > OSPF > OSPF Settings - Interface**

Clicking the **Edit** (✎) icon for an interface on the **Routing > Unicast Route > OSPF > OSPF Settings - Interface** page will open this dialog box. This dialog lets you edit the OSPF settings of the interface.

Click **APPLY** to save your changes.

**Edit Interface vlan1**

OSPF \*  
Disabled

Area ID \*  
0.0.0.0

Hello Interval \*  
10  
1 - 65535 sec.

Dead Interval \*  
40  
1 - 65535 sec.

Priority \*  
1  
0 - 255

Cost \*  
1  
1 - 65535

Network Type \*  
Broadcast

Auth Type \*  
SHA-512





Key \*  
SHA-512  
0 / 16

Key ID \*  
0 - 255

Passive Interface \*  
Disabled

CANCEL APPLY

UI Setting	Description	Valid Range	Default Value
<b>OSPF</b>	Enable or disable the OSPF function for the interface.	Enabled/ Disabled	Disabled
<b>Area ID</b>	Specify the area ID for the interface.	Drop-down list of the area ID	0.0.0.0

UI Setting	Description	Valid Range	Default Value
<b>Hello Interval</b>	<p>Specify the hello packet send interval in seconds. Hello packets are packets sent to OSPF neighbors to maintain connectivity with those neighbors.</p> <div style="background-color: #f0f0f0; padding: 5px; margin-top: 10px;"> <p> <b>Note</b></p> <p>The value of all hello intervals must be the same within a network.</p> </div>	1 to 65535	10
<b>Dead Interval</b>	<p>Specify the dead interval in seconds. This is the amount of time that must pass with no hello packet responses received from the neighbor before the neighbor is declared dead.</p> <div style="background-color: #f0f0f0; padding: 5px; margin-top: 10px;"> <p> <b>Note</b></p> <p>The dead interval is often set as four times the hello interval.</p> </div>	1 to 65535	40
<b>Priority</b>	<p>Specify the L3 priority for the interface. Higher values mean higher priority to be selected as the designated router.</p>	0 to 255	1
<b>Cost</b>	<p>Specify cost for the interface. Lower values mean higher priority.</p>	1 to 65535	1
<b>Network Type</b> (Only in Advanced Mode)	<p>Select the network type for the interface to determine how hello packets will be sent.</p> <div style="background-color: #f0f0f0; padding: 5px; margin-top: 10px;"> <p> <b>Note</b></p> <p>When the network type is set to <b>Non-broadcast</b> or <b>Point-to-multipoint</b>, you will need to add a neighbor manually.</p> </div>	Broadcast / Non-broadcast / Point-to-multipoint / Point-to-point	Broadcast
<b>Auth Type</b>	<p>Specify the OSPF authentication type to use when authenticating OSPF neighbors, or select <b>None</b> for no authentication.</p> <div style="background-color: #f0f0f0; padding: 5px; margin-top: 10px;"> <p> <b>Note</b></p> <p>If OSPF authentication is used, all L3 switches and routers on the same segment must use the same authentication method and key.</p> </div>	None / Simple / MD5 / SHA1 / SHA-224 / SHA-256 / SHA-385 / SHA-512	N/A



UI Setting	Description	Valid Range	Default Value
<b>Key</b> <b>(If Auth Type is not None)</b>	Specify the key for OSPF authentication.	If Auth Type is None: N/A  If Auth Type is Simple: 1 to 8 characters  All other Auth Types: 1 to 16 characters	N/A
<b>Key ID</b> <b>(If Auth Type is not None or Simple)</b>	Specify the key ID for OSPF authentication.	1 to 255 characters	N/A
<b>Passive Interface</b> <b>(Only in Advanced Mode)</b>	Enable or disable passive mode for the interface. In passive mode, OSPF-related operations will not execute, but interface's route information can still be learned by other non-passive interfaces.	Enabled / Disabled	Disabled

## OSPF Settings - Neighbor

**Menu Path:** [Routing](#) > [Unicast Route](#) > [OSPF](#) > [OSPF Settings - Neighbor](#)

This page lets you configure OSPF neighbor settings.

### Note

This page is only available in Advanced Mode.

### 🔔 Limitations

You can create up to 64 OSPF neighbors.

## OSPF Neighbor List

The screenshot shows a table interface for OSPF neighbors. At the top left, there are icons for adding (+) and deleting (trash) neighbors. A search bar is located at the top right. The table has two columns: 'Neighbor IP Address' and 'Priority'. Below the table, there is a pagination control showing 'Max. 64' items, 'Items per page: 50', and '0 of 0' items. Navigation arrows are also present.

UI Setting	Description
<b>Neighbor IP Address</b>	Shows the IP address of the neighbor device.
<b>Priority</b>	Shows the L3 priority of the neighbor. Higher values mean higher priority for becoming the designated router. A value of 0 means this neighbor will not become a designated router.

## Creating an OSPF Neighbor

**Menu Path:** [Routing](#) > [Unicast Route](#) > [OSPF](#) > [OSPF Settings - Neighbor](#)

Clicking the **Add (+)** icon on the **Routing > Unicast Route > OSPF > OSPF Settings - Neighbor** page will open this dialog box. This dialog lets you add an OSPF neighbor.

Click **CREATE** to save your changes.

The 'Create a Neighbor' dialog box contains two input fields: 'Neighbor IP Address \*' and 'Priority \*'. The 'Priority' field has a range of '0 - 255' indicated below it. At the bottom right, there are two buttons: 'CANCEL' and 'APPLY'.

UI Setting	Description	Valid Range	Default Value
<b>Neighbor IP Address</b>	Specify the IP address for the neighbor.	Valid IP address	N/A
<b>Priority</b>	Specify the priority for the neighbor. Higher values mean higher priority for becoming the designated router. A value of 0 means this neighbor will not become a designated router.	0 to 255	N/A

## Editing an OSPF Neighbor

**Menu Path:** Routing > Unicast Route > OSPF > OSPF Settings - Neighbor

Clicking the **Edit** (✎) icon for an OSPF neighbor on the **Routing > Unicast Route > OSPF > OSPF Settings - Neighbor** page will open this dialog box. This dialog lets you edit the OSPF neighbor.

Click **APPLY** to save your changes.

### Edit This Neighbor

Neighbor IP Address  
192.168.24.221

---

Priority \*  
3

---

0 - 255

CANCEL
APPLY

UI Setting	Description	Valid Range	Default Value
<b>Neighbor IP Address (View only)</b>	Shows the IP address for the neighbor. This value cannot be changed	N/A	Neighbor IP address

UI Setting	Description	Valid Range	Default Value
<b>Priority</b>	Specify the L3 priority for the neighbor. Higher values mean higher priority for becoming the designated router. A value of 0 means this neighbor will not become a designated router.	0 to 255	N/A

## Deleting an OSPF Neighbor

**Menu Path:** [Routing](#) > [Unicast Route](#) > [OSPF](#) > [OSPF Settings - Neighbor](#)

You can delete an OSPF neighbor by using the checkboxes to select the ones you want to delete, then clicking the **Delete** (🗑️) icon.

## OSPF Settings - Aggregation

**Menu Path:** [Routing](#) > [Unicast Route](#) > [OSPF](#) > [OSPF Settings - Aggregation](#)

This page lets you configure OSPF aggregation settings.

### 🔔 Limitations

You can create up to 192 OSPF aggregations.

## OSPF Aggregation List

<input type="checkbox"/>	Area ID	IP Address	Subnet Mask	LSA Type
Max. 192      Items per page: 50      0 of 0      << < > >>				

UI Setting	Description
<b>Area ID</b>	Shows the area ID of the aggregation.
<b>IP Address</b>	Shows the IP address of the aggregation.

UI Setting	Description
<b>Subnet Mask</b>	Shows the subnet mask of the aggregation.
<b>LSA Type</b>	Shows the LSA type used for the aggregation.

## Creating an OSPF Aggregation

### Menu Path: Routing > Unicast Route > OSPF > OSPF Settings - Aggregation

Clicking the **Add (+)** icon on the **Routing > Unicast Route > OSPF > OSPF Settings - Aggregation** page will open this dialog box. This dialog lets you create an OSPF aggregation.

Click **CREATE** to save your changes.

### Create an Aggregation


CANCEL
CREATE

UI Setting	Description	Valid Range	Default Value
<b>Area ID</b>	Select the Area ID that you want to use for the aggregation.	Drop-down list of area IDs	0.0.0.0
<b>IP Address</b>	Specify the IP address for the aggregation.	Valid IP address	N/A
<b>Subnet Mask</b>	Specify the subnet mask for the aggregation.	Drop-down list of subnet masks	N/A

UI Setting	Description	Valid Range	Default Value
<b>LSA Type</b>	Specify the type of LSA to use for the aggregation.	Summary / Type 7	N/A

## Deleting an OSPF Aggregation

**Menu Path:** [Routing](#) > [Unicast Route](#) > [OSPF](#) > [OSPF Settings - Aggregation](#)

You can delete an OSPF aggregation by using the checkboxes to select the ones you want to delete, then clicking the **Delete** (  ) icon.

## OSPF Settings - Virtual Link

**Menu Path:** [Routing](#) > [Unicast Route](#) > [OSPF](#) > [OSPF Settings - Virtual Link](#)

This page lets you configure OSPF virtual link settings.

### Limitations

You can create up to 128 OSPF virtual links.

## OSPF Virtual Link List

<input type="checkbox"/>	Area ID	Router ID	Hello Interval (sec.)	Dead Interval (sec.)	Auth Type	Key ID
Max. 128						
Items per page: 50						0 of 0

UI Setting	Description
<b>Area ID</b>	Shows the area ID for the virtual link.
<b>Router ID</b>	Shows the router ID for the virtual link.
<b>Hello Interval (sec.)</b>	Shows the hello packet send interval in seconds for the virtual link.

UI Setting	Description
<b>Dead Interval (sec.)</b>	Shows the dead interval in seconds for the virtual link.
<b>Auth Type</b>	Shows the OSPF authentication type used for the virtual link.
<b>Key ID</b>	Shows the OSPF authentication key ID used for the virtual link.

## Creating an OSPF Virtual Link

### Menu Path: Routing > Unicast Route > OSPF > OSPF Settings - Virtual Link

Clicking the **Add (+)** icon on the **Routing > Unicast Route > OSPF > OSPF Settings - Virtual Link** page will open this dialog box. This dialog lets you create an OSPF virtual link.

Click **CREATE** to save your changes.

### Create a Virtual Link




Area ID \*

Router ID \*

Hello Interval \*  sec. Dead Interval \*  sec.


Auth Type \*  Key \*   Key ID \*

UI Setting	Description	Valid Range	Default Value
<b>Area ID</b>	Select the area ID to use for the virtual link.	Drop-down list of area IDs	N/A
<b>Router ID</b>	Specify the L3 switch or router's ID.	Valid router ID	N/A

UI Setting	Description	Valid Range	Default Value
<b>Hello Interval</b>	Specify the hello packet send interval in seconds. Hello packets are packets sent to OSPF neighbors to maintain connectivity with those neighbors.  <div style="border: 1px solid #ccc; background-color: #f9f9f9; padding: 5px; margin-top: 10px;"> <p> <b>Note</b></p> <p>The value of all hello intervals must be the same within a network.</p> </div>	1 to 65535	N/A
<b>Dead Interval</b>	Specify the dead interval in seconds.  <div style="border: 1px solid #ccc; background-color: #f9f9f9; padding: 5px; margin-top: 10px;"> <p> <b>Note</b></p> <p>The dead interval is often set as four times the hello interval.</p> </div>	1 to 65535	N/A
<b>Auth Type</b>	Specify the OSPF authentication type to use when authenticating OSPF neighbors, or select <b>None</b> for no authentication.  <div style="border: 1px solid #ccc; background-color: #f9f9f9; padding: 5px; margin-top: 10px;"> <p> <b>Note</b></p> <p>If OSPF authentication is used, all L3 switches and routers on the same segment must use the same authentication method and key.</p> </div>	None / Simple / MD5 / SHA1 / SHA-224 / SHA-256 / SHA-385 / SHA-512	N/A
<b>Key</b> <b>(If Auth Type is not None)</b>	Specify the key for OSPF authentication.	If Auth Type is None: N/A  If Auth Type is Simple: 1 to 8 characters  All other Auth Types: 1 to 16 characters	N/A
<b>Key ID</b> <b>(If Auth Type is not None or Simple)</b>	Specify the key ID for OSPF authentication.	1 to 255 characters	N/A

## Deleting an OSPF Virtual Link

### Menu Path: [Routing](#) > [Unicast Route](#) > [OSPF](#) > [OSPF Settings - Virtual Link](#)

You can delete an OSPF virtual link by using the checkboxes to select the ones you want to delete, then clicking the **Delete** (  ) icon.



## OSPF Status

**Menu Path: Routing > Unicast Route > OSPF > OSPF Status**

This page lets you monitor OSPF status information.

This page includes these tabs:

- Interface
- Neighbor
- Database
- Virtual Link

### OSPF Status - Interface

**Menu Path: Routing > Unicast Route > OSPF > OSPF Status - Interface**

This page lets you view the status of your device's OSPF interfaces.

#### OSPF Status Interface List

Interface Name	Interface Alias	IP Address	Area	State	DR Router ID	BDR Router ID
vlan1		192.168.127.253	0.0.0.0	Down	N/A	N/A

Items per page: 50 1 - 1 of 1 |< < > >|

UI Setting	Description
<b>Interface Name</b>	Shows the name of the interface this entry is for.
<b>Interface Alias</b>	Shows the alias for the interface.
<b>IP Address</b>	Shows the IP address for the interface.
<b>Area</b>	Shows the area ID for the interface.
<b>State</b>	Shows whether the interface is currently up or down.

UI Setting	Description
<b>DR Router ID</b>	Shows the ID of the designated router (DR).
<b>BDR Router ID</b>	Shows the ID of the backup designated router (BDR).

## OSPF Status - Neighbor

**Menu Path:** [Routing](#) > [Unicast Route](#) > [OSPF](#) > [OSPF Status - Neighbor](#)

This page lets you view the status of your device's OSPF neighbors.

### OSPF Status Neighbor List

Neighbor ID	Priority	State	IP Address	Interface Name	Dead Interval (sec.)
-------------	----------	-------	------------	----------------	----------------------

UI Setting	Description
<b>Neighbor ID</b>	Shows the ID of the neighbor device.
<b>Priority</b>	Shows the L3 priority of the neighbor.
<b>State</b>	Shows the state of the neighbor.
<b>IP Address</b>	Shows the IP address of the neighbor device.
<b>Interface Name</b>	Shows which interface the neighbor is connected to.
<b>Dead Interval (sec.)</b>	Shows the dead interval in seconds for the neighbor.

## OSPF Status - Database

**Menu Path:** [Routing](#) > [Unicast Route](#) > [OSPF](#) > [OSPF Status - Database](#)

This page lets you view the status of your device's OSPF database.

## OSPF Status Database List

UI Setting	Description
<b>LSA Type</b>	Shows the type of the link state advertisement (LSA).
<b>Area</b>	Shows the area ID of the LSA.
<b>Link ID</b>	Shows the link ID of the LSA.
<b>ADV Router</b>	Shows the router where the LSA originated from.
<b>Age (sec.)</b>	Shows the age of the LSA in seconds.

## OSPF Status - Virtual Link

**Menu Path:** [Routing](#) > [Unicast Route](#) > [OSPF](#) > [OSPF Status - Virtual Link](#)

This page lets you view the status of your device's OSPF virtual links.

## OSPF Status Virtual Link List

UI Setting	Description
<b>Area</b>	Shows the area ID for the virtual link.

UI Setting	Description
<b>Router ID</b>	Shows the router ID for the virtual link.
<b>Neighbor State</b>	Shows the current state of the neighbor.
<b>Events</b>	Shows the number of events that have occurred since the device was booted. Events include the state of the virtual link changing and errors.
<b>LSA Retransmission Queue Length</b>	Shows the current length of the LSA retransmission queue.
<b>Hello Suppressed</b>	Shows whether hello messages to the neighbor are being suppressed.

## Routing Table

### Menu Path: Routing > Unicast Route > Routing Table

This page lets you see the current routing table for your device.

Type	Destination	Netmask	Next Hop	AD/Metric
Static	192.168.122.2	255.255.255.254	vlan1	1/1
Connected	192.168.127.0	255.255.255.0	vlan1	0/0
Connected	255.223.12.11	255.255.255.255	loopback1	0/0

Max. 3000      Items per page: 50      1 - 3 of 3

UI Setting	Description
<b>Type</b>	Shows the source type of the route.
<b>Destination</b>	Shows the address of the destination network for the route.
<b>Netmask</b>	Shows the netmask of the destination network for the route.
<b>Next Hop</b>	Shows the IP address or interface of the next hop that the packet should be forwarded to.

UI Setting	Description
<b>AD/Metric</b>	Shows the metric value/cost of the route to the destination network.

**Note**

Metrics are used to calculate the shortest path for data to travel through the network, and are determined by assigning cost values to the interfaces connecting to each router. The lower the cost value, the more the path will be preferred.

## Multicast Route

### Menu Path: [Routing](#) > [Multicast Route](#)

This section lets you configure and monitor the information about multicast routing protocols.

This section includes these pages:

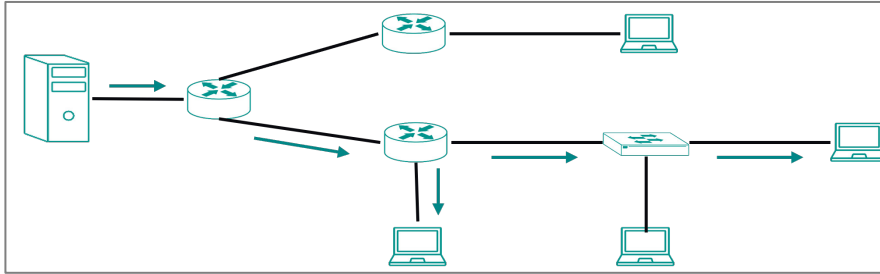
- PIM-DM
- PIM-SM
- Multicast Local Route
- Multicast Routing Table

### PIM-DM

PIM-DM (Protocol Independent Multicast - Dense Mode) is a multicast routing protocol that can efficiently deliver multicast traffic to many receivers within a single network domain. It is designed for environments where multicast receivers are densely distributed throughout the network.

In PIM-DM, multicast traffic is flooded to all nodes within the network domain by default, which is known as dense mode. It uses a flood and prune mechanism to manage multicast traffic and relies on periodic reflooding to handle changes in the network. When a multicast packet is received by a node, it forwards the packet to all its connected interfaces, except the interface it received the packet from.

PIM-DM is simpler but less efficient than PIM-SM in networks with sparse multicast receivers.



## PIM-DM In Depth

PIM-DM works through these three mechanisms to prevent excessive traffic.

- **Flood and Prune:** Initially, PIM-DM floods multicast traffic to all Layer 3 switches in the network. Layer 3 switches that do not have any interested receivers for the multicast traffic send prune messages to their upstream neighbors, stopping the unwanted traffic.
- **Periodic Flooding:** To account for changes in group membership, PIM-DM periodically refloods the multicast traffic to ensure new receivers can join the multicast group.
- **Reverse Path Forwarding (RPF):** PIM-DM uses RPF checks to prevent loops. A multicast packet is only accepted if it arrives on the interface that is the best route back to the source of the packet.

## PIM-DM

**Menu Path:** [Routing](#) > [Multicast Route](#) > [PIM-DM](#)

This page lets you manage PIM-DM for your device.

This page includes these tabs:

- Settings
- Neighbor

### PIM-DM - Settings

**Menu Path:** [Routing](#) > [Multicast Route](#) > [PIM-DM - Settings](#)

This page lets you configure PIM-DM for your device.

## PIM-DM Settings

PIM-DM\* i

Disabled ▼

---

State Refresh\* i

Enabled ▼

State Refresh Interval\* i

60 sec.

10 - 100

APPLY

UI Setting	Description	Valid Range	Default Value
<b>PIM-DM</b>	Enable or disable use of PIM-DM protocol. <div style="background-color: #f0f0f0; padding: 10px; margin-top: 10px;"> <p><b>Note</b></p> <p>Only one multicast routing protocol can be active. If you want to enable <b>PIM-DM</b>, make sure you disable <b>PIM-SM</b> and <b>Multicast Local Route</b>.</p> </div>	Enabled / Disabled	Disabled
<b>State Refresh</b>	Enable or disable state refresh.	Enabled / Disabled	Enabled
<b>State Refresh Interval</b>	Specify the interval in seconds for the state to refresh.	10 - 100	60

## PIM-DM Interface List

Q Search

Interface Name	Interface Alias	IP Address	PIM-DM	Hello Interval (sec.)
vlan1	---	192.168.127.253	Disabled	30

Max. 256 1 - 1 of 1

UI Setting	Description
<b>Interface Name</b>	Shows the name of the interface.
<b>Interface Alias</b>	Shows the alias of the interface.

UI Setting	Description
<b>IP Address</b>	Shows the IP address of the interface.
<b>PIM-DM</b>	Shows whether PIM-DM is enabled on the interface.
<b>Hello Interval (sec.)</b>	Shows the interval in seconds to send Hello messages for the interface.

## Editing a PIM-DM Interface

### Menu Path: Routing > Multicast Route > PIM-DM - Settings

Clicking the **Edit** (✎) icon for an interface on the **Routing > Multicast Route > PIM-DM - Settings** page will open this dialog box. This dialog lets you edit the PIM-DM settings for the interface.

Click **APPLY** to save your changes.

**Edit Interface vlan1**

PIM-DM\*  
 Disabled ▼

---

Hello Interval\*  
 30

10 - 3600 sec.

CANCEL APPLY

UI Setting	Description	Valid Range	Default Value
<b>PIM-DM</b>	Enable or disable PIM-DM for the interface.	Enabled / Disabled	Disabled
<b>Hello Interval</b>	Specify the interval in seconds to send Hello messages.	10 - 3600	30

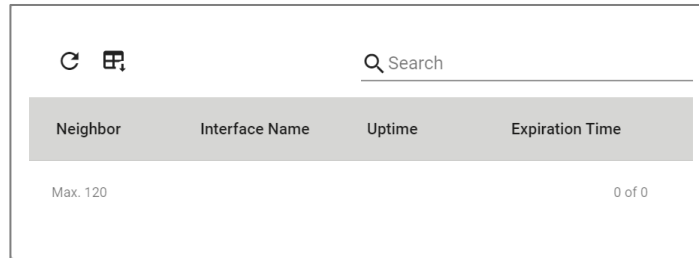
## PIM-DM - Neighbor

### Menu Path: Routing > Multicast Route > PIM-DM - Neighbor

This page lets you view the status of PIM-DM neighbors.



## PIM-DM Neighbor List



Neighbor	Interface Name	Uptime	Expiration Time
Max. 120			
0 of 0			

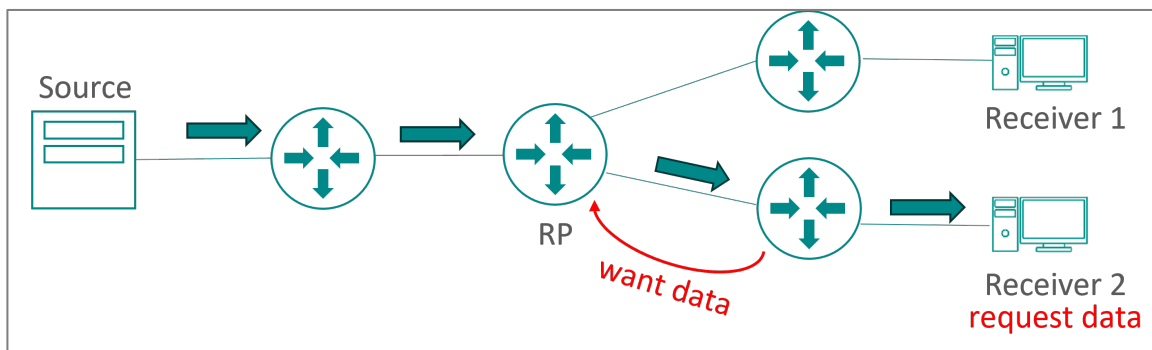
UI Setting	Description
<b>Neighbor</b>	Shows the PIM-DM neighbor this entry is for.
<b>Interface Name</b>	Shows which interface the neighbor is connected to.
<b>Uptime</b>	Shows how long this multicast route entry has been maintained by this switch.
<b>Expiration Time</b>	Shows the time remaining before this multicast route is removed from the PIM-DM neighbor list if it is not refreshed.

## About PIM-SM

PIM-SM (Protocol Independent Multicast – Sparse Mode) is a multicast routing protocol designed for environments where multicast receivers are sparsely distributed throughout the network. It assumes that only a very low percentage of receivers subscribe to a particular multicast group.

PIM-SM uses a key component called the Rendezvous Point (RP) as the root of the multicast distribution tree. When multicast traffic starts flowing in a group, PIM-SM initially builds a multicast distribution tree rooted at the RP. However, this tree may not always provide the shortest path between the source and the receivers. It is configured to manage the initial distribution of multicast traffic. If a shorter path to the source is discovered, PIM-SM can perform an SPT switchover to switch to the new shortest path.

Since PIM-SM only forwards multicast data to someone who requests it and always tries to route traffic the data through the shortest path, it is more scalable and efficient than PIM-DM.



## PIM-SM In Depth

### Identifying the RP and Building Paths

#### Rendezvous Point (RP)

The RP plays a crucial role in PIM-SM. It is responsible for receiving multicast traffic from sources and forwarding it down the multicast distribution tree to all receivers that have joined the multicast group. The RP can be statically configured in the network or discovered dynamically using a Bootstrap Router (BSR) mechanism.

#### Joining a Multicast Group (Join Messages)

When a host wants to receive multicast traffic for a specific group, its local router sends a PIM Join message towards the RP. This message is propagated hop-by-hop through the network until it reaches the RP, building a shared tree along the path.

#### Switching to the Shortest Path

Initially, multicast data is distributed along the shared tree, which is rooted at the RP and branches out to all receivers. For efficiency, once the first few packets have been received, the routers closer to the receivers may decide to switch from the shared tree to a source-specific shortest path tree (SPT).

The designated Layer 3 switch sends PIM Join messages directly towards the source of the multicast traffic, establishing the shortest path to the source. As the routers establish the SPT, Layer 3 switches in the longer path send PIM Prune messages to remove

themselves from the shared tree, ensuring that multicast traffic follows the most efficient path from the source to the receivers.

## **Maintaining the Tree**

Switches periodically send Join messages to maintain their place in the tree and send Prune messages to leave the tree if they no longer need the multicast traffic, and to resolve which switch will forward multicast traffic on a given network segment, preventing duplicate packets by Assert messages.

When a host no longer wants to receive multicast traffic, the switch sends a PIM Prune message towards the RP or the source. If the source stops sending multicast traffic, the RP eventually times out the shared tree branches, and switches using the SPT will also time out their branches.

## **PIM-SM**

**Menu Path: [Routing](#) > [Multicast Route](#) > [PIM-SM](#)**

This section lets you manage PIM-SM for your device.

This section includes these pages:

- [PIM-SM Settings](#)
- [PIM-SM Status](#)

## **PIM-SM Settings**

**Menu Path: [Routing](#) > [Multicast Route](#) > [PIM-SM](#) > [PIM-SM Settings](#)**

This page lets you configure PIM-SM for your device.

This page includes these tabs:

- [General](#)
- [RP](#)
- [SSM](#)

## PIM-SM Settings - General

**Menu Path: Routing > Multicast Route > PIM-SM > PIM-SM Settings - General**

This page lets you configure PIM-SM general settings.

## PIM-SM Settings - General

PIM-SM 🔔

Disabled ⓘ

---

Shortest-path Tree Switchover Method \*

Never ▼

**APPLY**

UI Setting	Description	Valid Range	Default Value
<b>PIM-SM</b>	Enable or disable use of PIM-SM protocol. <div style="background-color: #f0f0f0; padding: 5px; margin-top: 10px;"> <p><b>Note</b></p> <p>Only one multicast routing protocol can be active. If you want to enable <b>PIM-SM</b>, make sure you disable <b>PIM-DM</b> and <b>Multicast Local Route</b>.</p> </div>	Enabled / Disabled	Disabled
<b>Shortest-path Tree Switchover Method</b>	Select whether the device should switch over to the shortest-path tree if one is found.	Never / Immediate	Never

## PIM-SM Interface List

🔍 Search

Interface Name	Interface Alias	IP Address	PIM-SM	Hello Interval (sec.)	Join/Prune Interval (sec.)	DR Priority	BSR Candidate	BSR Priority	BSR Hash Mask Length
vlan1	---	192.168.127.253	Disabled	30	60	1	Disabled	64	30

Max. 256 1 - 1 of 1

UI Setting	Description
<b>Interface Name</b>	Shows the name of the interface.

UI Setting	Description
<b>Interface Alias</b>	Shows the alias of the interface.
<b>IP Address</b>	Shows the IP address of the interface.
<b>PIM-SM</b>	Shows whether PIM-SM is enabled on the interface.
<b>Hello Interval (sec.)</b>	Shows the interval in seconds to send Hello messages for the interface.
<b>Join/Prune Interval (sec.)</b>	Shows the interval in seconds to send Join/Prune messages.
<b>DR Priority</b>	Shows the DR (Designated Router) priority for the interface. Higher values have higher preference for the DR election process.
<b>BSR Candidate</b>	Shows whether the interface can be a BSR (Bootstrap Router) Candidate.
<b>BSR Priority</b>	Shows the BSR priority for the interface. Higher values have higher preference for the BSR election process.
<b>BSR Hash Mask Length</b>	Shows the mask length in bits to use for the BSR hash.

## Editing a PIM-SM Interface

### Menu Path: Routing > Multicast Route > PIM-SM > PIM-SM Settings - General

Clicking the **Edit** (✎) icon for an interface on the **Routing > Multicast Route > PIM-SM > PIM-SM Settings - General** page will open this dialog box. This dialog lets you edit the PIM-SM settings for the interface.

Click **APPLY** to save your changes.

### ui-dialog PIM-SM - Edit Interface

### Edit Interface vlan1

PIM-SM \*

Hello Interval \*       Join/Prune Interval \*   
10 - 3600 sec.      10 - 3600 sec.

DR Priority \*  i  
1 - 4294967295

BSR Candidate \*

BSR Priority \*  i  
0 - 255

BSR Hash Mask Length \*   
4 - 32

UI Setting	Description	Valid Range	Default Value
<b>PIM-SM</b>	Enable or disable PIM-SM for the interface.	Enabled / Disabled	Disabled
<b>Hello Interval</b>	Specify the interval in seconds to send Hello messages.	10 - 3600	30
<b>Join/Prune Interval</b>	Specify the interval in seconds to send Join/Prune messages.	10 - 3600	60
<b>DR Priority</b>	Specify the DR (Designated Router) priority for the interface. Higher values have higher preference for the DR election process.	1	4294967295
<b>BSR Candidate</b>	Enable or disable whether the interface can be a BSR (Bootstrap Router) Candidate.	Enabled / Disabled	Disabled
<b>BSR Priority</b>	Specify the BSR priority for the interface. Higher values have higher preference for the BSR election process.	0 - 255	64
<b>BSR Hash Mask Length</b>	Specify the mask length in bits to use for the BSR hash.	4 - 32	30

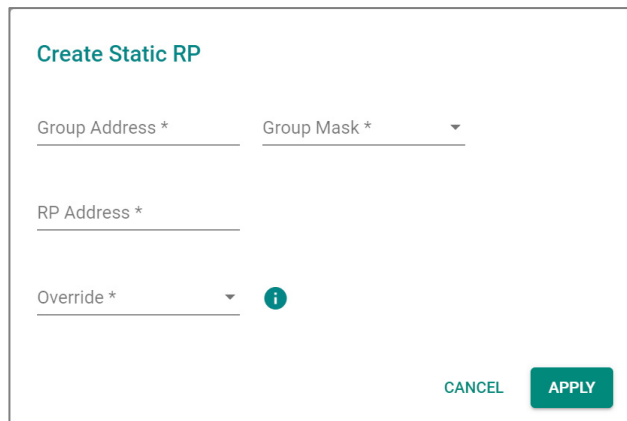


### Menu Path: Routing > Multicast Route > PIM-SM > PIM-SM Settings - RP

Clicking the **Add (+)** icon for the Static RP List of the **Routing > Multicast Route > PIM-SM > PIM-SM Settings - RP** page will open this dialog box. This dialog lets you create a new static RP.

Click **CREATE** to save your changes and add the static RP.

#### ui-dialog Create Static RP



UI Setting	Description	Valid Range	Default Value
<b>Group Address</b>	Specify the PIM multicast group address.	224.0.0.0 - 239.255.255.255	N/A
<b>Group Mask</b>	Specify the subnet mask of the group.	Drop-down list of subnet masks	N/A
<b>RP Address</b>	Specify the IP address of the static RP for this multicast group.	Valid IP address	N/A
<b>Override</b>	Enable or disable the override function for the multicast group. When enabled, the static RP will be used before a dynamically learned BSR candidate if there is a conflict.	Enabled / Disabled	N/A

#### Editing a Static RP

### Menu Path: Routing > Multicast Route > PIM-SM > PIM-SM Settings - RP

Clicking the **Edit (✎)** icon for a static RP on the **Routing > Multicast Route > PIM-SM > PIM-SM Settings - RP** page will open this dialog box. This dialog lets you edit the settings of the static RP.

Click **APPLY** to save your changes.



## ui-dialog Edit Static RP

**Edit Static RP**

Group Address \* 230.1.5.0

Group Mask \* 24 (255.255.255.0) ▼

RP Address \* 192.168.126.24

Override \* Enabled ▼ ⓘ

CANCEL APPLY

UI Setting	Description	Valid Range	Default Value
<b>Group Address</b>	Specify the PIM multicast group address.	224.0.0.0 - 239.255.255.255	N/A
<b>Group Mask</b>	Specify the subnet mask of the group.	Drop-down list of subnet masks	N/A
<b>RP Address</b>	Specify the IP address of the static RP for this multicast group.	Valid IP address	N/A
<b>Override</b>	Enable or disable the override function for the multicast group. When enabled, the static RP will be used before a dynamically learned BSR candidate if there is a conflict.	Enabled / Disabled	N/A

## Deleting a Static RP

### Menu Path: Routing > Multicast Route > PIM-SM > PIM-SM Settings - RP

You can delete a static RP by using the checkboxes to select the entries you want to delete, then clicking the **Delete** (🗑️) icon.



### Create Candidate RP

Group Address \*
Group Mask \* ▾

RP Interface Name (RP Address) \* ▾

RP Priority \* i  
0 - 255

CANCEL
APPLY

UI Setting	Description	Valid Range	Default Value
<b>Group Address</b>	Specify the PIM multicast group address.	224.0.0.0 - 239.255.255.25	N/A
<b>Group Mask</b>	Specify the subnet mask of the group.	Drop-down list of subnet masks	N/A
<b>RP Interface Name (RP Address)</b>	Specify the interface of the candidate RP for this group.	Drop-down list of interfaces	N/A
<b>RP Priority</b>	Specify the RP priority. Lower values have higher preference for the RP election process.	0 - 255	N/A
<p><b>Note</b></p> <p>If the RP Priority is not set, the default value of 192 will be used.</p>			

## Editing a Candidate RP

**Menu Path:** Routing > Multicast Route > PIM-SM > PIM-SM Settings - RP

Clicking the **Edit (✎)** icon for a candidate RP on the **Routing > Multicast Route > PIM-SM > PIM-SM Settings - RP** page will open this dialog box. This dialog lets you edit the settings of the candidate RP.

Click **APPLY** to save your changes.

### ui-dialog Edit Candidate RP

### Edit Candidate RP

Group Address \*  
230.1.5.0

Group Mask \*  
24 (255.255.255.0) ▼

RP Interface Name (RP Address) \*  
vlan1(192.168.127.253) ▼

RP Priority \*  
123 i


0 - 255

CANCEL
APPLY

UI Setting	Description	Valid Range	Default Value
<b>Group Address</b>	Specify the PIM multicast group address.	224.0.0.0 - 239.255.255.25	N/A
<b>Group Mask</b>	Specify the subnet mask of the group.	Drop-down list of subnet masks	N/A
<b>RP Interface Name (RP Address)</b>	Specify the interface of the candidate RP for this group.	Drop-down list of interfaces	N/A
<b>RP Priority</b>	Specify the RP priority. Lower values have higher preference for the RP election process.	0 - 255	N/A
<p><b>Note</b></p> <p>If the RP Priority is not set, the default value of 192 will be used.</p>			

## Deleting a Candidate RP

**Menu Path:** [Routing](#) > [Multicast Route](#) > [PIM-SM](#) > [PIM-SM Settings - RP](#)

You can delete a candidate RP by using the checkboxes to select the entries you want to delete, then clicking the **Delete** (  ) icon.

## PIM-SM Settings - SSM

**Menu Path:** [Routing](#) > [Multicast Route](#) > [PIM-SM](#) > [PIM-SM Settings - SSM](#)

This page lets you configure PIM Source-specific Multicast (SSM) related settings.

**Note**

PIM-SSM (Source-Specific Multicast) lets you specify the source for the group address. To ensure smooth operation, make sure switches have IGMP Snooping v3 enabled and that the host supports IGMP v3.

**Limitations**

You can create up to 8 SSM sources.

### PIM-SSM Settings

PIM-SSM \*  
Disabled

APPLY

UI Setting	Description	Valid Range	Default Value
<b>PIM-SMM</b>	Enable or disable Source-specific Multicast (SSM).  <b>Note</b> When enabling SSM, the source range for 232.0.0.0/8 will be enabled automatically.	Enabled / Disabled	Disabled

### PIM-SSM Range List

**+**

<input type="checkbox"/>	Group Address	Group Mask
<input type="checkbox"/>	<input type="text" value="232.0.0.0"/>	<input type="text" value="255.0.0.0"/>

Max. 8

UI Setting	Description
<b>Group Address</b>	Shows the group address for the PIM-SSM range.
<b>Group Mask</b>	Shows the subnet mask of the group address for the PIM-SSM range.

## Adding a PIM-SSM Range

**Menu Path:** [Routing](#) > [Multicast Route](#) > [PIM-SM](#) > [PIM-SM Settings - SSM](#)

Clicking the **Add (+)** icon on the **Routing > Multicast Route > PIM-SM > PIM-SM Settings - SSM** page will open this dialog box. This dialog lets you add a new PIM-SSM range.

Click **CREATE** to save your changes and add the new range.

### ui-dialog Add SSM Range

UI Setting	Description	Valid Range	Default Value
<b>Group Address</b>	Specify the group address for the PIM-SSM range.	Valid multicast IP address	N/A
<b>Group Mask</b>	Specify the subnet mask of the group address for the PIM-SSM range.	Drop-down list of subnet masks	N/A

## Editing a PIM-SSM Range

**Menu Path:** [Routing](#) > [Multicast Route](#) > [PIM-SM](#) > [PIM-SM Settings - SSM](#)

Clicking the **Edit (✎)** icon for a PIM-SSM range on the **Routing > Multicast Route > PIM-SM > PIM-SM Settings - SSM** page will open this dialog box. This dialog lets you edit the range.

Click **APPLY** to save your changes.

**Note**

Group address 232.0.0.0/8 is the address range reserved for SSM usage as defined in RFC 4607, so it can not be edited.

### ui-dialog Edit PIM-SSM Range

**Edit SSM Range**

Group Address \* 224.0.0.0      Group Mask \* 8 (255.0.0.0) ▼

CANCEL      APPLY

UI Setting	Description	Valid Range	Default Value
<b>Group Address</b>	Specify the group address for the PIM-SSM range.	Valid multicast IP address	N/A
<b>Group Mask</b>	Specify the subnet mask of the group address for the PIM-SSM range.	Drop-down list of subnet masks	N/A

### Deleting a PIM-SSM Range

**Menu Path:** [Routing](#) > [Multicast Route](#) > [PIM-SM](#) > [PIM-SM Settings - SSM](#)

You can delete a PIM-SSM range by using the checkboxes to select the entries you want to delete, then clicking the **Delete (🗑)** icon.

**Note**

Group address 232.0.0.0/8 is the address range reserved for SSM usage as defined in RFC 4607, so it can not be deleted.

### PIM-SM Status

**Menu Path:** [Routing](#) > [Multicast Route](#) > [PIM-SM](#) > [PIM-SM Status](#)

This page lets you monitor the status of PIM-SM.

This page includes these tabs:

- Interface

- Neighbor
- BSR/RP

## PIM-SM Status - Interface

**Menu Path: Routing > Multicast Route > PIM-SM > PIM-SM Status - Interface**

This page lets you monitor the PIM-SM status of your device's interfaces.

Interface Name	Interface Alias	IP Address	PIM-SM	DR Address
Max. 256				
0 of 0				

UI Setting	Description
<b>Interface Name</b>	Shows the name of the interface.
<b>Interface Alias</b>	Shows the alias of the interface.
<b>IP Address</b>	Shows the IP address of the interface.
<b>PIM-SM</b>	Shows whether PIM-SM is enabled or disabled on this interface.
<b>DR Address</b>	Shows the DR address of the interface.

## PIM-SM Status - Neighbor

**Menu Path: Routing > Multicast Route > PIM-SM > PIM-SM Status - Neighbor**

This page lets you monitor the status of PIM-SM neighbors.



Neighbor	Interface Name	Uptime	Expiration Time	DR Priority
Max. 256				0 of 0

UI Setting	Description
<b>Neighbor</b>	Shows the IP address of the neighbor connected to your device.
<b>Interface Name</b>	Shows the interface the neighbor is connected to.
<b>Uptime</b>	Shows how long this multicast route entry has been maintained by this device.
<b>Expiration Time</b>	Shows the time remaining before this multicast route is removed from the multicast routing table if it is not refreshed.
<b>DR Priority</b>	Shows the DR priority of this neighbor. Higher values have higher preference for the DR election process.

## PIM-SM Status - BSR/RP

**Menu Path: Routing > Multicast Route > PIM-SM > PIM-SM Status - BSR/RP**

This page lets you monitor the BSR and static RP status of PIM-SM in the network.

### Elected BSR

Elected BSR	
BSR Address	---
BSR Priority	0
BSR Hash Mask Length	0

UI Setting	Description
<b>BSR Address</b>	Shows the address of the current elected BSR.
<b>BSR Priority</b>	Shows the priority of the BSR.
<b>BSR Hash Mask Length</b>	Shows the hash mask length of the BSR.

## RP Mapping

**RP Mapping**

Group Address \* RP Mapping Result

---

**FIND RP**

UI Setting	Description
<b>Group Address</b>	Enter a group address and click <b>FIND RP</b> to search for the RP for the group address.
<b>RP Mapping Result</b>	Shows the result of the RP search.

## PIM-SM Status - BSR/RP List

🔄 🏠
🔍 Search

Type	Group Address	Group Mask	RP Address	Priority	Hold Time (sec.)	Expiration Time
0 of 0						

UI Setting	Description
<b>Type</b>	Shows the role type of this entry.

UI Setting	Description
<b>Group Address</b>	Shows the group address of the BSR or RP this entry is for.
<b>Group Mask</b>	Shows the subnet mask of the group address.
<b>RP Address</b>	Shows the RP of this group address.
<b>Priority</b>	Shows the RP priority. Lower values have higher preference for the RP election process.
<b>Hold Time (sec.)</b>	Shows the hold time in seconds. The hold time is the amount of time a router will maintain the state information for this multicast group before deleting it due to inactivity.
<b>Expiration Time</b>	Shows the time remaining before this multicast route is removed from the multicast routing table if it is not refreshed.

## Multicast Local Route

Multicast Local Route is a method of forwarding traffic to multicast groups based on source and downstream VLAN settings. It enables precise control over multicast traffic within a network by allowing specific multicast streams to be permitted or denied.

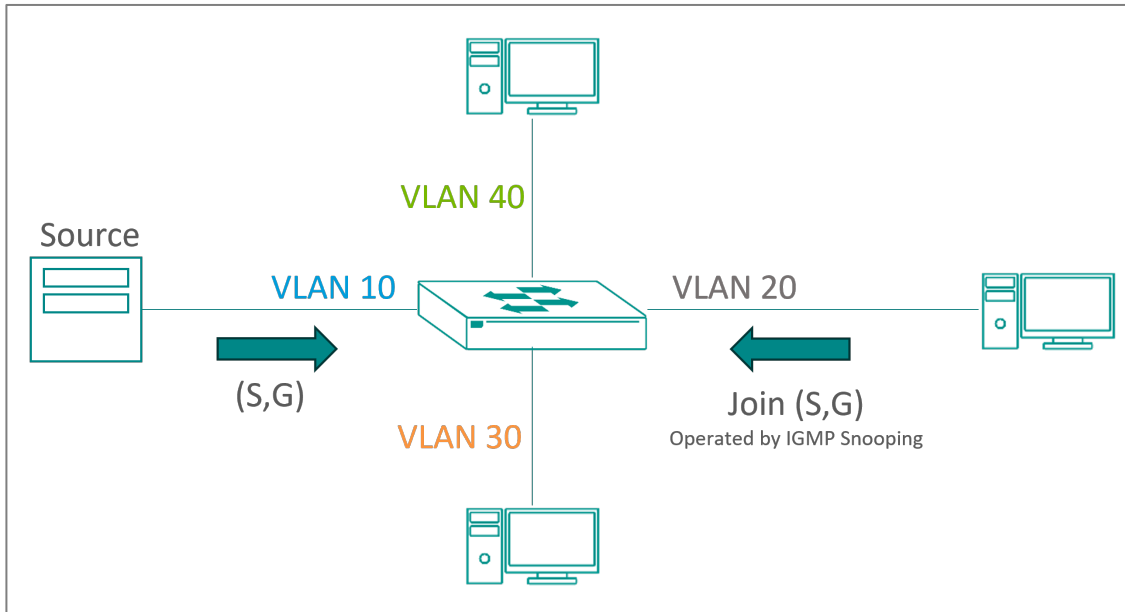
### Multicast Local Route In Depth

#### Using VLANs

Users can set a multicast route by configuring its source VLAN and downstream VLAN interfaces.

#### Using MACL

MACL (Multicast ACL) determines whether to allow or block multicast streams. The MACL checking sequence is prioritized based on MACL IDs, with smaller ID numbers having higher priority. If a multicast routing is filtered by a higher-priority MACL profile, lower-priority access control profiles will not be executed, ensuring that only the most critical routing decisions are applied.



## Multicast Local Route

**Menu Path: Routing > Multicast Route > Multicast Local Route**

This page lets you manage multicast local routing for your device.

This page includes these tabs:

- General
- Routes
- MACL

### Multicast Local Route

**Menu Path: Routing > Multicast Route > Multicast Local Route - General**

This page lets you configure general settings for multicast local routing.

## Multicast Local Route - General

Multicast Local Route \*

Disabled ▼ ⓘ

---

VRRP Master Only \*

Enabled ▼ ⓘ

---

**APPLY**

UI Setting	Description	Valid Range	Default Value
<b>Multicast Local Route</b>	<p>Enable or disable multicast local routing.</p> <div style="background-color: #f0f0f0; padding: 5px; margin-top: 10px;"> <p><b>Note</b></p> <p>Multicast local routing is based on IGMP snooping, so if you enable <b>Multicast Local Route</b>, make sure IGMP snooping is enabled. Refer to <a href="#">IGMP Snooping</a> for more information.</p> </div> <div style="background-color: #f0f0f0; padding: 5px; margin-top: 10px;"> <p><b>Note</b></p> <p>Only one multicast routing protocol can be active, so if you enable <b>Multicast Local Route</b>, make sure you disable PIM-DM and PIM-SM. Refer to <a href="#">PIM-DM</a> and <a href="#">PIM-SM</a> for more information.</p> </div>	Enabled / Disabled	Disabled
<b>VRRP Master Only</b>	When enabled, the device will only be able to route multicast streams if it is acting as the VRRP master.	Enabled / Disabled	Enabled

## Multicast Local Route - Routes

**Menu Path:** [Routing](#) > [Multicast Route](#) > [Multicast Local Route - Routes](#)

This page lets you create and edit multicast local routes.

## Multicast Local Route List

The screenshot shows a user interface for managing Multicast Local Routes. At the top left is a plus sign icon for adding new routes. To its right is a search bar with a magnifying glass icon and the text 'Search'. Below these is a table with a header row containing a checkbox, 'Source VLAN ↑', and 'Downstream VLAN'. The table is currently empty. At the bottom left, it says 'Max. 16' and at the bottom right, it says '0 of 0'.

UI Setting	Description
Source VLAN	Shows the source VLAN of the multicast route.
Downstream VLAN	Shows the downstream VLANs of the multicast route.



## Creating a Multicast Local Route

### Menu Path: Routing > Multicast Route > Multicast Local Route - Routes

Clicking the **Add (+)** icon on the **Routing > Multicast Route > Multicast Local Route - Routes** page will open this dialog box. This dialog lets you create a new multicast local route.


Click **CREATE** to save your changes and add the new route.

The screenshot shows a dialog box titled 'Create Multicast Local Route'. It has two dropdown menus: 'Source VLAN \*' and 'Downstream VLAN \*'. At the bottom right, there are two buttons: 'CANCEL' and 'CREATE'.

UI Setting	Description	Valid Range	Default Value
<b>Source VLAN</b>	Select the source VLAN of this multicast route.  <div style="border: 1px solid #ccc; background-color: #f9f9f9; padding: 5px;"> <p> <b>Note</b> A VLAN must be created and set to an L3 interface before you can select it.</p> </div>	Drop-down list of VLAN interfaces	N/A
<b>Downstream VLAN</b>	Select the downstream VLANs for this multicast route. You can select multiple VLANs.  <div style="border: 1px solid #ccc; background-color: #f9f9f9; padding: 5px;"> <p> <b>Note</b> A VLAN must be created and set to an L3 interface before you can select it.</p> </div>	Drop-down list of VLAN interfaces, multiple VLANs can be selected	N/A

## Editing a Multicast Local Route - Routes

**Menu Path:** [Routing](#) > [Multicast Route](#) > [Multicast Local Route - Routes](#)

Clicking the **Edit** () icon for a route on the **Routing > Multicast Route > Multicast Local Route - Routes** page will open this dialog box. This dialog lets you edit the route.

Click **APPLY** to save your changes.

### Edit Source VLAN 1

Downstream VLAN \*

vlan20 

---

CANCEL APPLY

UI Setting	Description	Valid Range	Default Value
<b>Downstream VLAN</b>	Select the downstream VLANs for this multicast route. You can select multiple VLANs.  <div style="border: 1px solid #ccc; padding: 5px; background-color: #f9f9f9;"> <p> <b>Note</b> A VLAN must be created and set to an L3 interface before you can select it.</p> </div>	Drop-down list of VLAN interfaces, multiple VLANs can be selected	N/A

## Deleting a Multicast Local Route

**Menu Path:** [Routing](#) > [Multicast Route](#) > [Multicast Local Route - Routes](#)

You can delete a route by using the checkboxes to select the routes you want to delete, then clicking the **Delete** () icon.

## Multicast Local Route - MACL

**Menu Path:** [Routing](#) > [Multicast Route](#) > [Multicast Local Route - MACL](#)

This page lets you manage the Multicast Access Control List (MACL).

Multicast Local Route								
General		Routes			MACL			
		Q Search						
<input type="checkbox"/>	MACL ID	Multicast Group	Group Mask	Source IP Address	Source IP Mask	Source VLAN	Downstream VLAN	Action
<input type="checkbox"/>	1	224.0.0.0	255.255.255.0	192.168.126.253	255.255.255.255	1	20	Permit
Max. 16								1 - 1 of 1

UI Setting	Description
<b>MACL ID</b>	Shows the ID for this MACL entry.
<b>Multicast Group</b>	Shows the multicast group of this multicast route.
<b>Group Mask</b>	Shows the subnet mask of this multicast route.



UI Setting	Description
<b>Source IP Address</b>	Shows the source IP address of this multicast route.
<b>Source IP Mask</b>	Shows the subnet mask of the source IP.
<b>Source VLAN</b>	Shows the source VLAN ID for the source IP.
<b>Downstream VLAN</b>	Shows the downstream VLAN for this multicast route.
<b>Action</b>	Shows the action to take for this route. <ul style="list-style-type: none"> <li>• <b>Permit:</b> Traffic using this route will be permitted</li> <li>• <b>Deny:</b> Traffic through this route will be dropped</li> </ul>

## Creating a MACL Entry

**Menu Path:** [Routing](#) > [Multicast Route](#) > [Multicast Local Route - MACL](#)

Clicking the **Add (+)** icon on the **Routing > Multicast Route > Multicast Local Route - MACL** page will open this dialog box. This dialog lets you create a new MACL entry.

Click **CREATE** to save your changes and add the new entry.

### Create Multicast ACL

MACL ID \*

Multicast Group  
Any

Group Mask

Source IP Address  
Any

Source IP Mask

Source VLAN  
Any

1 - 4094

Downstream VLAN  
Any

1 - 4094

Action \*

UI Setting	Description	Valid Range	Default Value
<b>MACL ID</b>	Specify the ID for this MACL entry.	1 to 16	N/A
<b>Multicast Group</b>	Specify the multicast group of this multicast route.	224.0.0.0 to 239.255.255.25	N/A
<b>Group Mask</b>	Select the subnet mask of this multicast route.	Drop-down list of subnet masks	N/A
<b>Source IP Address</b>	Specify the source IP address of this multicast route.	Valid IP address	N/A
<b>Source IP Mask</b>	Select the subnet mask of the source IP.	Drop-down list of subnet masks	N/A

UI Setting	Description	Valid Range	Default Value
<b>Source VLAN</b>	Specify the source VLAN ID for the source IP.	1 to 4094	N/A
<b>Downstream VLAN</b>	Specify the downstream VLAN for this multicast route.	1 to 4094	N/A
<b>Action</b>	Select the action to take for this route. <ul style="list-style-type: none"> <li>• <b>Permit:</b> Traffic using this route will be permitted</li> <li>• <b>Deny:</b> Traffic through this route will be dropped</li> </ul>	Permit / Deny	N/A

### Editing a MACL Entry

**Menu Path:** [Routing](#) > [Multicast Route](#) > [Multicast Local Route - MACL](#)

Clicking the **Edit** (✎) icon for an entry on the **Routing > Multicast Route > Multicast Local Route - MACL** page will open this dialog box. This dialog lets you edit the entry.

Click **APPLY** to save your changes.

### Edit MACL ID 1

Multicast Group	Group Mask
224.0.0.0	24 (255.255.255.0) ▼
Source IP Address	Source IP Mask
192.168.126.253	32 (255.255.255.255) ▼
Source VLAN	
1	
1 - 4094	
Downstream VLAN	
20	
1 - 4094	
Action *	
Permit ▼	


CANCEL
APPLY

UI Setting	Description	Valid Range	Default Value
<b>MACL ID</b>	Specify the ID for this MACL entry.	1 to 16	N/A
<b>Multicast Group</b>	Specify the multicast group of this multicast route.	224.0.0.0 to 239.255.255.25	N/A
<b>Group Mask</b>	Select the subnet mask of this multicast route.	Drop-down list of subnet masks	N/A
<b>Source IP Address</b>	Specify the source IP address of this multicast route.	Valid IP address	N/A
<b>Source IP Mask</b>	Select the subnet mask of the source IP.	Drop-down list of subnet masks	N/A
<b>Source VLAN</b>	Specify the source VLAN ID for the source IP.	1 to 4094	N/A
<b>Downstream VLAN</b>	Specify the downstream VLAN for this multicast route.	1 to 4094	N/A

UI Setting	Description	Valid Range	Default Value
<b>Action</b>	Select the action to take for this route. <ul style="list-style-type: none"> <li><b>Permit:</b> Traffic using this route will be permitted</li> <li><b>Deny:</b> Traffic through this route will be dropped</li> </ul>	Permit / Deny	N/A

## Deleting a MACL Entry

### Menu Path: Routing > Multicast Route > Multicast Local Route - MACL

You can delete an entry by using the checkboxes to select the entries you want to delete, then clicking the **Delete** (  ) icon.

## Multicast Routing Table

### Menu Path: Routing > Multicast Route > Multicast Routing Table

This page lets you see the current multicast routing table for your device.

## Multicast Routing Table

Multicast Routing Table							
Mode	Multicast Group	Source	Upstream Neighbor	Uptime	Expiration Time	Incoming Interface	Outgoing Interface
Multicast Local Route	239.1.1.1	192.168.110.50	—	0d0h4m7s	0h3m22s	vlan10	vlan20

Max. 2048 Items per page: 50 1 - 1 of 1

UI Setting	Description
<b>Mode</b>	Shows the multicast routing protocol used for the route this entry is for.
<b>Multicast Group</b>	Shows the group address of the route.
<b>Source</b>	Shows the source IP of the multicast group.

UI Setting	Description
<b>Upstream Neighbor</b>	Shows the closest neighbor forwarding multicast traffic to this device for this route.
<b>Uptime</b>	Shows how long this multicast route entry has been maintained by this device.
<b>Expiration Time</b>	Shows the time remaining before this multicast route is removed from the multicast routing table if it is not refreshed.
<b>Incoming Interface</b>	Shows the interface receiving multicast traffic for this route.
<b>Outgoing Interface</b>	Shows the interface forwarding multicast traffic for this route.

# Security

## Menu Path: Security

This section lets you configure the security settings of your device.

This section includes these pages:

- Device Security
- Network Security
- Authentication

## Security - User Privileges

Privileges to settings are granted to the different authority levels as follows. Refer to [System > Account Management > User Accounts](#) for more information on user accounts.

Settings	Admin	Supervisor	User
<b>Device Security</b>			
<b>Login Policy</b>	R/W	R	R
<b>Trusted Access</b>	R/W	R	R
<b>SSH &amp; SSL</b>	R/W	R/W	-
<b>Network Security</b>			
<b>IEEE 802.1X</b>	R/W	R/W	R
<b>MAC Authentication Bypass</b>	R/W	R/W	R
<b>MAC Security</b>	R/W	R/W	R
<b>Port Security</b>	R/W	R/W	R
<b>Traffic Storm Control</b>	R/W	R/W	R
<b>Access Control List</b>	R/W	R/W	R
<b>Network Loop Protection</b>	R/W	R/W	R

Settings	Admin	Supervisor	User
<b>Binding Database</b>	R/W	R/W	R
<b>DHCP Snooping</b>	R/W	R/W	R
<b>IP Source Guard</b>	R/W	R/W	R
<b>Dynamic ARP Inspection</b>	R/W	R/W	R
<b>Authentication</b>			
<b>Login Authentication</b>	R/W	-	-
<b>RADIUS</b>	R/W	-	-
<b>TACACS+</b>	R/W	-	-

## Device Security

### Menu Path: [Security](#) > [Device Security](#)

This section lets you configure the device-level security settings of your device.

This section includes these pages:

- [Login Policy](#)
- [Trusted Access](#)
- [SSH & SSL](#)

### About Login Policy

Login Policy lets you define and enforce login restrictions to improve the security of your device and protect it from unauthorized access from brute force attacks.

### Login Policy

#### Menu Path: [Security](#) > [Device Security](#) > [Login Policy](#)

This page lets you configure the login policies for your device.

Click **APPLY** to save your changes.



## Login Policy Settings

### Login Policy

Login Message 0 / 500

---

Login Authentication Failure Message 0 / 500

---

Account Login Failure Lockout \*  
Disabled

Retry Failure Threshold \*  
5  
1 - 10 times

Lockout Duration \*  
5  
1 - 10 min.

Auto Logout After \*  
5  
0 - 1440 min.

APPLY

UI Setting	Description	Valid Range	Default Value
<b>Login Message</b>	Specify the welcome message to display when users log in to the device.	0 to 500 characters	N/A
<b>Login Authentication Failure Message</b>	Specify the message to display if the user fails to log in.  <div style="background-color: #fff9c4; padding: 10px; border: 1px solid #ccc;"> <p><b>⚠ Warning</b></p> <p>The Login Authentication Failure Message should not include information about passwords or other sensitive information.</p> </div>	0 to 500 characters	N/A
<b>Account Login Failure Lockout</b>	Enable or disable the lockout function, which will temporarily prevent users from logging in for the <b>Lockout Duration</b> after the <b>Retry Failure Threshold</b> is exceeded. This can be useful for preventing brute force attacks.	Enabled / Disabled	Disabled
<b>Retry Failure Threshold</b>	Specify the number of login retry attempts allowed before the user is locked out for the <b>Lockout Duration</b> .	1 to 10	5
<b>Lockout Duration</b>	Specify the lockout duration in minutes during which a locked-out user will be unable to log in.	1 to 10	5
<b>Auto Logout After</b>	Specify the amount of time in minutes a user can be idle before they will be automatically logged out from the device.	0 to 1440	5

## About Trusted Access

Trusted Access is a feature that allows device management only from trusted IP addresses that you specify.

Trusted access is a crucial mechanism for maintaining the security and integrity of your network infrastructure. It ensures that only authorized devices can connect to sensitive network resources, reducing the risk of unauthorized access and potential security breaches.

### Why Trusted Access Matters

- **Security:** By allowlisting IP addresses, administrators ensure that only devices with approved IP addresses can access the network configuration, helping to prevent unauthorized connections.
- **Access Control:** Trusted access enables administrators to define which IP addresses can connect to sensitive resources, ensuring that only trusted devices interact with critical areas of the network.

### How Trusted Access Works


Enabling trusted access on a device involves configuring IP allowlists. Once an IP address is allowlisted, the device treats it as trusted, allowing access to device management functions. Devices not on the allowlist are denied access, helping to maintain a secure and controlled network environment.

### Example: Configuring and Enabling Trusted Access

Enable trusted IP address settings to only allow users to access network device management features from IP addresses you choose. Only IPv4 addresses are supported.

Make sure you add all management devices to the allowlist before enabling Trusted Access, otherwise you may lose access to the management console.

To configure trusted access, do the following:

1. Sign in to the device using administrator credentials.
2. Go to **Security > Device Security > Trusted Access**, and then click  **[Add]**.

The Create Entry screen appears.

3. Specify the **IP Address** and **Subnet Mask** of the device to add the device IP to the allowlist, and then click **Create**.

The specified **IP Address** and **Netmask** appear on the Trusted Access list.

4. Once you have created entries for all devices, under **Trusted Access**, choose **Enabled**, and then click **Apply**.

Trusted access will now be enabled, and only devices on the allowlist will be able to access management features.

## Trusted Access

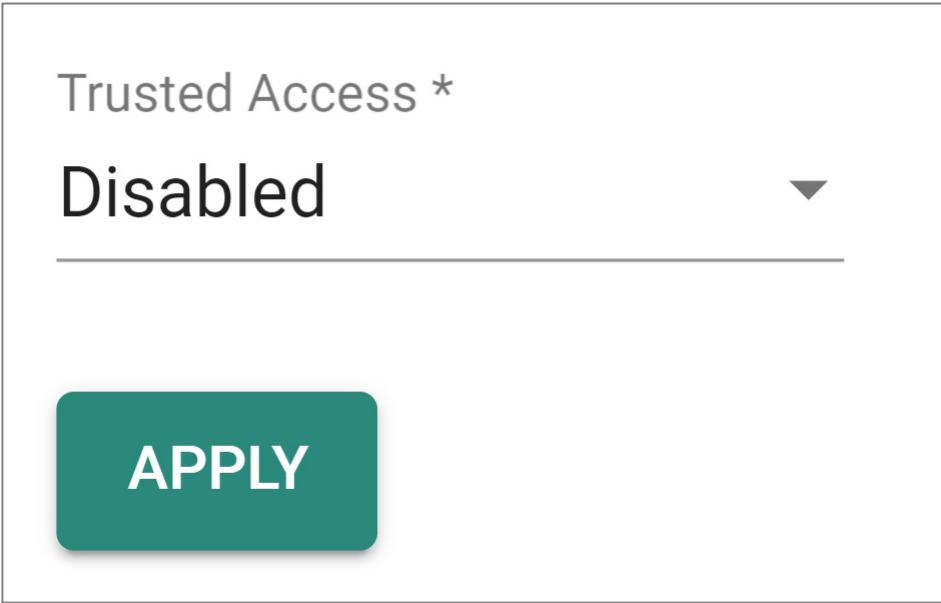
**Menu Path: Security > Device Security > Trusted Access**

This page lets you limit access to the device to trusted IP addresses you specify. You can also limit access to the device to LAN connections only.

### ⓘ Limitations

You can create up to 20 trusted IP entries.

## Trusted Access Settings



Trusted Access \*

Disabled ▼

**APPLY**

UI Setting	Description	Valid Range	Default Value
<b>Trusted Access</b>	<p>Enable or disable the Trusted IP List.</p> <p><b>Enabled:</b> Only IP addresses in the Trusted IP List can access the device.</p> <p><b>Disabled:</b> Any IP address can access the device.</p> <div style="background-color: #f0f0f0; padding: 10px; margin: 10px 0;"> <p><b>Note</b></p> <p>Trusted Access cannot be enabled if there are no entries in the Trusted Access List.</p> </div> <div style="background-color: #fff9c4; padding: 10px; margin: 10px 0;"> <p><b>Warning</b></p> <p>Depending on the features you enable, you may lose access to your device if the computer you are using to configure the device is not in the Trusted Access List or connected through a LAN connection.</p> </div>	Enabled / Disabled	Disabled

## Trusted Access List

		Search
<input type="checkbox"/>	IP Address	Netmask
<input type="checkbox"/>	196.122.23.23	255.255.255.0
Max. 20		1 - 1 of 1

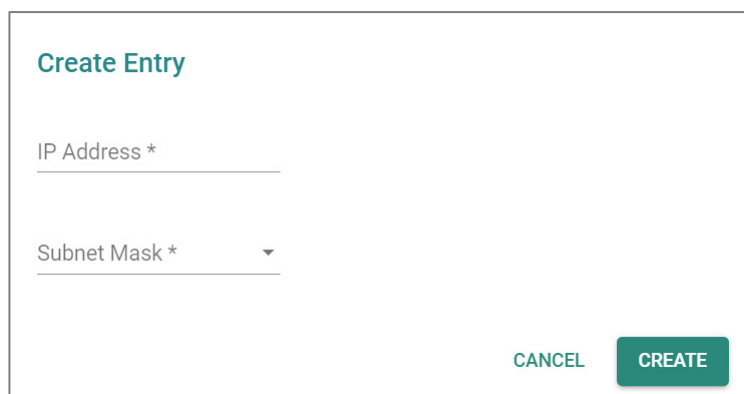
UI Setting	Description
<b>IP Address</b>	Shows the IP address of the Trusted IP entry.
<b>Subnet Mask</b>	Shows the netmask of the Trusted IP entry.

## Trusted Access - Create Entry

### Menu Path: Security > Device Security > Trusted Access

Clicking the **Add (+)** icon on the **Security > Device Security > Trusted Access** page will open this dialog box. This dialog lets you create a trusted IP entry.

Click **CREATE** to save your changes and add the new entry.



The dialog box titled "Create Entry" contains two input fields: "IP Address \*" and "Subnet Mask \*". The "Subnet Mask \*" field is a dropdown menu. At the bottom right, there are two buttons: "CANCEL" and "CREATE".

UI Setting	Description	Valid Range	Default Value
<b>IP Address</b>	Specify the IP address of the trusted host(s).	Valid IP Address	N/A
<b>Subnet Mask</b>	Select a netmask for the trusted host(s).	Drop-down list of subnet masks	N/A

## About SSH & SSL

SSH and SSL are security protocols.

- **Secure Shell (SSH):** SSH is the recommended protocol for secure command-line access. This protocol encrypts the communication channel between a user and a device's management interface. This helps ensure that any data exchanged—like usernames, passwords, or configuration commands—remains hidden from eavesdroppers on the network.
- **Secure Sockets Layer (SSL):** While functionally similar to SSH, SSL is often used for web-based applications. Though The term "Secure Sockets Layer (SSL)" is still commonly used, it's important to note that it's been deprecated in favor of the more secure Transport Layer Security (TLS) protocol. In the context of

Ethernet switches, some may offer a web interface for management tasks. Moxa switches support TLS versions 1.2 and 1.3. TLS encrypts the communication channel between a user's web browser and a device's web interface. This ensures the security of sensitive data during remote configuration tasks performed through the web interface.

**✎ Note**

Certificates: Self-signed vs. Trusted

There are two main types of certificates used for TLS connections: self-signed certificates and trusted certificates.

- Self-signed certificates: These certificates are issued by the device itself and are not verified by a third-party Certificate Authority (CA). While they provide basic encryption, they may generate warnings in web browsers due to the lack of trust verification.
- Trusted certificates: These certificates are issued by a trusted CA and are generally considered more secure. Web browsers readily accept connections secured with trusted certificates.

The choice between self-signed and trusted certificates depends on your specific security requirements.

## SSH & SSL

**Menu Path: [Security](#) > [Device Security](#) > [SSH & SSL](#)**

This page lets you manage your SSH key and SSL certificate.

This page includes these tabs:

- SSH
- SSL

### SSH

**Menu Path: [Security](#) > [Device Security](#) > [SSH & SSL - SSH](#)**

This page lets you manage your device's SSH key.

**Note**

Regenerating your SSH key regularly strengthens SSH security by invalidating potentially compromised keys and adding another layer of defense against unauthorized access. There's no one-size-fits-all answer for how often to regenerate keys; it depends on security risk factors like server importance, access frequency, and potential exposure. Consider regenerating them every few months or every year, especially for critical servers.

## Regenerate SSH Key

Created on  
Aug 10 07:23:59 2023 GMT

---

Regenerate SSH Key

**REGENERATE**

UI Setting	Description	Valid Range	Default Value
<b>Created on</b>	Shows the date and time the current SSH key was created.	N/A	N/A
<b>Regenerate SSH Key</b>	Click <b>REGENERATE</b> to regenerate the SSH key.  <b>Warning</b> Regenerating the SSH key will restart the device's system services and will make the device temporarily unavailable.	N/A	N/A

## SSL

### Menu Path: Security > Device Security > SSH & SSL - SSL

This page lets you manage your device's SSL certificate. Click **APPLY** to save your changes.

## Certificate Information

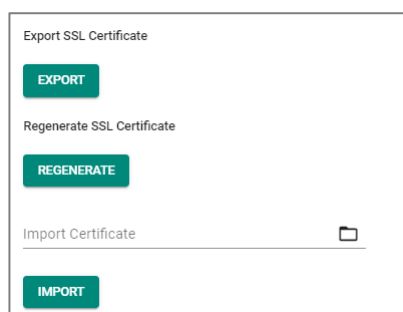
Certificate Information	
CA Name	Expiration Date
Moxa Networking Co., Ltd.	2034-01-18 18:53:53

UI Setting	Description
<b>CA Name</b>	Shows the CA name of the SSL certificate.
<b>Expiration Date</b>	Shows when the current certificate will expire.

## SSL Settings

To import a customer certificate, follow the steps below:

1. Import root CA generated by customer's CA server to a PC.
2. 'Export' the CSR file from the switch and use the customer's CA server to generate a certificate.
3. 'Import' the certificate to the switch.



UI Setting	Description	Valid Range	Default Value
<b>Export SSL Certificate Request</b>	Click <b>EXPORT</b> to export the SSL Certificate Signing Request (*.csr) to your local computer.	N/A	N/A
<b>Regenerate SSL Certificate</b>	Click <b>REGENERATE</b> to regenerate the SSL certificate.	N/A	N/A
<b>Import Certificate</b>	Select an SSL certificate from your computer (*.cert), then click <b>IMPORT</b> to import the certificate to your device.	N/A	N/A

## Network Security

### Menu Path: Security > Network Security

This section lets you configure the network-level security settings of your device.



This section includes these pages:

- IEEE 802.1X
- MAC Authentication Bypass
- MACsec
- Port Security
- Traffic Storm Control
- Access Control List
- Network Loop Protection
- Binding Database
- DHCP Snooping
- IP Source Guard
- Dynamic ARP Inspection

## **About IEEE 802.1X**

IEEE 802.1X is a standard for managing access control, ensuring that devices seeking to access network resources are what they claim to be.

## **About IEEE 802.1X**

802.1X is a standard for port-based Network Access Control (NAC) that provides an authentication framework for devices trying to connect to a network.

Part of the IEEE 802.1 group of networking protocols, the primary purpose of 802.1X is to enhance the security of wired and wireless networks by requiring users and devices to authenticate themselves before gaining access to network resources.

## **Topology**

An 802.1X topology has three roles:

- Supplicant: The client device (e.g., laptop, smartphone) seeking network access.
- Authenticator: The network device (e.g., switch, wireless access point) that controls access to the network ports.

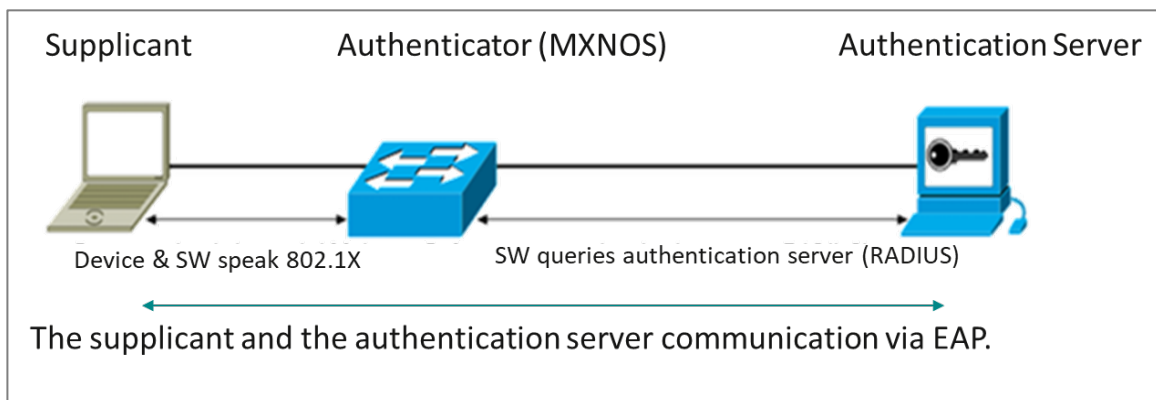
- **Authentication Server:** A server that performs the actual authentication of the supplicant. It could be a RADIUS (Remote Authentication Dial-In User Service) server or another centralized authentication service.

**Note**

In an 802.1X environment, Moxa switches primarily function as authenticators. However, they can also be optionally configured to act as authentication servers.

In an 802.1X authentication system, the supplicant (client), authenticator device (Switch or Wi-Fi AP), and authentication server exchange information using the Extensible Authentication Protocol (EAP).

A supplicant and an authenticator exchange EAPOL (Extensible Authentication Protocol over LAN) frames with each other. We can either use an external RADIUS server as the authentication server or implement the authentication server in the Moxa switch by using a Local User Database as the authentication look-up table. When using an external RADIUS server as the authentication server, the authenticator and the authentication server exchange EAP frames.

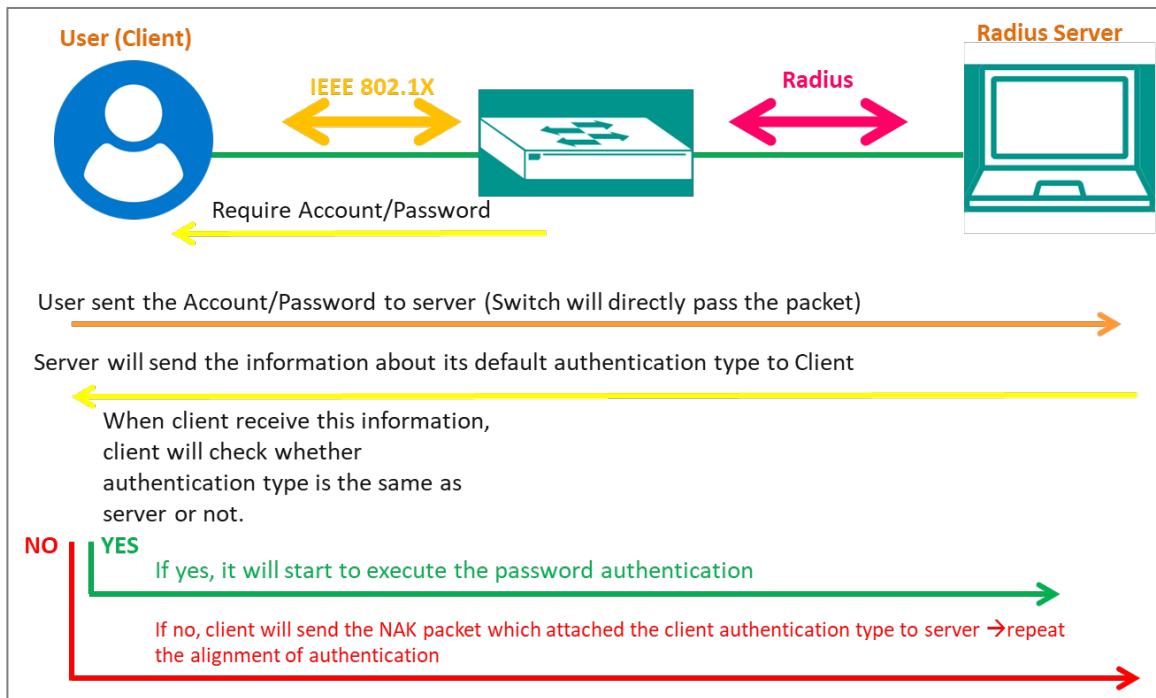


**Note**

It is possible to use 802.1X authentication without a separate authentication server using local authentication. The Authenticator can be configured to determine client access rights.

### Authentication Process

When a device connects to a network port configured for 802.1X, the following process occurs:



1. Initialization: The supplicant sends an EAPOL (Extensible Authentication Protocol Over LAN) start message to the authenticator.
2. Authentication Request: The authenticator replies with an EAP Request/Identity message, prompting the supplicant to provide its identity.
3. Identity Response: The supplicant responds with its identity, typically a username.
4. Authentication Exchange: The authenticator relays the identity to the authentication server, which then initiates an authentication exchange with the supplicant using EAP (Extensible Authentication Protocol).
5. Authentication Result: Based on the outcome of the authentication process (which could involve methods like username/password, digital certificates, or other credentials), the authentication server sends an Accept or Reject message to the authenticator.
6. Access Granted/Denied: If authentication is successful, the authenticator allows the supplicant access to the network. If authentication fails, access is denied.

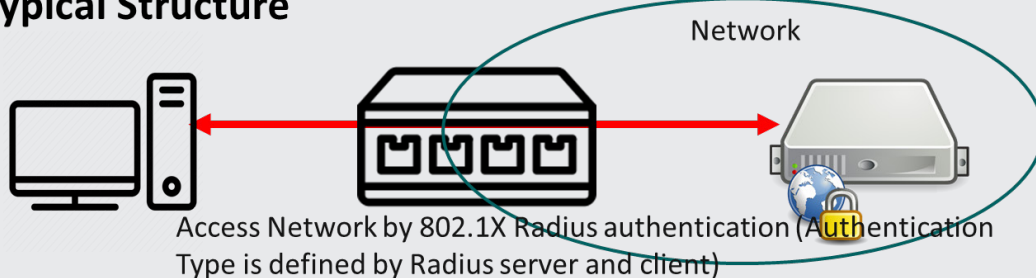
802.1X provides a robust mechanism for controlling network access, ensuring that only authorized users and devices can connect to the network. It's widely used in enterprise environments to enforce security policies and protect against unauthorized access. The following diagram illustrates the process of a client establishing 802.1X communication with the authentication server through the MXNOS switch.

**Note**

Authentication can also be initiated by the authenticator. Ordinarily, supplicants initiate the authentication process, with an EAPOL-Start frame sent to the authenticator. When the authenticator initiates the authentication process (either on its own, or on receipt of an EAPOL-Start frame), it sends an EAP Request/Identity frame to ask for the username of the supplicant.

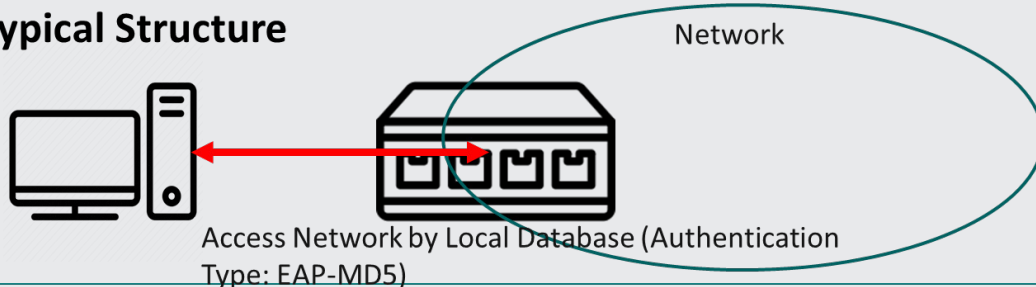
**802.1X Radius**

**Typical Structure**



**802.1X Local**

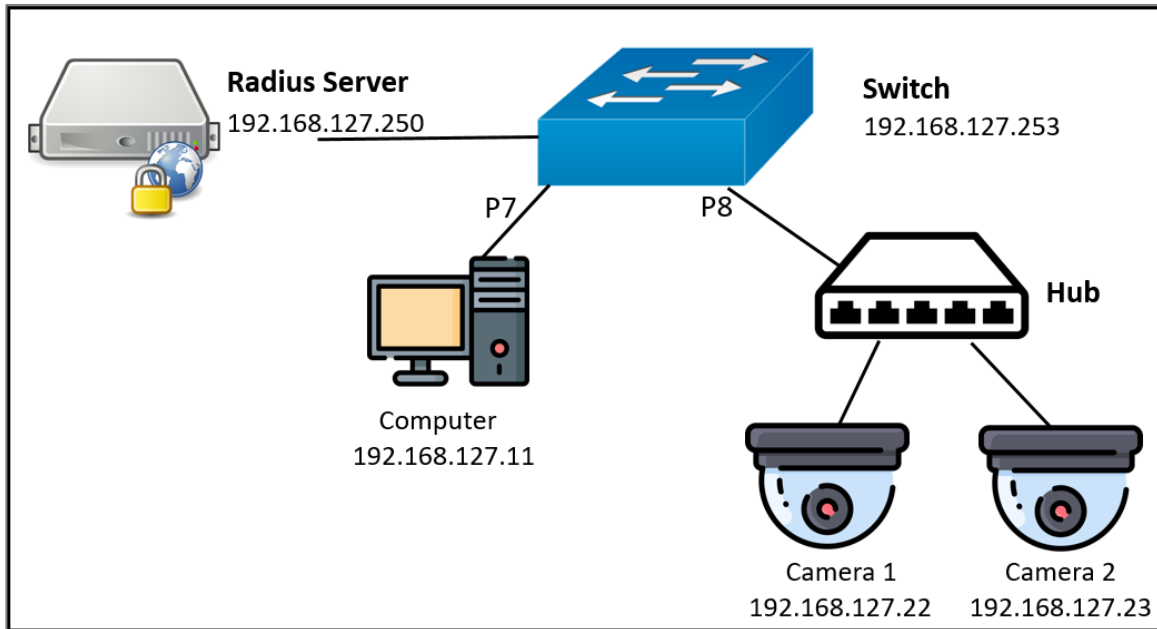
**Typical Structure**



**Example: Configuring a Switch as an Authenticator**

In this example, we configure a Moxa switch as an authenticator, connecting supplicant devices (2 cameras and a computer) to a RADIUS server.

Our sample topology should look like the following:




The topology uses the following roles:

- Supplicants:
  - Cameras 1 and 2, connected to the switch with a hub on port 8
  - Computer, connected on Port 7
- Authenticator: Switch
- Server: RADIUS server

**Before you begin:** This task uses sample values and assumes that a RADIUS server is already configured.


To configure the switch as an authenticator, do the following:

1. Sign in to the device using administrator credentials.
2. Got to **Security > Network Security > IEEE 802.1X**→**General**.
3. Click **IEEE 802.1X** and choose **Enabled** from the drop-down menu.
4. Click **Authentication Mode**, choose **RADIUS** from the drop-down menu, and then click **Apply** to save your settings.
5. To configure the example computer, click  **[Edit]** corresponding to **Port 7**.  
**Result:** The **Port Settings** screen appears.
6. Configure the following:

7.

Option	Value
Enabled	Enabled
Port Control	Auto
Authentication Session Type	Port-Based
Max. Request	2
Quiet Period	60
Reauthentication	Disabled

8. Click **Apply**.

9. To configure the example cameras, click  **[Edit]** corresponding to **Port 8**.

**Result:** The **Port Settings** screen appears.

10. Configure the following:

Option	Value
Enabled	Enabled
Port Control	Auto
Authentication Session Type	MAC-based
Max. Request	2
Quiet Period	60
Reauthentication	Disabled

11. Click **Apply**.

**What to do next:** You must configure RADIUS server settings before the switch can function as an authenticator.

### Example: Configuring RADIUS Server Settings

The switch must be configured with the RADIUS server settings before it can serve as an authenticator.

1. Sign in to the device using administrator credentials.
2. Go to **Security > Network Security > IEEE 802.1X > RADIUS**.
3. Specify all of the following:

Option	Value
<b>Server IP Address 1</b>	192.168.127.11
<b>Auth Port</b>	1812
<b>Share Key</b>	Type your key here
<b>Timeout</b>	5
<b>Retransmit</b>	5

4. Click **Apply** to save changes.

**What to do next:** Once configured, status information will be available under **Security > Network Security > IEEE 802.1X > Status**.

## IEEE 802.1X

**Menu Path:** [Security > Network Security > IEEE 802.1X](#)

This page lets you manage your device's IEEE 802.1X authentication feature.

This page includes these tabs:

- General
- RADIUS
- Local Database

### IEEE 802.1X - General

**Menu Path:** [Security > Network Security > IEEE 802.1X - General](#)

This page lets you configure your device's IEEE 802.1X settings.

## IEEE 802.1X Settings

IEEE 802.1X \*  
 Disabled ▼

---

Authentication Mode \*  
 Local Database ▼

---

APPLY

UI Setting	Description	Valid Range	Default Value
<b>IEEE 802.1X</b>	Enable or disable IEEE 802.1X authentication.  <div style="background-color: #f0f0f0; padding: 5px; border: 1px solid #ccc;"> <p> <b>Note</b>                          As of MX-NOS v5.0, enabling IEEE 802.1X allows VLAN assignment through a RADIUS server, but the VLAN must already exist.</p> </div>	Enabled / Disabled	Disabled
<b>Authentication Mode</b>	Specify the authentication mode to use. <ul style="list-style-type: none"> <li><b>RADIUS:</b> Use a RADIUS server for authentication.</li> <li><b>Local Database:</b> Use the local database for authentication.</li> </ul>	RADIUS / Local Database	Local Database

## IEEE 802.1X List

↻
🔍 Search

Port	Enable	Port Control	Max. Request	Quiet Period	Reauthentication	Reauthentication Period	Server Timeout	Supp Timeout	Tx Period	Port Status
1	Disabled	Auto	2	60	Disabled	3600	30	30	30	Authorized
2	Disabled	Auto	2	60	Disabled	3600	30	30	30	Authorized
3	Disabled	Auto	2	60	Disabled	3600	30	30	30	Authorized
4	Disabled	Auto	2	60	Disabled	3600	30	30	30	Authorized
5	Disabled	Auto	2	60	Disabled	3600	30	30	30	Authorized
6	Disabled	Auto	2	60	Disabled	3600	30	30	30	Authorized
7	Disabled	Auto	2	60	Disabled	3600	30	30	30	Authorized
8	Disabled	Auto	2	60	Disabled	3600	30	30	30	Authorized
9	Disabled	Auto	2	60	Disabled	3600	30	30	30	Authorized
10	Disabled	Auto	2	60	Disabled	3600	30	30	30	Authorized
11	Disabled	Auto	2	60	Disabled	3600	30	30	30	Authorized

1 - 24 of 24



UI Setting	Description
<b>Port</b>	Shows the port number the entry is for.
<b>Enable</b>	Shows whether IEEE 802.1X is enabled for the port.
<b>Port Control</b>	Shows the port control method used for the port.
<b>Max. Request</b>	Shows the maximum number of re-authentication requests allowed for the port.
<b>Quiet Period</b>	Shows the amount of time in seconds the device will remain in a quiet state following a failed authentication exchange with a client through the port.
<b>Reauthentication</b>	Shows whether IEEE 802.1X reauthentication is enabled for the port.
<b>Reauthentication Period</b>	Shows the amount of time in seconds to wait in between reauthentication attempts for the port.
<b>Server Timeout</b>	Shows the amount of time in seconds the device will try to retransmit packets to an authentication server.
<b>Supp Timeout</b>	Shows the amount of time in seconds the device will try to retransmit packets to a supplicant, such as a client PC.
<b>Tx Period</b>	Shows the amount of time in seconds the device will try to retransmit the data to a client.

## IEEE 802.1X - Edit Port Settings

**Menu Path:** Security > Network Security > IEEE 802.1X - General

Clicking the **Edit** (✎) icon for a port on the **Security > Network Security > IEEE 802.1X - General** page will open this dialog box. This dialog lets you edit the IEEE 802.1X settings for the port.

Click **APPLY** to save your changes.

### Port 1 Settings

Enabled\*  
Disabled ▼

Port Control\*  
Auto ▼

Max. Request\* Quiet Period\*  
2 60

1 - 10 times 0 - 65535 sec.

Reauthentication\* Reauthentication Period\*  
Disabled 3600

1 - 65535 sec.

Server Timeout\*  
30

1 - 65535 sec.

Supp Timeout\*  
30

1 - 65535 sec.

Tx Period\*  
30

1 - 65535 sec.

Copy configurations to ports ▼ ⓘ

CANCEL
APPLY

UI Setting	Description	Valid Range	Default Value
<b>Enabled</b>	Enable or disable IEEE 802.1X authentication for the port.	Enabled / Disabled	Disabled
<b>Port Control</b>	Select the port control method to use for the port. <ul style="list-style-type: none"> <li><b>Force Unauthorized:</b> The controlled port will stay in the unauthorized state.</li> <li><b>Auto:</b> The controlled port will be set to the authorized or unauthorized state based on the outcome of an authentication exchange between the supplicant and the authentication server.</li> <li><b>Force Authorized:</b> The controlled port will stay in the authorized state.</li> </ul>	Force Unauthorized / Auto / Force Authorized	Auto
<b>Max. Request</b>	Specify how many times to attempt reauthentication for the port.	1 to 10	2
<b>Quiet Period</b>	Specify the amount of time in seconds the device will remain in a quiet state following a failed authentication exchange with a client through the port.	0 to 65535	60

UI Setting	Description	Valid Range	Default Value
<b>Reauthentication</b>	Enable/disable IEEE 802.1X reauthentication for the port.	Enabled / Disabled	Disabled
<b>Reauthentication Period</b>	Specify the amount of time in seconds to wait in between reauthentication attempts for the port.	1 to 65535	3600
<b>Server Timeout</b>	Specify the amount of time in seconds the device will try to retransmit packets to an authentication server.	1 to 65535	30
<b>Supp Timeout</b>	Specify the amount of time in seconds the device will try to retransmit packets to a supplicant, such as a client PC.	1 to 65535	30
<b>Tx Period</b>	Specify the amount of time in seconds the device will try to retransmit the data to a client.	1 to 65535	30
<b>Copy configurations to ports</b>	Select the ports you want to copy this configuration to.	Drop-down list of ports	N/A

## IEEE 802.1X - RADIUS

### Menu Path: Security > Network Security > IEEE 802.1X - RADIUS

This page lets you specify a RADIUS server to use for IEEE 802.1X authentication. Click **APPLY** to save your changes.

#### Note

The system will use the primary RADIUS server by default. If the primary RADIUS server is unavailable, it will use the secondary RADIUS server.

## IEEE 802.1X RADIUS Settings

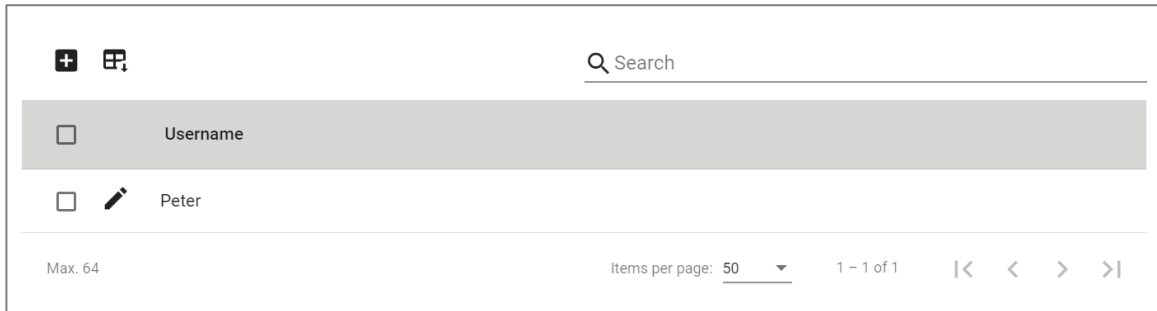
#### Note

802.1X and MAC authentication bypass share the same RADIUS server settings; changes made here will also affect the other feature.



### 🔔 Limitations

You can create up to 64 IEEE 802.1X local database accounts.



UI Setting	Description
<b>Username</b>	Shows the username of the account.

## IEEE 802.1X - Local Database - Account Settings

### Menu Path: Security > Network Security > IEEE 802.1X - Local Database

Clicking the **Add (+)** icon on the **Security > Network Security > IEEE 802.1X - Local Database** page will open this dialog box. This dialog lets you create a new user account for IEEE 802.1X authentication.

Click **CREATE** to save your changes and add the new account.

### Account Settings

Username \*

0 / 20

Password \*

Minimum 4 characters 0 / 20

Confirm Password \*

Minimum 4 characters 0 / 20

CANCEL
APPLY

UI Setting	Description	Valid Range	Default Value
<b>Username</b>	Specify the username for this account.	1 to 20 characters	N/A
<b>Password</b>	Specify the password for this user account.	4 to 20 characters	N/A
<b>Confirm Password</b>	Re-enter the password for this user account.	4 to 20 characters	N/A

## About MAC Authentication Bypass

MAC Authentication Bypass (MAB) allows network access based on a device's Media Access Control (MAC) address, bypassing traditional username/password authentication methods like 802.1X. This feature is particularly useful for granting access to devices that cannot support more advanced authentication protocols.

### How MAC Authentication Bypass Works

MAB operates like a VIP list for your network. When a device connects, the network checks its MAC address against an approved list. If the MAC address is recognized, the device is granted access without needing additional authentication. If the MAC address isn't on the list, access is denied.

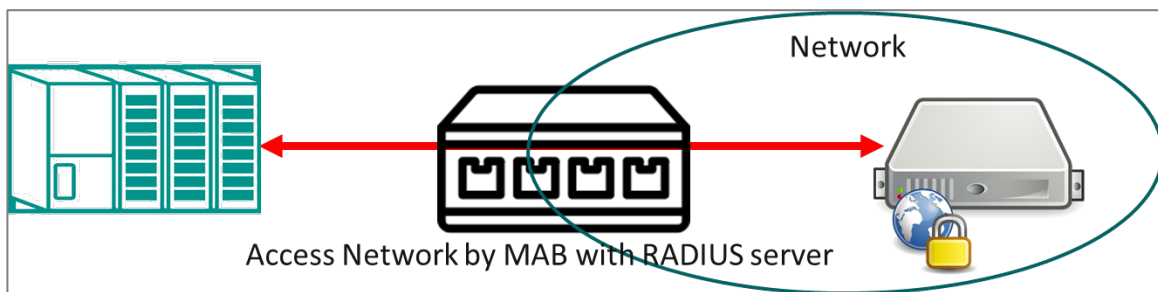
## When to Use MAB

- **Legacy Devices:** Some older devices may not support advanced authentication methods like 802.1X. MAB provides a way to allow these devices to connect using their MAC address.

While MAB is convenient, it's important to note that MAC addresses can be spoofed, making this method less secure compared to more robust authentication techniques. Therefore, MAB should be used in scenarios where ease of access is prioritized over stringent security measures.

## Configuring MAC Authentication Bypass

To add a device to MAC Authentication Bypass, first add the MAC address of the bypass device to the **Local Database**, then enable **MAC Authentication Bypass** on the Port the bypass device is attached to.




This procedure assumes that devices on your network are authenticated using either a RADIUS server or a local database.

### **Note**

MAC addresses are easily spoofed, and are not generally accepted as adequate means of authentication without other forms of security. Make sure that you have fully evaluated the security risks associated with this feature before use in a sensitive environment.


To configure MAC Authentication Bypass, do the following:

1. Sign in to the device using administrator credentials.
2. Go to **Security > Network Security > MAC Authentication Bypass**, click on the **Local Database** tab, and then click  **[Add]**.

The Create Entry screen appears.

3. Specify the **MAC Address** of the device to be added to the local database, and then click **Create**.

The MAC address appears in the table.

4. Click the **General** tab at the top of the screen, and verify that **MAC Authentication Bypass** is **Enabled**.
5. Locate the port the bypass device is attached to, and then click the corresponding  **[Edit]** button.

The Edit Port Settings screen appears.

6. Set **MAC Authentication Bypass** to **Enabled**, and then click **Apply**.

The bypass device will now be authenticated for network access.

## MAC Authentication Bypass

**Menu Path:** [Security](#) > [Network Security](#) > [MAC Authentication Bypass](#)

This page lets you configure the MAC Authentication Bypass settings.

This page includes these tabs:

- General
- RADIUS
- Local Database

### MAC Authentication Bypass - General

**Menu Path:** [Security](#) > [Network Security](#) > [MAC Authentication Bypass - General](#)

This page lets you configure general settings for MAC authentication bypass.



## MAC Authentication Bypass Settings

MAC Authentication Bypass \*

Disabled ▼

---

Authentication Mode \*

Local Database ▼

---

APPLY
CLEAR

UI Setting	Description	Valid Range	Default Value
<b>MAC Authentication Bypass</b>	Enable or disable MAC authentication bypass.	Enabled / Disabled	Disabled
<b>Authentication Mode</b>	Specify the authentication mode for MAC authentication bypass.	RADIUS / Local Database	Local Database

## MAC Authentication Bypass List

🔍 Search

	Port	MAB	Quiet Period (sec.)	Reauthentication	Reauth Period (sec.)
✎	1	Disabled	60	Disabled	3600
✎	2	Disabled	60	Disabled	3600
✎	3	Disabled	60	Disabled	3600
✎	4	Disabled	60	Disabled	3600
✎	5	Disabled	60	Disabled	3600
✎	6	Disabled	60	Disabled	3600
✎	7	Disabled	60	Disabled	3600
✎	8	Disabled	60	Disabled	3600

1 - 24 of 24

UI Setting	Description
<b>Port</b>	Shows the port number the entry is for.
<b>MAB</b>	Shows whether MAC Authentication Bypass is enabled for the port.
<b>Quiet Period</b>	Show the amount of time in seconds the device will remain in a quiet state following a failed authentication exchange with a client through the port.
<b>Reauthentication</b>	Shows whether IEEE 802.1X reauthentication is enabled for the port.
<b>Reauthentication Period</b>	Shows the amount of time in seconds to wait in between reauthentication attempts for the port.

## MAC Authentication Bypass - Edit Port Settings

**Menu Path:** Security > Network Security > MAC Authentication Bypass - General

Clicking the **Edit** (✎) icon for a port on the **Security > Network Security > MAC Authentication Bypass - General** page will open this dialog box. This dialog lets you edit the MAC Authentication Bypass settings for the port.

Click **APPLY** to save your changes.

### Edit Port 1 Settings

MAC Authentication Bypass \*

Disabled ▾

---

Quiet Period \*

60

5 - 300 sec.

Reauthentication \*      Reauth Period \*

Disabled ▾      3600

60 - 65535 sec.

Copy configurations to ports ▾ ⓘ

CANCEL    APPLY

UI Setting	Description	Valid Range	Default Value
<b>MAC Authentication Bypass</b>	Enable or disable MAC Authentication Bypass for the port.	Enabled / Disabled	Disabled
<b>Quiet Period</b>	Specify the amount of time in seconds the device will remain in a quiet state following a failed authentication exchange with a client through the port.	5 to 300	60 sec.
<b>Reauthentication</b>	Enable or disable IEEE 802.1X reauthentication for the port.	Enabled / Disabled	Disabled
<b>Reauthentication Period</b>	Specify the amount of time in seconds to wait in between reauthentication attempts for the port.	60 to 65535	3600 sec.
<b>Copy configurations to ports</b>	Select the ports you want to copy this configuration to.	Drop-down list of ports	N/A

## MAC Authentication Bypass - RADIUS

### Menu Path: [Security](#) > [Network Security](#) > [MAC Authentication Bypass - RADIUS](#)

This page lets you configure the RADIUS settings for MAC authentication bypass.

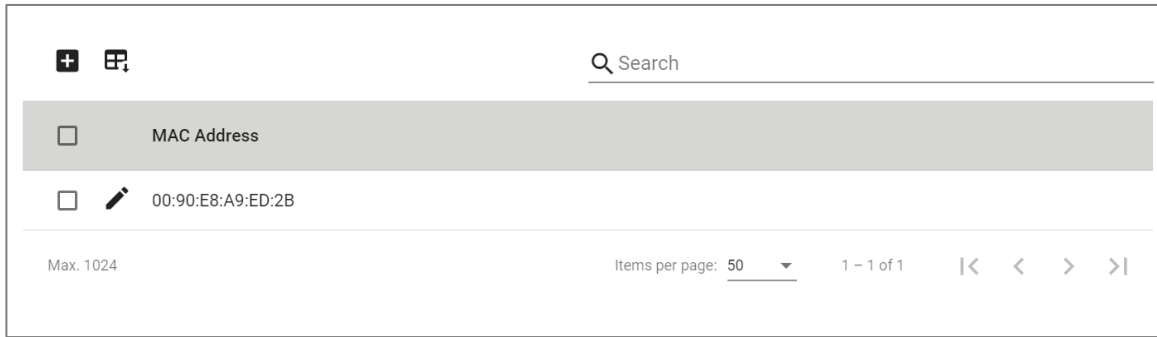
#### Note

As of MX-NOS v5.0, enabling MAC Authentication Bypass allows VLAN assignment through a RADIUS server, but the VLAN must already exist.

#### Note

802.1X and MAC authentication bypass share the same RADIUS server settings; changes made here will also affect the other feature.





**UI Setting**      **Description**

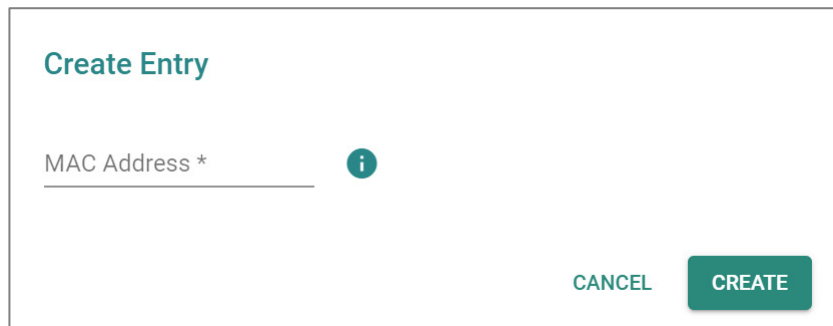
**MAC Address**      Shows the MAC address used for MAC authentication bypass.

**MAC Authentication Bypass - Local Database - Create Entry**

**Menu Path: Security > Network Security > MAC Authentication Bypass - Local Database**

Clicking the **Add (+)** icon on the **Security > Network Security > MAC Authentication Bypass - Local Database** page will open this dialog box. This dialog lets you create a new MAC authentication bypass entry.

Click **CREATE** to save your changes and add the new entry.



UI Setting	Description	Valid Range	Default Value
<b>MAC Address</b>	Specify the MAC address to use for MAC authentication bypass.	Valid unicast MAC address	N/A

## Port Security

**Menu Path:** Security > Network Security > Port Security

This page lets you enable and configure a port security mode for your device.

This page includes these tabs:

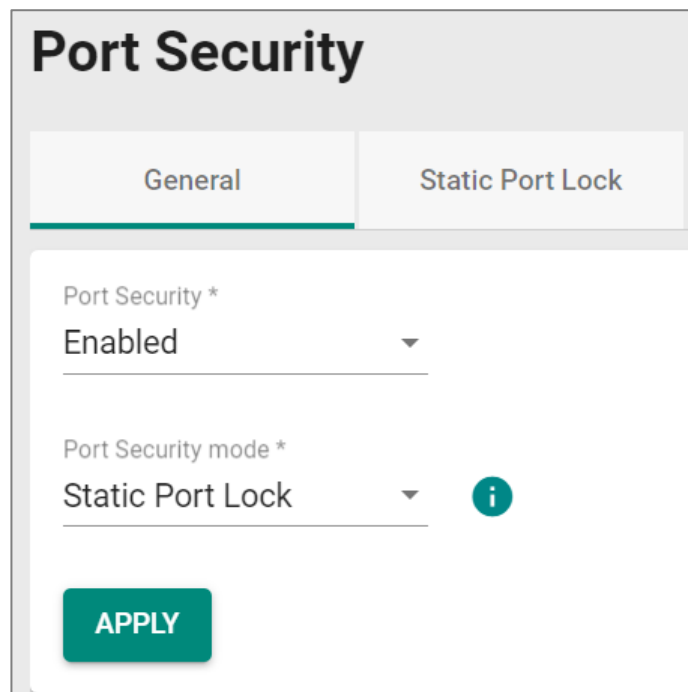
- General
- Static Port Lock (if **Static Port Lock** is selected for **Port Security Mode**)
- MAC Sticky (if **MAC Sticky** is selected for **Port Security Mode**)

### Port Security - General

**Menu Path:** Security > Network Security > Port Security - General

This page lets you enable port security and select a port security mode.

### Port Security Settings



The screenshot shows the 'Port Security' configuration page. At the top, there are two tabs: 'General' (selected) and 'Static Port Lock'. Below the tabs, there are two dropdown menus. The first is labeled 'Port Security \*' and is set to 'Enabled'. The second is labeled 'Port Security mode \*' and is set to 'Static Port Lock'. There is an information icon (i) next to the 'Static Port Lock' option. At the bottom left, there is a green 'APPLY' button.

UI Setting	Description	Valid Range	Default Value
<b>Port Security</b>	Enable or disable port security.	Enabled / Disabled	Enabled
<b>Port Security Mode</b>	Select a port security mode. <div style="background-color: #fff9c4; padding: 5px; margin-top: 10px;"> <p><b>⚠ Warning</b></p> <p>When changing the port security mode, all configured port security entries in the <b>Static Port Lock/MAC Sticky</b> tab will be deleted.</p> </div>	Static Port Lock / MAC Sticky	Static Port Lock

### Port Security List - Static Port Lock





If **Port Security Mode** is set to **Static Port Lock**, the following table will appear.

↻				🔍 Search
	Port	Static Port Lock	Manually Configured Address	
✎	1/1	Disabled	0	
✎	1/2	Enabled	1	
✎	1/3	Disabled	0	

UI Setting	Description
<b>Port</b>	Shows the port number the entry is for.
<b>Static Port Lock</b>	Shows whether static port lock is enabled for the port.
<b>Manually Configured Address</b>	Shows the number of MAC addresses manually configured for the port.

### Port Security List - MAC Sticky


If **Port Security Mode** is set to **MAC Sticky**, the following table will appear.

Port	MAC Sticky	Address Limit	Secure Action	Current Address	Manually Configured Address	Violation
 1/1	Disabled	1	Packet Drop	0	0	No
 1/2	Enabled	20	Packet Drop	1	1	No
 1/3	Disabled	1	Packet Drop	0	0	No
 1/4	Disabled	1	Packet Drop	0	0	No

UI Setting	Description
<b>Port</b>	Shows the port number the entry is for.
<b>MAC Sticky</b>	Shows whether MAC Sticky mode is enabled for the port.
<b>Address Limit</b>	Shows the maximum number of MAC addresses to learn for the port.
<b>Secure Action</b>	Shows the action the device will take when the number of MAC addresses exceeds the address limit.
<b>Current Address</b>	Shows the current number of MAC addresses learned for the port.
<b>Manually Configured Address</b>	Shows the number of manually configured MAC addresses for the port.
<b>Violation</b>	Shows whether there have been any violations for the port.

## Port Security - Edit Port Settings

### Menu Path: Security > Network Security > Port Security - General

Clicking the **Edit** () icon for a port on the **Security > Network Security > Port Security - General** page will open this dialog box. This dialog lets you configure port security settings for the port.

Click **APPLY** to save your changes.

If **Port Security Mode** is set to **Static Port Lock**, the following dialog will appear when editing port security settings.



### Edit Port 1 Settings

Static Port Lock \*

Disabled ▼

CANCEL APPLY

UI Setting	Description	Valid Range	Default Value
<b>Static Port Lock</b>	Enable or disable Static Port Lock for the port.	Enabled / Disabled	Disabled

If **Port Security Mode** is set to **MAC Sticky**, the following dialog will appear when editing port security settings.

### Edit Port 1 Settings

MAC Sticky \*

Disabled ▼

Address Limit \*

1 ⓘ


1 - 1001

Secure Action \*

Packet Drop ▼

CANCEL APPLY

UI Setting	Description	Valid Range	Default Value
<b>MAC Sticky</b>	Enable or disable MAC Sticky for the port.	Enabled / Disabled	Disabled

UI Setting	Description	Valid Range	Default Value
<b>Address Limit</b>	Specify the maximum number of the learned and configured MAC addresses allowed for the port.  <div style="background-color: #f0f0f0; padding: 5px;"> <p> <b>Note</b> Changing the address limit will clear all currently configured MAC addresses for the port.</p> </div>	1 to 1001	1
<b>Secure Action</b>	Specify the action to take when a violation occurs. <ul style="list-style-type: none"> <li>• <b>Port Shutdown:</b> The port will be shut down.</li> <li>• <b>Packet Drop:</b> Packets for the additional MAC addresses will be dropped.</li> </ul>	Port Shutdown / Packet Drop	Packet Drop

### About Static Port Lock

Static Port Lock provides port-based security by letting you specify which device MAC addresses are allowed to access the network through a specific port. Packets sent from unknown devices or from configured devices with mismatching ports will be dropped. In other words, only packets from devices with allowed MAC addresses can be sent to the specific port, helping secure network data transmissions.

### Static Port Lock

**Menu Path:** [Security](#) > [Network Security](#) > [Port Security - Static Port Lock](#)

This page lets you configure Static Port Lock.

 **Note**

This tab will only appear when Port Security Mode is set to Static Port Lock.

### 🔔 Limitations

You can create up to 1024 static port lock entries.

## Static Port Lock - Port Security Info

# Port Security

General    **Static Port Lock**

### Port Security Info

Port Security mode	Total Trust Hosts	The max. number of addresses in the system
Static Port Lock	0	1024

UI Setting	Description
<b>Port Security mode</b>	Shows the port security mode being used.
<b>Total Trust Hosts</b>	Shows the number of trusted hosts allowed to access the network.
<b>The max. number of address in the system</b>	Show the maximum number of MAC addresses allowed to be learned or specified for port security.


## Static Port Lock - Port List

🔍 Search

<input type="checkbox"/>	Port	VLAN ID	MAC Address	Type	Effective
<input type="checkbox"/>	1/2	1	00:B0:D0:63:C2:26	Lock Configured	Yes


Max. 1024      Items per page: 50      1 - 1 of 1

UI Setting	Description
<b>Port</b>	Shows the port number the entry is for.

UI Setting	Description
<b>VLAN ID</b>	Show the VLAN applied to the port.
<b>MAC Address</b>	Show the MAC address of the device which is used as a reliable source for network access.
<b>Type</b>	Shows how the entry was created.
<b>Effective</b>	Shows whether the entry is effective.
	<p> <b>Note</b></p> <p>If an entry is not effective, it may have an invalid interface set for it.</p>

### Static Port Lock - Add Entry Settings

**Menu Path:** [Security](#) > [Network Security](#) > [Port Security - Static Port Lock](#)

Clicking the **Add** () icon on the **Security > Network Security > Port Security - Static Port Lock** page will open this dialog box. This dialog lets you configure static port lock settings for a port.

Click **CREATE** to save your changes and add the new account.

### Edit Entry Settings

Port \* ▼

---

VLAN ID \*

---

MAC Address \* i

---

CANCEL
APPLY

UI Setting	Description	Valid Range	Default Value
<b>Port</b>	Select the port to add an entry for.	Drop-down list of ports	N/A
<b>VLAN ID</b>	Specify the VLAN ID to use with the port.	Valid VLAN ID	N/A
<b>MAC Address</b>	Specify the MAC address of the device that will be used as the reliable source for network access.	Valid MAC address	N/A

## About MAC Sticky

MAC Sticky is a function that allows you to configure the maximum number of MAC addresses that a port can "learn." You can also configure what action should be taken when a new MAC address tries to access a port after the maximum number of MAC addresses have already been learned.

## How MAC Sticky Works

In MAC Sticky mode, you can set a proper limit number and then configure trusted devices manually, or let the device configure trusted devices automatically. Aside from dropping packets as a response to any violations, you can also configure ports to enter "port shutdown" and achieve a strict security guarantee. When a violation is registered on a port, the port will shut down and an administrator will receive a notification to perform a check.

## MAC Sticky

### Menu Path: [Security](#) > [Network Security](#) > [Port Security - MAC Sticky](#)

This page lets you configure MAC Sticky.

#### Note

This tab will only appear when Port Security Mode is set to MAC Sticky.

### 🔔 Limitations

You can create up to 1024 MAC Sticky entries.

## MAC Sticky - Port Security Info

### Port Security

General    **MAC Sticky**

#### Port Security Info

Port Security mode	Total Trust Hosts	The max. number of addresses in the system
MAC Sticky	0	1024

UI Setting	Description
<b>Port Security mode</b>	Shows the port security mode being used.
<b>Total Trust Hosts</b>	Shows the number of trusted hosts allowed to access the network.
<b>The max. number of address in the system</b>	Show the maximum number of MAC addresses allowed to be learned or specified for port security.


## MAC Sticky - Port List

⊕ ↻ 🗪    🔍 Search

<input type="checkbox"/>	Port	VLAN ID	MAC Address	Type	Effective
<input type="checkbox"/>	1/2	1	00:B0:D0:63:C2:26	Sticky Configured	Yes


Max. 1024    Items per page: 50    1 - 1 of 1

UI Setting	Description
<b>Port</b>	Shows the port number the entry is for.

UI Setting	Description
<b>VLAN ID</b>	Show the VLAN applied to the port.
<b>MAC Address</b>	Show the MAC address of the device which is used as a reliable source for network access.
<b>Type</b>	Shows how the entry was created.
<b>Effective</b>	Shows whether the entry is effective.
	<div style="background-color: #f0f0f0; padding: 5px;"> <p> <b>Note</b></p> <p>If an entry is not effective, it may have an invalid interface set for it.</p> </div>

## MAC Sticky - Create Entry Settings

**Menu Path:** Security > Network Security > Port Security - MAC Sticky

Clicking the **Add** () icon on the **Security > Network Security > Port Security - MAC Sticky** page will open this dialog box. This dialog lets you configure MAC Sticky settings for a port.

Click **CREATE** to save your changes and add the new account.

### Edit Entry Settings

Port \* ▼

---

VLAN ID \*

---

MAC Address \* i

---

CANCEL APPLY

UI Setting	Description	Valid Range	Default Value
<b>Port</b>	Select the port to add an entry for.	Drop-down list of ports	N/A
<b>VLAN ID</b>	Specify the VLAN ID to use with the port.	Valid VLAN ID	N/A
<b>MAC Address</b>	Specify the MAC address of the device that will be used as the reliable source for network access.	Valid MAC address	N/A

## About Traffic Storm Control

A traffic storm can happen when packets flood the network and cause excessive traffic, slowing down network performance. To counter this, Traffic Storm Control provides an efficient design to prevent the network from flooding caused by a broadcast, multicast, or unicast traffic storm on a physical network layer. Traffic Storm Control can handle packets from both ingress and egress data.








### Traffic Storm Control

**Menu Path:** [Security](#) > [Network Security](#) > [Traffic Storm Control](#)

This page lets you configure traffic storm control for each port.



## Traffic Storm Control

	Port	Broadcast	Multicast	DLF	Threshold (fps)
	1	Enabled	Disabled	Disabled	12700
	2	Enabled	Disabled	Disabled	12700
	3	Enabled	Disabled	Disabled	12700
	4	Enabled	Disabled	Disabled	12700
	5	Enabled	Disabled	Disabled	12700
	6	Enabled	Disabled	Disabled	12700
	7	Enabled	Disabled	Disabled	12700

UI Setting	Description
<b>Port</b>	Shows the port number the entry is for.
<b>Broadcast</b>	Shows whether traffic storm control is enabled for broadcast packets for the port.
<b>Multicast</b>	Shows whether traffic storm control is enabled for multicast packets for the port.
<b>DLF</b>	Shows whether traffic storm control is enabled for DLF for the port.
<b>Threshold</b>	Shows the traffic storm threshold value in fps for the port.

## Traffic Storm Control - Edit Port Settings

**Menu Path:** Security > Network Security > Traffic Storm Control

Clicking the **Edit** (✎) icon for a port on the **Security > Network Security > Traffic Storm Control** page will open this dialog box. This dialog lets you configure traffic storm control for the port.

Click **APPLY** to save your changes.

### Edit Port 1 Settings

Broadcast \*  
Enabled ▼

Multicast \*  
Disabled ▼

DLF \*  
Disabled ▼

Threshold \*  
12700 ⓘ  
625 - 148810 fps

Copy configurations to ports ▼ ⓘ

CANCEL APPLY

UI Setting	Description	Valid Range	Default Value
<b>Broadcast</b>	Enable or disable traffic storm control for broadcast packets for the port.	Enabled / Disabled	Disabled

UI Setting	Description	Valid Range	Default Value
<b>Multicast</b>	Enable or disable traffic storm control for multicast packets for the port.	Enabled / Disabled	Disabled
<b>DLF</b>	Enable or disable traffic storm control for DLF packets for the port.	Enabled / Disabled	Disabled
<b>Threshold</b>	Specify the threshold in frames per second to reach before detecting a traffic storm for the port.	625 to 14881000	12700 fps
<b>Copy configurations to ports</b>	Select the ports you want to copy this configuration to.	Drop-down list of ports	N/A

## About Access Control Lists

Access Control Lists (ACLs) help you control network traffic based on specific criteria.

Here's an overview of some different kinds of ACLs:

- **Security:** ACLs provide a means to control access to network resources based on specific criteria such as source or destination IP addresses, MAC addresses, protocols, or port numbers. By implementing ACLs, you can enforce security policies and restrict unauthorized access to sensitive resources.
- **Traffic Management:** ACLs allow you to manage network traffic by selectively permitting or denying certain types of traffic. This helps optimize network performance by prioritizing critical traffic and controlling bandwidth usage.
- **Compliance:** In many industries, organizations are required to comply with security regulations and standards that mandate access control measures. By enabling ACLs, you can implement and demonstrate compliance with these requirements and mitigate security risks.
- **Protection Against Attacks:** ACLs can help protect networks against various types of attacks by blocking malicious traffic before it reaches its intended destination.
- **Preventing Unauthorized Access:** By implementing ACLs, you can prevent unauthorized users or devices from accessing network resources, reducing the risk of data breaches and unauthorized activities.

Overall, enabling ACLs enhances network security, improves traffic management, helps ensure compliance with regulations, and protects against various threats and attacks.

## Access Control Lists In Depth

In an Ethernet switch, Access Control Lists (ACLs) work by examining incoming or outgoing packets and making decisions based on predefined rules. Each access list is a filter. When a packet enters into or exits from a switch, ACL will compare the packet to the rules in the access lists, starting from the first rule. If a packet is rejected or accepted by the first rule, the switch will drop or pass this packet directly without checking the rest of the lower-priority rules.

Here's how it typically works:

1. **Packet Inspection:** When a packet arrives at a switch port, the switch inspects the packet headers, including source and destination MAC addresses, IP addresses, and port numbers.
2. **ACL Lookup:** The switch compares the packet's header information against the ACL rules configured on the switch. These rules define which types of traffic are allowed or denied based on specific criteria such as MAC addresses, IP addresses, protocols, or port numbers.
3. **Decision Making:** Based on the ACL rules, the switch decides whether to permit or deny the packet. If the packet matches an ACL rule that permits the traffic, it is forwarded according to the switch's normal forwarding behavior. If the packet matches an ACL rule that denies the traffic, it is either dropped or forwarded to a specified destination, depending on the ACL configuration.
4. **Logging and Statistics:** Some switches may also provide logging and statistical features for ACLs, allowing administrators to monitor and analyze network traffic and ACL rule matches.

Overall, ACLs in Ethernet switches provide a mechanism for controlling access to network resources based on specific criteria, helping to enforce security policies and manage network traffic.

## Access Control List

**Menu Path:** Security > Network Security > Access Control List

This page lets you configure the access control list and its related settings.

This page includes these tabs:

- Settings
- Status

### Access Control List - Settings


**Menu Path:** Security > Network Security > Access Control List - Settings


This page lets you configure your device's access control lists.

#### Limitations

You can create up to 32 access lists.

### Access Control List

Access Control List			
	<input type="text" value="Search"/>		
<input type="checkbox"/>	Index	Name	
<input type="checkbox"/>	MAC-1	Test 2	
<input type="checkbox"/>	IP-1	Test 1	

Max. 32 Items per page: 5  1 - 2 of 2 

UI Setting	Description
<b>Index</b>	Shows the access list type and its index value.
<b>Name</b>	Shows the name of the access list.


## Create an Access List


**Menu Path:** Security > Network Security > Access Control List - Settings

Clicking the **Add (+)** icon on the **Security > Network Security > Access Control List - Settings** page will open this dialog box. This dialog lets you create an access list.

Click **CREATE** to save your changes and add the new list.


### Create an Access List

Access List Type \* 

Index \* 

Name 0 / 127

[CANCEL](#) [CREATE](#)

UI Setting	Description	Valid Range	Default Value
<b>Access List Type</b>	Specify the access list type to determine how it should control access.	IP-based / MAC-based	N/A
<b>Index</b>	Specify an index value for the access list. <div style="background-color: #f0f0f0; padding: 5px; margin-top: 10px;"><p> <b>Note</b></p><p>Priority is determined by two factors: index value and address type.</p><p>Lower index values indicate higher priority. In cases where entries share the same index, MAC addresses take precedence over IP addresses.</p></div>	Drop-down list of index values	N/A
<b>Name</b>	Specify a name for the access list.	0 to 127 characters	N/A

## ACL Table Settings

You can switch between ACL tables by using the drop-down menu.

**ACL Table of IP-1** ▼

Active Interface Type \*

Port-based ▼

---

Active Ingress Ports ▼ ⓘ

---

Active Egress Ports ▼ ⓘ

---

**APPLY**

UI Setting	Description	Valid Range	Default Value
<b>Active Interface Type</b>	Specify the active interface type.	Port-based / VLAN-based	Port-based
<b>Active Ingress Ports</b>	Specify the active ingress ports.	Drop-down list of ports	N/A
<b>Active Egress Ports</b>	Specify the active egress ports.	Drop-down list of ports	N/A

### ACL Rule List (IP-based)

If the currently displayed ACL table is **IP-based**, the following table will appear.

		Search							
Index	ACL Rule	Rule Type	Protocol	Source	Destination	DSCP	Optional Parameter	Action	
1	Enabled	Permit	IGMP	196.255.1.25/ 255.255.255.255	196.255.1.45/ 255.255.255.255	30	IGMP Type: 23	Redirect to port 2 Remark DSCP to 2	

1 - 1 of 1

UI Setting	Description
<b>Index</b>	Shows the index number for the ACL rule.
<b>ACL Rule</b>	Shows whether the ACL rule is enabled.
<b>Rule Type</b>	Shows the rule type.
<b>Protocol</b>	Show the protocol used for the ACL rule.

UI Setting	Description
<b>Source</b>	Shows the source IP address with subnet mask for the ACL rule.
<b>Destination</b>	Shows the destination IP address with subnet mask for the ACL rule.
<b>DSCP</b>	Shows the DSCP value used to prioritize packets for the ACL rule.
<b>Optional Parameter</b>	Show the relevant parameters for the selected protocol.
<b>Action</b>	Show whether the redirect action or DSCP remark are enabled. If enabled, their respective configuration settings will be shown.

### ACL Rule List (MAC-based)

If the currently displayed ACL table is **MAC-based**, the following table will appear.

Index	ACL Rule	Rule Type	EtherType	Source	Destination	VLAN ID	CoS	Action
1	Enabled	Permit	Any	Any	Any	Any	Any	None

UI Setting	Description
<b>Index</b>	Shows the index number for the ACL rule.
<b>ACL Rule</b>	Shows whether the ACL rule is enabled.
<b>Rule Type</b>	Shows the rule type.
<b>EtherType</b>	Shows the EtherType for the ACL rule.
<b>Source</b>	Shows the source MAC address with mask for the ACL rule.
<b>Destination</b>	Shows the destination MAC address with mask for the ACL rule.
<b>VLAN ID</b>	Shows the VLAN ID for the ACL rule.
<b>CoS</b>	Shows the CoS value used to prioritize packets for the ACL rule.
<b>Optional Parameter</b>	Shows the relevant parameters for the selected EtherType.



UI Setting	Description
<b>Action</b>	Shows whether the redirect action or CoS remark are enabled for the ACL rule. If enabled, their respective configuration settings will be shown.

## ACL Rule List - Create Rule

### Menu Path: Security > Network Security > Access Control List - Settings

Clicking the **Add (+)** icon on the **Security > Network Security > Access Control List - Settings** page will open this dialog box. This dialog lets you create a rule for the displayed ACL table.

Click **CREATE** to save your changes and add the new rule.

If the currently displayed ACL table is **IP-based**, the following table will appear.

**Create Rule Index 1 for IP-1**

Rule Index 1 \*  
Enabled ▾

Rule Type \*  
Permit ▾

Protocol  
Any ▾

Source IP Address  
Any

Source IP Mask ▾

Destination IP Address  
Any

Destination IP Mask ▾

DSCP  
Any

0 - 63

**Action**  
Redirect \*  
Disabled ▾

DSCP Remark  
Disabled

0 - 63

CANCEL **CREATE**

UI Setting	Description	Valid Range	Default Value
<b>Rule Index</b>	Enable or disable the rule.	Enabled / Disabled	Enabled

UI Setting	Description	Valid Range	Default Value
<b>Rule Type</b>	Specify the rule type.	Permit / Deny	N/A
<b>Protocol</b>	Specify the protocol for the ACL rule.	TCP / UDP / ICMP / IGMP / OSPF / User-defined	Any
<b>Source IP Address</b>	Specify the source IP address.	Valid IP address	Any
<b>Source IP Mask</b>	Specify the source IP subnet mask.	Drop-down list of subnet masks	N/A
<b>Destination IP Address</b>	Specify the destination IP address.	Valid IP address	Any
<b>Destination IP Mask</b>	Specify the destination IP subnet mask.	Drop-down list of subnet masks	N/A
<b>DSCP</b>	Specify a DSCP value to prioritize packets for the ACL rule.	0 to 63	Any
<b>Action - Redirect (If Rule Type is Permit)</b>	Enable or disable redirects.	Enabled / Disabled	Disabled
<b>Action - DSCP Remark (If Rule Type is Permit)</b>	Enable adding a DSCP remark by specifying a DSCP Remark value. To disable it, leave this blank.	0 to 63	Disabled

If the displayed ACL table is **MAC-based**, the following dialog will appear.

### Create Rule Index 2 for MAC-1

Rule Index 2 \*

Enabled ▾

---

Rule Type \*

▾

---

EtherType

Any ▾

---

Source MAC Address

Any \_\_\_\_\_ Source MAC Mask ▾

---

Destination MAC Address

Any \_\_\_\_\_ Destination MAC Ma... ▾

---

VLAN ID

Any \_\_\_\_\_

1 - 4094

CoS

Any \_\_\_\_\_

0 - 7

CANCEL CREATE

UI Setting	Description	Valid Range	Default Value
<b>Rule Index</b>	Enable or disable the rule.	Enabled / Disabled	Enabled
<b>Rule Type</b>	Specify the rule type.	Permit / Deny	N/A
<b>EtherType</b>	Specify the EtherType for the ACL rule.	GOOSE / SMV / User-defined	Any
<b>Source MAC Address</b>	Specify a source MAC address.	Valid MAC address	Any
<b>Source MAC Mask</b>	Select a source MAC mask.	Drop-down list of MAC masks	N/A
<b>Destination MAC Address</b>	Specify a destination MAC address.	Valid MAC address	Any
<b>Destination MAC Mask</b>	Specify a destination MAC mask.	Drop-down list of MAC masks	N/A
<b>VLAN ID</b>	Specify the VLAN ID for the ACL rule.	1 to 4094	Any

UI Setting	Description	Valid Range	Default Value
<b>CoS</b>	Specify a CoS value to prioritize packets for the ACL rule.	0 to 7	Any
<b>Action - Redirect (If Rule Type is Permit)</b>	Enable or disable redirects.	Enabled / Disabled	Disabled
<b>Action - CoS Remark (If Rule Type is Permit)</b>	Enable adding a CoS remark by specifying a CoS Remark value. To disable it, leave this blank.	0 to 7	Disabled

## Access Control List - Status

**Menu Path: Security > Network Security > Access Control List - Status**

This page lets you view ACL status information for your device.

## ACL Summary

ACL Summary

Number of activated ACLs (Max. 16)  
1

Access Control List

Search

Index	Name	Activated	Direction
MAC-1	Test 2	Activated	Both
IP-1	test	Deactivated	--

Items per page: 5 | 1 - 2 of 2

UI Setting	Description
<b>Number of activated ACLs (Max. 16)</b>	Shows the number of activated ACLs.

## Access Control List - Status

**ACL Summary**

Number of activated ACLs (Max. 16)  
1

**Access Control List**

Search

Index	Name	Activated	Direction
MAC-1	Test 2	Activated	Both
IP-1	test	Deactivated	---

Items per page: 5 | 1 - 2 of 2 | < > >>

UI Setting	Description
<b>Index</b>	Shows the ACL type and its index value.
<b>Name</b>	Shows the name of the ACL.
<b>Activated</b>	Shows whether the ACL is enabled.
<b>Direction</b>	Shows the direction of the ACL.

## ACL Table Status - IP-index

If the selected ACL uses **IP-index**, the following table will appear.

**ACL Table of IP-1**

Name  
test

Active Ingress Ports  
---

Active Egress Ports  
---

Search

Index	ACL Rule	Rule Type	Protocol	Source	Destination	DSCP	Optional Parameter	Action	Hit Count
1	Enabled	Permit	IGMP	196.255.1.25/ 255.255.255.255	196.255.1.45/ 255.255.255.255	30	IGMP Type: 23	Redirect to port 2 Remark DSCP to 2	0

1 - 1 of 1

UI Setting	Description
<b>Name</b>	Shows the name of the access list.
<b>Active Ingress Port</b>	Shows the active ingress ports configured.

UI Setting	Description
<b>Active Egress Port</b>	Shows the active egress ports configured.
<b>Index</b>	Shows the index number for the ACL rule.
<b>ACL Rule</b>	Shows whether the ACL rule is enabled.
<b>Rule Type</b>	Shows the rule type.
<b>Protocol</b>	Shows the protocol used for the ACL rule.
<b>Source</b>	Shows the source IP address with its subnet mask.
<b>Destination</b>	Shows the destination IP address with its subnet mask.
<b>DSCP</b>	Shows the DSCP value specified to differentiate the prioritization of IP packets.
<b>Optional Parameter</b>	Shows the relevant parameters for the selected protocol.
<b>Action</b>	Shows whether the redirect action and DSCP remark are enabled. If enabled, shows their respective configuration settings.
<b>Hit Count</b>	Shows the hit count of the ACL rule.

### ACL Table Status - MAC-index

If the selected ACL uses **MAC-index**, the following table will appear.

ACL Table of MAC-1

Name: Test 2

Active Ingress Ports: 1, 3      Active Egress Ports: 4, 5

Search

Index	ACL Rule	Rule Type	EtherType	Source	Destination	VLAN ID	CoS	Action	Hit Count
1	Enabled	Permit	Any	Any	Any	Any	Any	None	0

1 - 1 of 1

UI Setting	Description
<b>Name</b>	Shows the name of the access list.

UI Setting	Description
<b>Active Ingress Port</b>	Shows the active ingress ports configured.
<b>Active Egress Port</b>	Shows the active egress ports configured.
<b>Index</b>	Shows the index number for the ACL rule.
<b>ACL Rule</b>	Shows whether the ACL rule is enabled.
<b>Rule Type</b>	Shows the rule type.
<b>EtherType</b>	Shows the EtherType used for the ACL rule.
<b>Source</b>	Shows the source MAC address with its mask.
<b>Destination</b>	Shows the destination MAC address with its mask.
<b>VLAN ID</b>	Shows the VLAN ID.
<b>CoS</b>	Shows the CoS value specified to differentiate the prioritization of packets.
<b>Optional Parameter</b>	Shows the relevant parameters for the selected EtherType.
<b>Action</b>	Shows whether the redirect action and CoS remark are enabled. If enabled, shows their respective configuration settings.
<b>Hit Count</b>	Shows the hit count of the ACL rule.

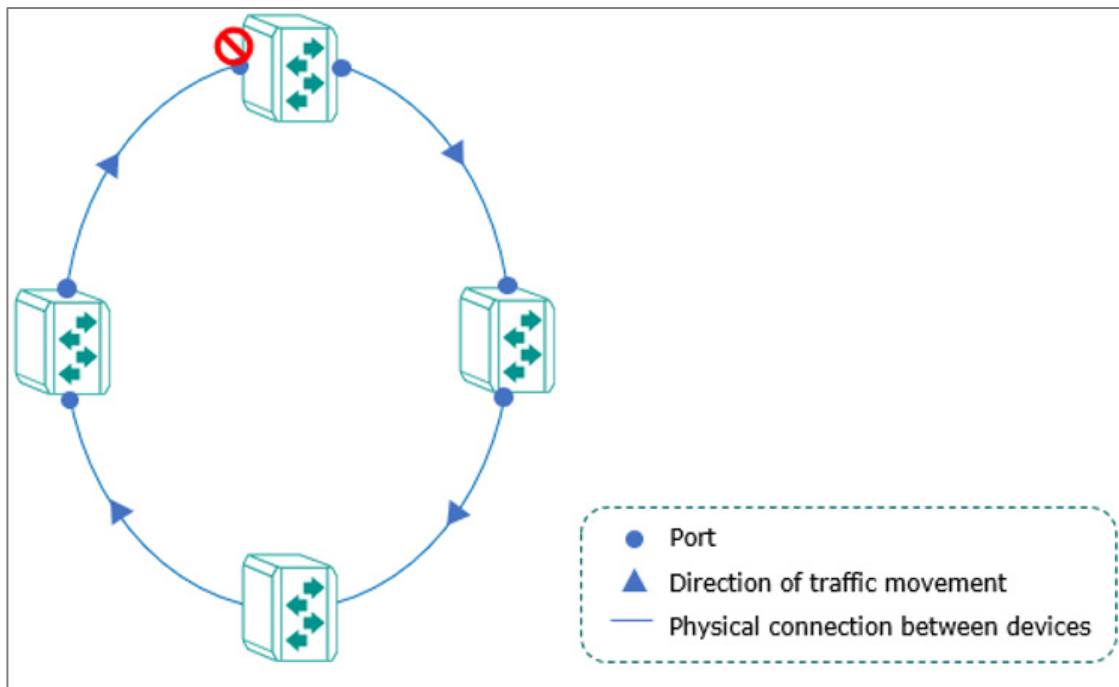
## About Network Loop Protection

Network Loop Protection helps avoid network loops by disabling ports when looping is detected in the network topology. This is designed for devices that do not support redundant protocols, when redundant protocols are not configured, or if the redundant protocol fails.

### Network Loop Protection In Depth

Network Loop Protection prevents looping by sending detection packets through the network topology to all ports. After receiving a packet, a port will check if the packet was sent by the device itself. If so, the receiving port will be disabled to prevent looping.

Network loop protection features cannot prevent ports from activating redundancy protocols—such as STP, RSTP, MSTP, Turbo Ring, Ring Coupling, Turbo Chain, Dual Homing, or Link Aggregation—from looping, as these ports do not process detection packets sent by the Network Loop Protection features.



## Network Loop Protection

**Menu Path:** [Security](#) > [Network Security](#) > [Network Loop Protection](#)

This page lets you manage network loop protection for your device.

This page includes these tabs:

- Settings
- Status

### Network Loop Protection - Settings

**Menu Path:** [Security](#) > [Network Security](#) > [Network Loop Protection - Settings](#)

This page lets you enable network loop protection settings.



## Network Loop Protection Settings

### Network Loop Protection

Settings Status

---

Network Loop Protection \*  
Disabled ▾

Detect Interval \*  
10  
1 - 30 sec.

**APPLY**

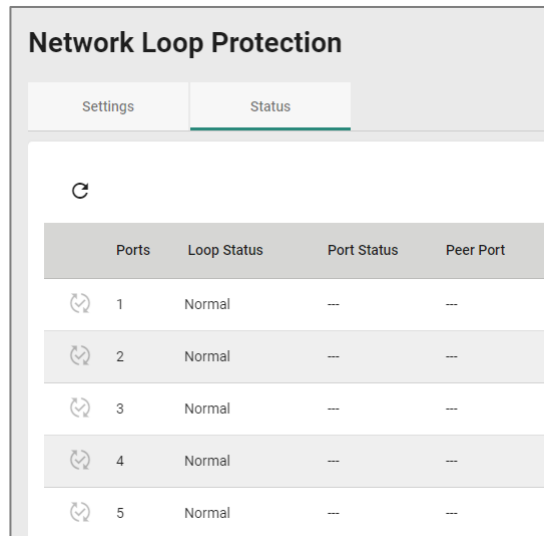
UI Setting	Description	Valid Range	Default Value
<b>Network Loop Protection</b>	Enable or disable the network loop protection.	Enabled / Disabled	Disabled
<b>Detect Interval</b>	Specify the detect interval in seconds.	1 to 30	10

## Network Loop Protection - Status

**Menu Path:** [Security](#) > [Network Security](#) > [Network Loop Protection - Status](#)

This page lets you view the status of network loop protection.

## Network Loop Protection - Port List



The screenshot shows the 'Network Loop Protection' interface with the 'Status' tab selected. It features a refresh icon and a table with the following data:

Ports	Loop Status	Port Status	Peer Port
1	Normal	--	--
2	Normal	--	--
3	Normal	--	--
4	Normal	--	--
5	Normal	--	--

UI Setting	Description
<b>Ports</b>	Shows the port number the entry is for.
<b>Loop Status</b>	Show the loop status of the port. <ul style="list-style-type: none"><li>• <b>Normal:</b> The port is not looping.</li><li>• <b>Looping:</b> The port is looping.</li></ul>
<b>Port Status</b>	Shows the port status of the specific port. <ul style="list-style-type: none"><li>• <b>Disabled:</b> The port is disabled due to a port shutdown or detected loop.</li></ul>
<b>Peer Port</b>	Shows the port where the looping frames are from when detecting a loop.

## About Binding Databases

A binding database acts as an allowlist for IP Source Guard and Dynamic ARP Inspection to help protect against unauthorized traffic.

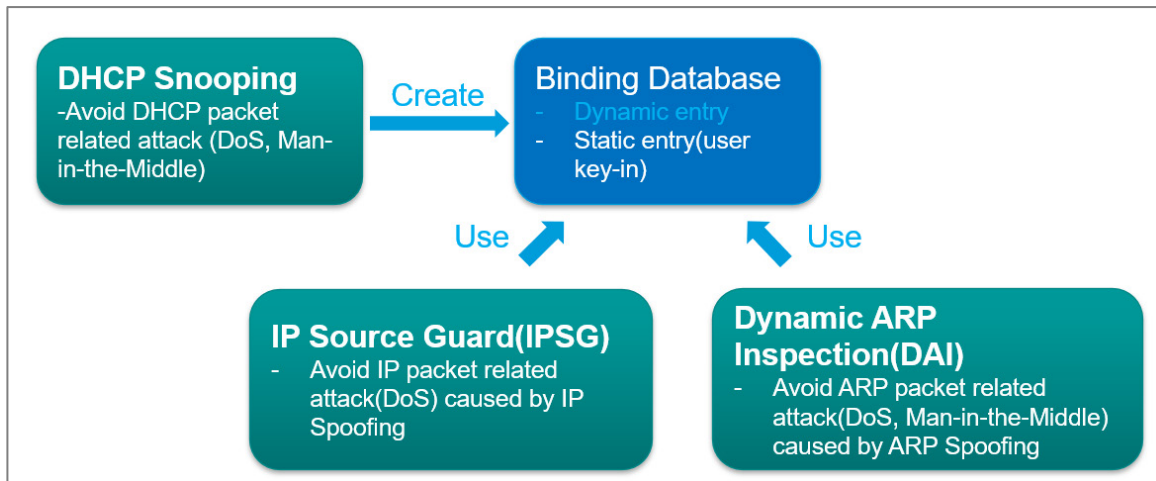
### Binding Databases In Depth

A binding database consists of dynamic entries and static entries.

- **Dynamic Entries:** Generated automatically after a DHCP client successfully obtains an IP while DHCP snooping is enabled. The entry will be released after exceeding the IP lease time or upon disabling DHCP snooping.

- **Static Entries:** User-generated/edited entry. The entry will be released only when a user deletes it.

Binding database entries consist of VLAN IDs, MAC addresses, ports, and IP addresses. This information forms an allowlist used by IP Source Guard to filter IP packets, and for Dynamic ARP Inspection to filter ARP packets. This helps prevent spoofing attacks such as man-in-the-middle and denial-of-service attacks.



## Configuring Binding Database

Binding Database is the base for IP Source Guard and Dynamic ARP Inspection, there are two ways to populate Binding Database entries, including entries automatically created after enabling DHCP Snooping or manually entries created by users.

### Before you begin:

- Determine which kind of Binding Database Entries to use: Static, or Dynamic. See above for guidelines to make this determination.

## Configuring Dynamic Binding Database Entries

To configure a Dynamic Binding Database entry:

1. Go to **Security > Network Security > DHCP Snooping**.
2. Click DHCP Snooping and then select Enable, optionally specify a VLAN ID, and then click Apply.

3. Under Port Settings, click **Edit** (✎) to configure the corresponding port binding settings.
4. Configure the following:
  - **Status**• **Copy configurations to ports**
5. Click **Apply**

**Results:** The Binding Database entries will be created upon a successful DHCP transaction on DHCP Snooping-enabled Untrusted ports. You can view the binding database entries by going to **Security > Network Security > Binding Database > Binding Status**.

### Configuring Static Binding Database Entries

To configure a Static Binding Database Entry:

1. Go to **Security > Network Security > Binding Database.> Binding Setting**.
2. Click (Add), and then specify all of the following:
  - **VLAN ID**• **MAC Address**• **Port**• **IP Address**
3. Click **Create** to add the entry to the database.

**Results:** The Binding Database entries will be created upon a successful DHCP transaction on DHCP Snooping-enabled Untrusted ports. You can view the binding database entries by going to **Security > Network Security > Binding Database > Binding Status**.

## Binding Database

**Menu Path:** [Security > Network Security > Binding Database](#)

This page lets you view and manage the binding database, which can be used for an allowlist for IP Source Guard or Dynamic ARP Inspection.

This page includes these tabs:

- Binding Settings
- Binding Status

### 🔑 Limitations

You can create up to 32 binding database entries, including dynamic and static entries. Entries will stop being generated or being user-addable when this limit is reached. More entries can only be added when existing entries are released, bringing the total number below 32.

## Binding Settings

**Menu Path: Security > Network Security > Binding Database - Binding Settings**

This page lets you manage the static entries you want to use for an allowlist.

### Binding Settings List

**Binding Database**

Binding Settings | Binding Status

+

<input type="checkbox"/>	VLAN ID	MAC Address	Port	IP Address
--------------------------	---------	-------------	------	------------

Max. 32 of Binding Status table

UI Setting	Description
<b>VLAN ID</b>	Shows the VLAN ID for the static entry.
<b>MAC Address</b>	Shows the MAC address for the static entry.
<b>Port</b>	Shows the port for the static entry.
<b>IP Address</b>	Shows the IP address for the static entry.

## Create a Binding Database Static Entry

**Menu Path:** Security > Network Security > Binding Database - Binding Settings

Clicking the **Add (+)** icon on the **Security > Network Security > Binding Database - Binding Settings** page will open this dialog box. This dialog lets you a new static entry to be an allowlist base for IP Source Guard or Dynamic ARP Inspection.

Click **CREATE** to save your changes and add the new entry.

### Create a Binding Database Static Entry

VLAN ID \*       MAC Address \*

Port \*

IP Address \*

UI Setting	Description	Valid Range	Default Value
<b>VLAN ID</b>	Specify the VLAN ID to allowlist for IP Source Guard or Dynamic ARP Inspection.	1 to 4094	N/A
<b>MAC Address</b>	Specify the MAC address to allowlist for IP Source Guard or Dynamic ARP Inspection.	Valid MAC address	N/A
<b>Port</b>	Specify the port to allowlist for IP Source Guard or Dynamic ARP Inspection.	Drop-down list of subnet masks	N/A
<b>IP Address</b>	Specify the IP address to allowlist for IP Source Guard or Dynamic ARP Inspection.	Valid IP address	N/A

## Binding Status

**Menu Path:** Security > Network Security > Binding Database - Binding Status


This page lets you view the current binding database entries of your device.

### Binding Status List

### Binding Database

Binding Settings    **Binding Status**

Dynamic binding is learning from DHCP snooping.  
The binding status will not be updated if the VLAN ID and MAC address combination of the static entry already exists.



Type	VLAN ID	MAC Address	Port	IP Address	Lease Time	Active
Max. 32						

UI Setting	Description
<b>VLAN ID</b>	Shows the VLAN ID for a successful DHCP packet transaction on an untrusted port, or the specified VLAN ID for a user-created static entry.
<b>MAC Address</b>	Shows the MAC address for a successful DHCP packet transaction on an untrusted port, or the specified MAC address for a user-created static entry.
<b>Port</b>	Shows the untrusted port for a successful DHCP packet transaction, or the specified port for a user-created static entry.
<b>IP Address</b>	Shows the IP address for a successful DHCP packet transaction on an untrusted port, or the specified IP address for a user-created static entry.
<b>Lease Time</b>	Shows the lease time for the entry to be active. The lease time is infinite for user-created static entries.
<b>Active</b>	Shows whether the entry is active for use with IP Source Guard, Dynamic ARP Inspection, or both.

## About DHCP Snooping

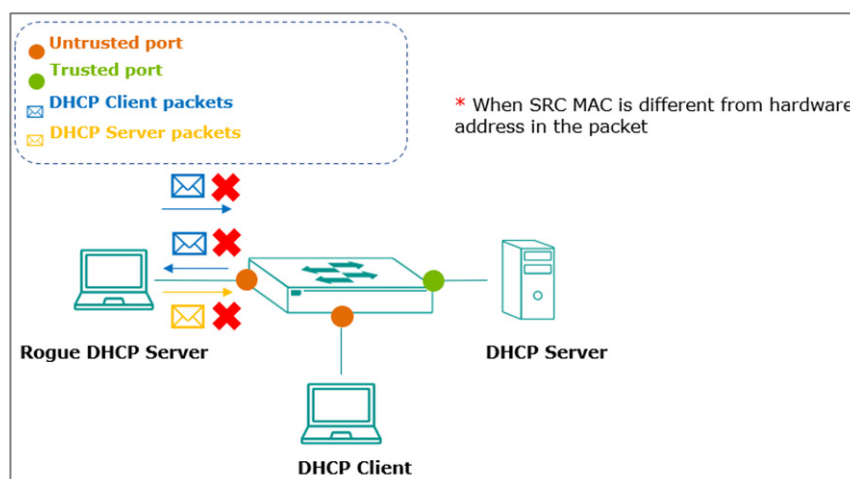
DHCP Snooping is a VLAN-specific security feature for DHCP operations. You can configure untrusted hosts and trusted DHCP servers for corresponding ports on your device, and then the feature will act like a firewall to validate DHCP messages received from untrusted sources and filter out invalid messages to exclude rogue DHCP servers and remove malicious DHCP traffic. This helps guarantee that clients obtain a legal address from the DHCP server you designate.

Enabling DHCP snooping will also set up a binding database, which will act as an allowlist for IP Source Guard and Dynamic ARP Inspection.

## DHCP Snooping In Depth

By configuring the designated ports connected to DHCP server ports as trusted ports, and ports connected to clients/hosts as untrusted ports:

- Trusted ports will allow all DHCP packets.
- Untrusted ports will handle DHCP packets as follows:
  - a. Pass ingress DHCP client packets and egress DHCP server packets to complete normal DHCP transactions.
  - b. Drop egress DHCP client packets and ingress DHCP server packets to avoid rogue DHCP server attacks.
  - c. Drop DHCP client packets with a different source MAC address and hardware address to avoid malicious DHCP client attacks.





Successful DHCP transactions with DHCP snooping enabled will create and update the binding database. The binding database contains VLAN IDs, MAC addresses, untrusted ports of DHCP clients, and IP addresses. The binding database can also be used for other security functions such as IP Source Guard and Dynamic ARP Inspection.

## DHCP Snooping





**Menu Path:** Security > Network Security > DHCP Snooping

This page lets you manage DHCP Snooping for your device.

### DHCP Snooping Settings

UI Setting	Description	Valid Range	Default Value
<b>DHCP Snooping</b>	Enable or disable DHCP snooping.	Enabled / Disabled	Disabled
<b>VLAN ID</b>	Specify the VLAN IDs to use for DHCP snooping. You can enter multiple VLAN IDs by separating them with commas or by using ranges (e.g., 2, 4-8, 10-13).	1 to 4094	N/A


## DHCP Snooping - Port Settings

Port Settings		
	Port	Status
	1	Untrusted
	2	Untrusted
	3	Untrusted
	4	Untrusted

UI Setting	Description
<b>Port</b>	Shows the port number the entry is for.
<b>Status</b>	Shows whether the port is trusted or untrusted.

## DHCP Snooping - Edit Port Settings

### Menu Path: Security > Network Security > DHCP Snooping

Clicking the **Edit** () icon for a port on the **Security > Network Security > DHCP Snooping** page will open this dialog box. This dialog lets you configure the port as trusted or untrusted for DHCP snooping.

Click **APPLY** to save your changes.

## Edit Port 1 Settings

Status \*  
Untrusted ▼

Copy configurations to ports ▼ i

CANCEL
APPLY

UI Setting	Description	Valid Range	Default Value
<b>Status</b>	Specify the port as untrusted or trusted.	Untrusted / Trusted	Untrusted
<b>Copy configurations to ports</b>	Select the ports you want to copy this configuration to.	Drop-down list of ports	N/A

## About IP Source Guard

IP Source Guard (IPSG) is an IP data packet filtering security feature that works on Layer 2 interfaces. It works together with DHCP Snooping and the Binding Database to filter IP data packets to defend against attacks such as denial-of-service (DoS) that are caused by forging/spoofing source IP addresses.

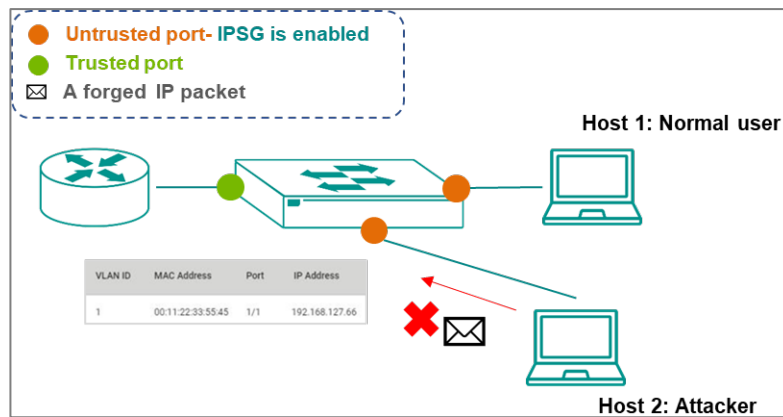
### IP Source Guard In Depth

IPSG checks all traffic to make sure its host IP address, MAC address, VLAN, and port match a valid entry in the binding database. If the host does not match a valid entry in the binding database, the traffic will not be forwarded.

**Note**

IP Source Guard (IPSG) works with DHCP snooping, so DHCP snooping must be enabled to create binding database entries before enabling IPSG

IPSG can only be used on ports specified as "untrusted" for DHCP snooping.








## IP Source Guard

**Menu Path: Security > Network Security > IP Source Guard**

This page lets you enable or disable IP Source Guard for each port.


## IP Source Guard List

IP Source Guard		
	Port	Status
	1	Disabled
	2	Disabled
	3	Disabled
	4	Disabled

UI Setting	Description
<b>Port</b>	Shows the port number the entry is for.
<b>Status</b>	Shows whether IP Source Guard is enabled for the port.
	 <b>Note</b> IP Source Guard can only be enabled on ports specified as untrusted in DHCP snooping.

### IP Source Guard - Edit Port Settings

**Menu Path:** Security > Network Security > IP Source Guard

Clicking the **Edit** () icon for a port on the **Security > Network Security > IP Source Guard** page will open this dialog box. This dialog lets you enable or disable IP Source Guard for the port.

Click **APPLY** to save your changes.

## Edit Port 1 Settings

Status \*  
Disabled ▼

Copy configurations to ports ▼ i

CANCEL
APPLY

UI Setting	Description	Valid Range	Default Value
<b>Status</b>	Enable or disable IP Source Guard for the port. When enabled, only traffic with packet headers that have a source IP and MAC address that match a valid entry in the Binding Database will be forwarded. <div style="background-color: #f0f0f0; padding: 5px; margin-top: 10px;"> <p><b>Note</b></p> <p>IP Source Guard can only be enabled on ports specified as untrusted in DHCP snooping.</p> </div>	Enabled / Disabled	Disabled
<b>Copy configurations to ports</b>	Select the ports you want to copy this configuration to.	Drop-down list of ports	N/A

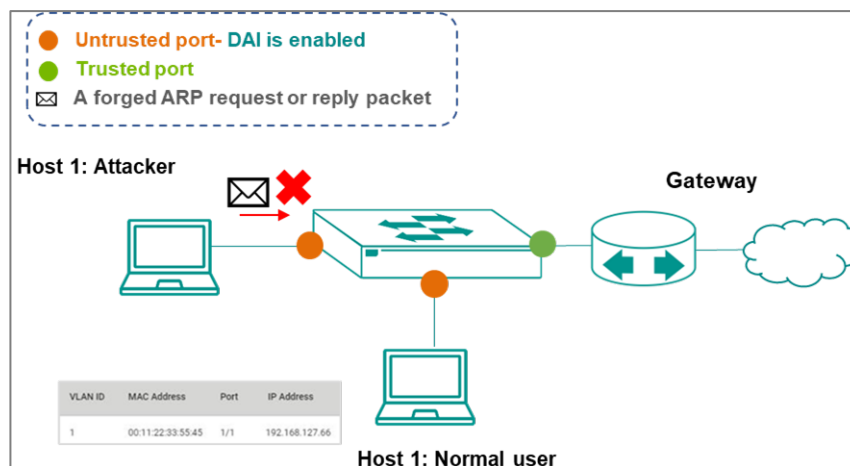
## About Dynamic ARP Inspection

Dynamic ARP Inspection (DAI) is an ARP packet filtering security feature that works on Layer 2 interfaces. It works together with DHCP snooping and the binding database to help defend against attacks such as man-in-the-middle or denial-of-service (DoS) attacks caused by ARP packet spoofing (also known as ARP poisoning or ARP cache poisoning).

## Dynamic ARP Inspection In Depth

Dynamic ARP Inspection (DAI) works with DHCP Snooping. Users must enable DHCP snooping to create Binding Database entries before enabling DAI, and DAI can only be used on ports specified as untrusted DHCP Snooping.

DAI inspects each ARP packet sent from a host attached to an untrusted port on the switch. The IP address, MAC address, VLAN, and port associated with the host are checked against entries stored in the Binding Database. If the host information does not match a valid entry in the Binding Database, the ARP packet will not be forwarded.









## Dynamic ARP Inspection

**Menu Path: Security > Network Security > Dynamic ARP Inspection**

This page lets you enable or disable Dynamic ARP Inspection for each port.

## Dynamic ARP Inspection List

Dynamic ARP Inspection		
	Port	Status
	1	Disabled
	2	Disabled
	3	Disabled
	4	Disabled
	5	Disabled

UI Setting	Description
<b>Port</b>	Shows the port number the entry is for.
<b>Status</b>	Shows whether Dynamic ARP Inspection is enabled for the port.   <b>Note</b> Dynamic ARP Inspection can only be enabled on ports specified as untrusted in DHCP snooping.



## Dynamic ARP Inspection - Edit Port Settings

**Menu Path:** Security > Network Security > Dynamic ARP Inspection

Clicking the **Edit** (✎) icon for a port on the **Security > Network Security > Dynamic ARP Inspection** page will open this dialog box. This dialog lets you enable or disable Dynamic ARP Inspection for the port.

Click **APPLY** to save your changes.

**Edit Port 2/1 Settings**

Status \*  
Disabled

Copy configurations to ports

CANCEL APPLY

UI Setting	Description	Valid Range	Default Value
<b>Status</b>	Enable or disable Dynamic ARP Inspection for the port. When enabled, ARP packets are inspected, and only ARP packets that have a source IP and MAC address that match a valid entry in the Binding Database will be forwarded.  <b>Note</b> Dynamic ARP Inspection can only be enabled on ports specified as untrusted in DHCP snooping.	Enabled / Disabled	Disabled
<b>Copy configurations to ports</b>	Select the ports you want to copy this configuration to.	Drop-down list of ports	N/A

## About MAC Security

Media Access Control Security (MAC security) is defined in IEEE802.1AE and 802.1X, specifying how to secure data communication over a Local Area Network (LAN). MAC security ensures data is securely sent and received at the MAC layer by providing data integrity checks, data origin authentication, and confidentiality.

MAC security cryptographically protects frames on a hop-by-hop basis at Layer 2 on LAN and can be enabled as in combination with other end-to-end Layer 3 security technologies such as IPsec, Secure Sockets Layer (SSL), Transport Layer Security (TLS), and Secure Shell Protocol (SSH).

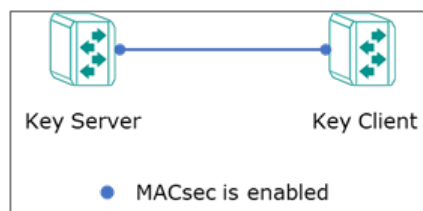
## MAC Security In-Depth

For data exchanged between devices in a LAN, MAC security ensures transmission security using cryptographic technology in the MAC layer.

MAC security involves two standards: IEEE802.1AE and 802.1X. The frame format for data encapsulation, encryption, and authentication is defined in IEEE802.1AE. MACsec Key Agreement (MKA), a key management protocol, is defined in IEEE 802.1X-2010. MKA provides agreement for MAC security policy and key generation mechanisms to extend and optimize the original 802.1X protocol.

MAC security operation starts by using a Pre-shared Key (PSK) to authenticate a peer switch. One switch is designated as the Key Server and the other switch as the Key Client. The Key Server and Key Client share the same user-specified connectivity Association Key Name (CKN) and Connectivity Association Key (CAK). The Key Server uses the CAK to generate a Secure Association Key (SAK) and distribute it to the Key Client to form a secure association. Data exchanged between the peer switches in the path will then be encrypted.

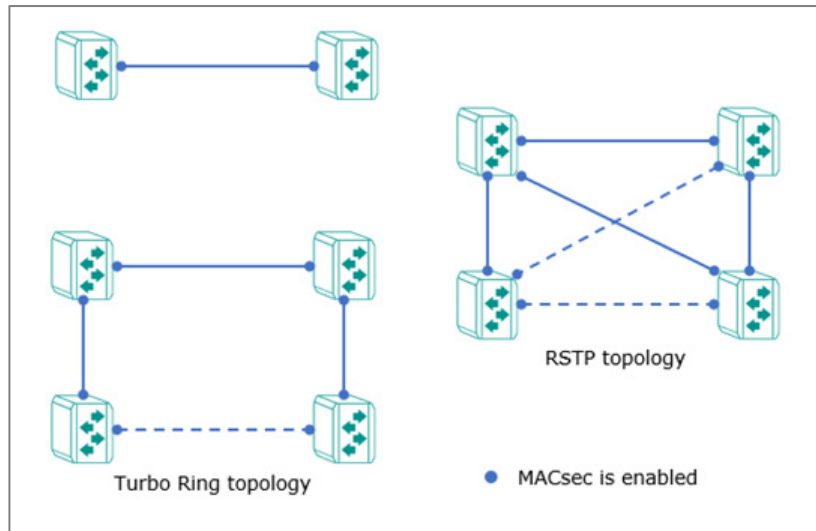
To ensure data traffic is transmitted securely, all data traffic ports must enable MAC security.



## MAC Security with Redundancy Protocols

When running MAC security with Redundancy Protocols, make sure of the following:


- For Turbo Ring topologies, all ring ports must enable MAC security.
- For RSTP topologies, all redundant ports must enable MAC security.



## Configuring MAC Security


MAC security must be configured on each relevant port and device to protect data.

To configure MAC security, do the following:

1. Sign in to the device with administrator credentials.
2. **Security > Network Security > MAC security**, and then click **Settings**.
3. To enable **MAC security**, under **MAC security** choose **Enabled** from the dropdown menu, and then click **Apply**.
4. To configure MAC security on a given port, click the corresponding  **[Edit]** and then configure all of the following:

Option	Value
<b>Status</b>	<b>Enabled</b>
<b>Participant CKN</b>	Specify a Connectivity association Key Name of 1-16 characters.

Option	Value
<b>Participant CAK</b>	Specify a Connectivity association Key of 1-16 characters.
<b>Key Server</b>	<ul style="list-style-type: none"> <li>• <b>Enabled:</b> The port is a key server.</li> <li>• <b>Disabled:</b> The port is a key client.</li> </ul>

 **Note**

- The CKN/CAK must match the connected port on the peer switch.
- One CKN and one CAK per port.
- CKNs/CAKs should not be reused on the same device.
- Valid CKN/CAK characters: a-z, A-Z, numbers 0-9, special characters @%^\*()-\_+={}[:.,~\$` , and do not permit whitespaces.
- CKNs/CAKs must be configured in pairs, and cannot be partially configured (such as configuring one, but not the other).
- Deleting a CKN/CAK may also delete its corresponding CAK/CKN.

5. Click **Apply** to save your changes.

Make sure to enable MAC security on all relevant devices and ports.

## MAC Security

**Menu Path:** [Security](#) > [Network Security](#) > [MAC Security](#)

This page lets you manage MAC security for your device.

This page includes these tabs:

- General
- MKA Status

### MAC Security - General

**Menu Path:** [Security](#) > [Network Security](#) > [MAC Security - General](#)

This section lets you configure MAC security for your device.

## MAC Security Settings











MAC security \*  
 Disabled 🔔

---

APPLY

UI Setting	Description	Valid Range	Default Value
<b>MAC Security</b>	Enable or disable MAC security (MACsec) for your device.	Enabled / Disabled	Disabled

## MAC Security Port List

	Port	Status	Participant CKN	Key Server
	1/1	Disabled	--	Disabled
	1/2	Disabled	--	Disabled
	1/3	Disabled	--	Disabled
	1/4	Disabled	--	Disabled
	2/1	Disabled	--	Disabled
	2/2	Disabled	--	Disabled
	2/3	Disabled	--	Disabled
	2/4	Disabled	--	Disabled
	2/5	Disabled	--	Disabled
	2/6	Disabled	--	Disabled

UI Setting	Description
<b>Port</b>	Shows the port this entry is for.
<b>Status</b>	Shows whether MAC security is enabled for the port.
<b>Participant CKN</b>	Shows the Connectivity association Key Name (CKN) configured for the port as the pre-shared key.
<b>Key Server</b>	Shows whether the port is a key server or a key client. <ul style="list-style-type: none"> <li>• <b>Enabled:</b> The port is a key server.</li> <li>• <b>Disabled:</b> The port is a key client.</li> </ul>

## Editing a MAC Security Port

**Menu Path:** Security > Network Security > MAC Security - General

Clicking the **Edit** (✎) icon for a port on the **Security > Network Security > MAC Security - General** page will open this dialog box. This dialog lets you edit the port's MAC security settings.



Click **APPLY** to save your changes.

### Edit Port 1/1 Settings

Status \*

Participant CKN  Participant CAK

Key Server \*

UI Setting	Description	Valid Range	Default Value
<b>Status</b>	Enable or disable MAC security for this port.	Enabled / Disabled	Disabled
<b>Participant CKN</b>	Specify the Connectivity association Key Name (CKN) to use for the port.  <div style="background-color: #f0f0f0; padding: 10px; margin-top: 10px;"> <p> <b>Note</b></p> <ul style="list-style-type: none"> <li>The CKN configured for this port should be the same as the connected port on the peer switch to enable MACsec for data exchange.</li> <li>Multiple CKNs are not allowed for a single port.</li> <li>Different CKNs on a device should be unique.</li> <li>A CKN can only contain the letters a-z, A-Z, numbers 0-9, special characters @%^*()-_+={}[:~\$` , and cannot have any spaces.</li> <li>CKNs and CAKs must be configured in pairs, and cannot be partially configured (such as configuring one, but not the other).</li> <li>Deleting a CKN may also delete its corresponding CAK.</li> </ul> </div>	1 to 16 characters	N/A
<b>Participant CAK</b>	Specify the Connectivity Association Key (CAK) to use for the port.  <div style="background-color: #f0f0f0; padding: 10px; margin-top: 10px;"> <p> <b>Note</b></p> <ul style="list-style-type: none"> <li>The CAK configured for this port should be the same as the connected port on the peer switch to enable MACsec for data exchange.</li> <li>Multiple CAKs are not allowed for a single port.</li> <li>Different CAKs on a device should be unique.</li> <li>A CAK can only contain the letters a-z, A-Z, numbers 0-9, special characters @%^*()-_+={}[:~\$` , and cannot have any spaces.</li> <li>CKNs and CAKs must be configured in pairs, and cannot be partially configured (such as configuring one, but not the other).</li> <li>Deleting a CAK may also delete its corresponding CKN.</li> </ul> </div>	1 to 16 characters	N/A

UI Setting	Description	Valid Range	Default Value
<b>Key Server</b>	<p>Enable or disable specifying the port as a key server.</p> <ul style="list-style-type: none"> <li><b>Enabled:</b> The port is a key server.</li> <li><b>Disabled:</b> The port is a key client.</li> </ul> <div style="background-color: #f0f0f0; padding: 10px; margin-top: 10px;"> <p><b>Note</b></p> <ul style="list-style-type: none"> <li>The column for the two connected switches are disabled is not allowed.</li> <li>If you enable Key Server for a port, Key Server should be disabled for the connected port of the other switch.</li> <li>If you disable Key Server for a port, Key Server should be enabled for the connected port of the other switch.</li> </ul> </div>	Enabled / Disabled	Disabled

## MAC Security - MKA Status

**Menu Path:** Security > Network Security > MAC Security - MKA Status

This page lets you view the current MAC security status for your device.

### MKA Status Port List

2024/10/29 14:44:54

Q Search

Port	Peer List Member Identifier (MI)	Peer List Message Number (MN)	Secure Channel ID (SCI)	Peer List Type
0 of 0				

UI Setting	Description
<b>Port</b>	Shows the port this entry is for.
<b>Peer List Member Identifier (MI)</b>	Shows the member identifier of the connected switch.
<b>Peer List Message Number (MN)</b>	Shows the message number received from the connected switch.



UI Setting	Description
<b>Secure Channel ID (SCI)</b>	Shows the session ID for the channel to the other switch.
<b>Peer List Type</b>	Shows the peer list type. <ul style="list-style-type: none"> <li>• <b>Potential Peer List:</b> The MI from the sender cannot be recognized by the receiver.</li> <li>• <b>Live Peer List:</b> The MI from the sender can be recognized by the receiver, and the MN from the sender is larger than the MN recorded in the receiver.</li> </ul>

## Authentication

### Menu Path: Security > Authentication

This section lets you manage the authentication features of your device.

This section includes these pages:

- Login Authentication
- RADIUS
- TACACS+

### About Login Authentication

Your device can authenticate user logins to protect against unauthorized access to your device.

### How Login Authentication Works

Your device has three different methods of authenticating user logins:

- TACACS+ (Terminal Access Controller Access-Control System Plus)
- RADIUS (Remote Authentication Dial In User Service)
- Local database

TACACS+ and RADIUS are centralized "AAA" (Authentication, Authorization, and Accounting) systems for connecting to network services. The fundamental purpose of these is to provide an efficient and secure mechanism for user account management.

You can use different combinations of these authentication methods:

1. **TACACS+, Local:** Check the TACACS+ database first. If checking the TACACS+ database fails, then check the local database.
2. **RADIUS, Local:** Check the RADIUS database first. If checking the RADIUS database fails, then check the local database.
3. **TACACS+:** Only check the TACACS+ database.
4. **RADIUS:** Only check the RADIUS database.
5. **Local:** Only check the local database.

## Login Authentication

**Menu Path:** [Security](#) > [Authentication](#) > [Login Authentication](#)

This page lets you select the login authentication protocol for your device.

### Login Authentication Settings

#### Note

The account privilege level is authorized under service type settings in RADIUS, and the privilege level is under TACACS+.

RADIUS Server

- RADIUS Service type = 6 = administrator
- RADIUS Service type = 3 = supervisor
- RADIUS Service type = all other values (1, 2, 4, 5, 7, 8, 9, 10, 11) = user

TACACS+ Server

- TACACS+ privilege level= 15 = administrator
- TACACS+ privilege level= 12 = supervisor
- TACACS+ privilege level= 1 = user

# Login Authentication

## Authentication Protocol

- Local
- RADIUS
- TACACS+
- RADIUS, Local
- TACACS+, Local

APPLY

UI Setting	Description	Valid Range	Default Value
<b>Authentication Protocol</b>	<p>Select the login authentication protocol to use for your device.</p> <ul style="list-style-type: none"> <li>• <b>Local:</b> Only the local database will be checked for login authentication.</li> <li>• <b>RADIUS:</b> Only the RADIUS database will be checked for login authentication.</li> <li>• <b>TACACS+:</b> Only the TACACS+ database will be checked for login authentication.</li> <li>• <b>RADIUS, Local:</b> The RADIUS database will be checked first for login authentication. If checking the RADIUS database fails, then the local database will be checked.</li> <li>• <b>TACACS+, Local:</b> The TACACS+ database will be checked first for login authentication. If checking the TACACS+ database fails, then the local database will be checked.</li> </ul>	Local / RADIUS / TACACS+ / RADIUS, Local / TACACS+, Local	Local

## RADIUS


RADIUS, or Remote Authentication Dial-In User Service, acts like a central security checkpoint for your network. It verifies the identities of users and devices trying to connect, ensuring only authorized ones gain access. Imagine it as a doorman for your switch – RADIUS checks credentials and grants permission to enter the network, enhancing overall security. This centralized approach simplifies user management and eliminates the need for individual security configurations on each device. RADIUS is particularly useful for businesses with many users, devices, or remote access needs.

## RADIUS

**Menu Path: Security > Authentication > RADIUS**

This page lets you configure the RADIUS settings for your device.

### RADIUS Settings

 **Note**

After leaving this page or refreshing, the Share Key fields will automatically be cleared to enhance security.

### RADIUS Server

Server IP Address 1 *	UDP Port *
<input type="text" value="0.0.0.0"/>	<input type="text" value="1812"/>
	1 - 65535
Share Key	
<input type="text" value="0 / 64"/>	
Auth Type *	
<input type="text" value="CHAP"/>	
Timeout *	
<input type="text" value="5"/>	
5 - 180 sec.	
Retry *	
<input type="text" value="1"/>	
0 - 5 times	
Server IP Address 2 *	UDP Port *
<input type="text" value="0.0.0.0"/>	<input type="text" value="1812"/>
	1 - 65535
Share Key	
<input type="text" value="0 / 64"/>	
Auth Type *	
<input type="text" value="CHAP"/>	
Timeout *	
<input type="text" value="5"/>	
5 - 180 sec.	
Retry *	
<input type="text" value="1"/>	
0 - 5 times	
<input type="button" value="APPLY"/>	

UI Setting	Description	Valid Range	Default Value
<b>Server Address 1/2</b>	Specify the address of the first/second RADIUS server.	Valid IP address	0.0.0.0
<b>UDP Port</b>	Specify the UDP port for the RADIUS server.	1 to 65535	1812
<b>Share Key</b>	Input the share key for server authentication verification.	0 to 64 characters	N/A
<b>Authentication Type</b>	Select the authentication type to use for the RADIUS server.	PAP / CHAP / MS-CHAPv1 / MS-CHAPv2	CHAP
<b>Timeout (sec.)</b>	Specify how long in seconds to wait for a response from the RADIUS server before timing out.	5 to 180	5

UI Setting	Description	Valid Range	Default Value
<b>Retry (sec.)</b>	Specify how many times to try reconnecting to the RADIUS server.	0 to 5	1

## TACACS+

Terminal Access Controller Access Control System Plus (TACACS+) helps provide network access control by verifying users, authorizing their actions (like read, write, or configure), and keeping a detailed log of activity. This granular control allows you to restrict what users can do on specific network devices, ensuring security and compliance. TACACS+ is especially beneficial for network administrators who need to manage user access privileges and track activity across multiple devices.

## TACACS+

### Menu Path: [Security](#) > [Authentication](#) > [TACACS+ Server](#)

This page lets you configure the TACACS+ settings for your device.

#### **Note**

The TACACS+ service will be operated using the 1st server specified. If it fails, it will run on the 2nd server specified.

#### **Note**





Users created with the TACACS+ server will be granted Admin privileges.

## TACACS+ Settings

#### **Note**

After leaving this page or refreshing, the Share Key fields will automatically be cleared to enhance security.

### TACACS+ Server

Server IP Address 1 *	TCP Port *
0.0.0.0	49
	1 - 65535
Share Key  	
0 / 64	
Auth Type *	
CHAP	
Timeout *	
5	
5 - 180	sec.
Retry *	
1	
0 - 5	times
Server IP Address 2 *	TCP Port *
0.0.0.0	49
	1 - 65535
Share Key  	
0 / 64	
Auth Type *	
CHAP	
Timeout *	
5	
5 - 180	sec.
Retry *	
1	
0 - 5	times

**APPLY**

UI Setting	Description	Valid Range	Default Value
<b>Server Address 1/2</b>	Specify the address of the first/second TACACS+ server.	Valid IP address	0.0.0.0
<b>TCP Port</b>	Specify the TCP port for the TACACS+ server.	1 to 65535	49
<b>Share Key</b>	Specify the share key for server authentication verification.	0 to 64 characters	N/A
<b>Authentication Type</b>	Select the authentication type to use for the TACACS+ server.	ASCII / PAP / CHAP	CHAP
<b>Timeout (sec.)</b>	Specify how long in seconds to wait for a response from the TACACS+ server before timing out.	5 to 180	5

UI Setting	Description	Valid Range	Default Value
<b>Retry</b>	Specify how many times to try reconnecting to the TACACS+ server.	0 to 5	1



# Diagnostics

## Menu Path: Diagnostics

This section lets you configure the diagnostics settings.

This section includes these pages:

- System Status
- Network Status
- Tools
- Event Logs and Notifications

## Diagnostics - User Privileges

Privileges to settings are granted to the different authority levels as follows. Refer to [System > Account Management > User Accounts](#) for more information on user accounts.

Settings	Admin	Supervisor	User
<b>System Status</b>			
Resource Utilization	R	R	R
Fiber Check	R/W	R/W	R
Module Information	R	R	R
<b>Network Status</b>			
Network Statistics	R	R	R
LLDP	R/W	R/W	R
ARP Table	R	R	R
<b>Tools</b>			
Port Mirroring	R/W	R/W	R
Ping	R/W	R/W	R/W

Settings	Admin	Supervisor	User
<b>Event Logs and Notifications</b>			
<b>Event Logs</b>	R/W	R/W	R
<b>Event Notifications</b>	R/W	R/W	R
<b>Syslog General</b>	R/W	R/W	R
<b>Syslog Authentication</b>	R/W	-	-
<b>SNMP Trap/Inform</b>	R/W	-	-
<b>Email Settings</b>	R/W	R/W	R
<b>Relay Alarm</b>	R/W	R/W	R

## System Status

### Menu Path: [Diagnostics](#) > [System Status](#)

This section lets you view the current system status.

This section includes these pages:

- Resource Utilization
- Fiber Check
- Module Information

## About Resource Utilization

Resource Utilization provides a set of monitoring tools to give you insights into the switch's current and historical resource usage.

These tools typically include:

- **CPU Utilization:** Percentage of CPU processing power currently being used by the device.
- **Memory History:** Historical trend of memory usage over time.
- **Power Consumption:** Current power consumption of the device.

- **Power History:** Historical trend of power consumption over time.

## Resource Utilization

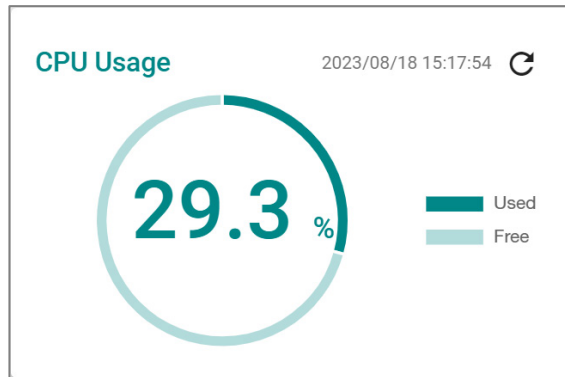
**Menu Path:** [Diagnostics](#) > [System Status](#) > [Resource Utilization](#)

This page lets you monitor current and historical system resource utilization.

### CPU Usage

This display shows the device's CPU usage.

Click the **Refresh** (🔄) icon to refresh the graph.



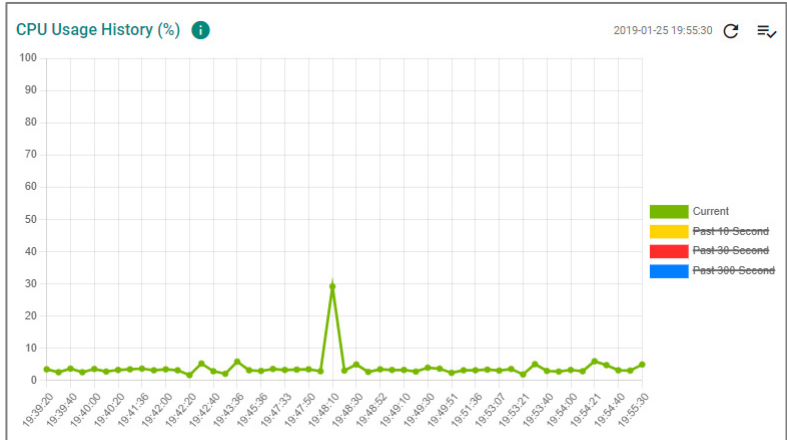
UI Setting	Description
<b>CPU Usage</b>	Displays the current utilization of the CPU.

### CPU Usage History (%)

The device's CPU usage will be shown as a percentage over time.

Click the **Refresh** (🔄) icon to refresh the graph.

Click the icon on the top-right corner of the widget to select which data to display.

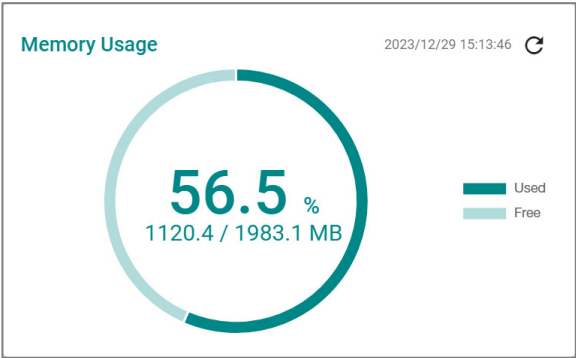


UI Setting	Description
<b>CPU Usage History</b>	Displays the CPU usage history trend in a chart.

**Memory Usage**

This display shows the device’s memory usage.

Click the **Refresh** (🔄) icon to refresh the graph.

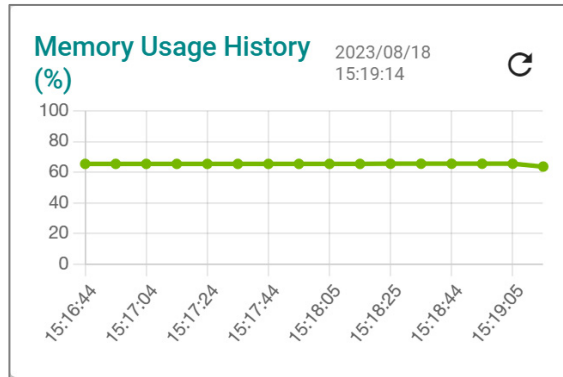


UI Setting	Description
<b>Memory Usage</b>	Displays the memory utilization status.

**Memory Usage History**

The device's memory usage will be shown as a percentage over time.

Click the **Refresh** (🔄) icon to refresh the graph.



UI Setting	Description
<b>Memory Usage History</b>	Displays the history of the memory usage.

## About Fiber Check


Optical fiber is commonly used for long-distance data transmission, so it is very costly to troubleshoot fiber cables and fiber transceivers at remote sites when issues occur. This device provides Fiber Check features to help check and diagnose the link status of fiber connectors—including Moxa’s SFP and fixed type (multi-mode SC/ST and single-mode SC) connectors—by displaying the optical parameters and corresponding thresholds. This makes it easier to remotely determine if the modules are working properly, and lets you send notifications when a threshold has been exceeded, greatly facilitating the troubleshooting process and reducing the need for onsite checks.

## Fiber Check In Depth

The Fiber Check feature displays the running status and corresponding thresholds for your device's fiber ports.

The running status shows the current wavelength, temperature, voltage, Tx power, and Rx power for the port. It also shows the corresponding high and low thresholds for temperature, voltage, Tx power, and Rx power for the port, based on its module. You can choose to use the default thresholds for a port by using Auto mode, or define the thresholds manually by using the User Define mode. Refer to Fiber Check Threshold Values for Auto Mode for more information on the default thresholds.

When a threshold is exceeded, a **Fiber Check warning** event will be triggered, which can be used to send notifications to a trap server, email, or relay, or add an event log to the syslog. Refer to [Event Notifications - Port](#) for more information.

 **Note**

This feature is only designed for Moxa's SFP and fixed type (multi-mode SC/ST and single-mode SC) fiber modules.

## Fiber Check

### Menu Path: [Diagnostics](#) > [System Status](#) > [Fiber Check](#)

This page lets you diagnose the link status of the device's fiber connectors, including SFP and fixed type (multi-mode SC/ST and single-mode SC) connectors. It lets you monitor the temperature, TX/RX power, and other parameters on fiber ports to determine if the ports are working properly.

You can enable trap, email warning, and/or relay warning functions to receive an alarm or relay if one of the fiber ports exceeds the threshold for that port. Refer to [Diagnostics > Event Logs and Notifications](#) for more information.

This page includes these tabs:

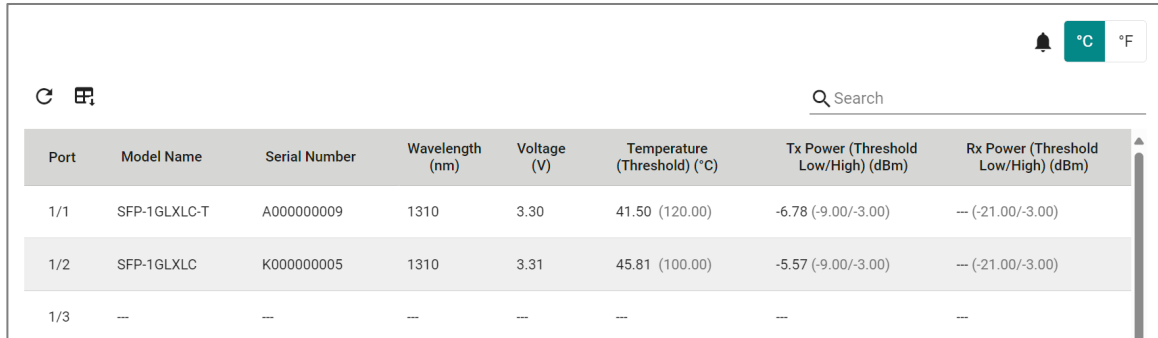
- Status
- Threshold Settings

### Fiber Check - Status

#### Menu Path: [Diagnostics](#) > [System Status](#) > [Fiber Check - Status](#)

This page lets you view the current status of your device's fiber ports.

## Fiber Check Port List



Port	Model Name	Serial Number	Wavelength (nm)	Voltage (V)	Temperature (Threshold) (°C)	Tx Power (Threshold Low/High) (dBm)	Rx Power (Threshold Low/High) (dBm)
1/1	SFP-1GLXLC-T	A000000009	1310	3.30	41.50 (120.00)	-6.78 (-9.00/-3.00)	--- (-21.00/-3.00)
1/2	SFP-1GLXLC	K000000005	1310	3.31	45.81 (100.00)	-5.57 (-9.00/-3.00)	--- (-21.00/-3.00)
1/3	--	--	--	--	--	--	--

UI Setting	Description
<b>Port</b>	Shows the port the entry is for.
<b>Model Name</b>	Shows the model name of the port.
<b>Serial Number</b>	Shows the serial number of the port.
<b>Wavelength</b>	Shows the wavelength in nm of the port.
<b>Voltage</b>	Shows the voltage in V of the port.
<b>Temperature Threshold</b>	Shows the current temperature of the port, and the low and high temperature thresholds in parentheses ( ). You can change between C and F temperatures by using the buttons at the top of the table.
<b>Tx Power (Threshold Low/High)</b>	Shows the current Tx power in dBm of the port, and the low and high thresholds for Tx power in parentheses ( ).
<b>Rx Power (Threshold Low/High)</b>	Shows the current Rx power in dBm of the port, and the low and high thresholds for Rx power in parentheses ( ).

## Fiber Check - Threshold Settings

### Menu Path: [Diagnostics](#) > [System Status](#) > [Fiber Check - Threshold Settings](#)

This page lets you configure fiber check threshold parameters for sending event notifications.

## Fiber Check Threshold Port List

	Port	Mode	Temperature Threshold (°C)	Tx Power Threshold Low (dBm)	Tx Power Threshold High (dBm)	Rx Power Threshold Low (dBm)	Rx Power Threshold High (dBm)
	1/1	Auto	---	---	---	---	---
	1/2	Auto	---	---	---	---	---
	1/3	Auto	---	---	---	---	---
	1/4	Auto	---	---	---	---	---
	2/1	---	---	---	---	---	---

UI Setting	Description
<b>Port</b>	Shows the port the entry is for.
<b>Mode</b>	Shows whether the port is using Auto or User Defined threshold settings.
<b>Temperature Threshold</b>	Shows the temperature threshold for the port. An event will be triggered if the temperature goes above this threshold.  You can change between °C and °F temperatures by using the buttons at the top of the table.
<b>Tx Power Threshold Low</b>	Shows the low threshold for Tx power in dBm. An event will be triggered if Tx power goes below this threshold.
<b>Tx Power Threshold High</b>	Shows the high threshold for Tx power in dBm. An event will be triggered if Tx power goes above this threshold.
<b>Rx Power Threshold Low</b>	Shows the low threshold for Rx power in dBm. An event will be triggered if Rx power goes below this threshold.
<b>Rx Power Threshold High</b>	Shows the high threshold for Rx power in dBm. An event will be triggered if Rx power goes above this threshold.

## Fiber Check - Edit Port Settings

### Menu Path: [Diagnostics](#) > [System Status](#) > [Fiber Check - Threshold Settings](#)

Clicking the **Edit** () icon for a port on the **Diagnostics > System Status > Fiber Check - Threshold Settings** page will open this dialog box. This dialog lets you set fiber check threshold values for the port.

Click **APPLY** to save your changes.



### Edit Port 1/1 Settings

Mode \*  
User Defined

Temperature Threshold \*  
128

-128 - 128 °C

Tx Power Threshold Low \*  
-40

-40 - 8.2 dBm

Tx Power Threshold High \*  
8.2

-40 - 8.2 dBm

Rx Power Threshold Low \*  
-40

-40 - 8.2 dBm

Rx Power Threshold High \*  
8.2

-40 - 8.2 dBm

Copy configurations to ports

CANCEL APPLY

UI Setting	Description	Valid Range	Default Value
<b>Mode</b>	Specify how fiber check threshold values should be set. <ul style="list-style-type: none"> <li><b>Auto:</b> Threshold values will be automatically specified. Refer to Fiber Check Threshold Values for more information.</li> <li><b>User Defined:</b> Threshold values are manually specified.</li> </ul>	Auto / User Defined	Auto
<b>Temperature Threshold</b>	Specify the temperature threshold for the port. An event will be triggered if the temperature goes above this threshold.  You can change between °C and °F temperatures by using the buttons to the right.	In °C: -128 to 128  In °F: -198.4 to 262.4	In °C: 128  In °F: 262.4
<b>Tx Power Threshold Low</b>	Specify the low threshold for Tx power in dBm. An event will be triggered if Tx power goes below this threshold.	-40 to 8.2 dBm	-40
<b>Tx Power Threshold High</b>	Specify the high threshold for Tx power in dBm. An event will be triggered if Tx power goes above this threshold.	-40 to 8.2 dBm	8.2
<b>Rx Power Threshold Low</b>	Specify the low threshold for Rx power in dBm. An event will be triggered if Rx power goes below this threshold.	-40 to 8.2 dBm	-40

UI Setting	Description	Valid Range	Default Value
<b>Rx Power Threshold High</b>	Specify the high threshold for Rx power in dBm. An event will be triggered if Rx power goes above this threshold.	-40 to 8.2 dBm	8.2
<b>Copy configurations to ports</b>	Select the ports you want to copy this configuration to.	Drop-down list of ports	N/A

## Module Information

**Menu Path: Diagnostics > System Status > Module Information**

This page lets you view information about the modules currently installed in your device.

### Note

Availability of this feature may vary depending on your product model and version.

## Module List

Slot	Module Name	Serial Number	Product Revision	Status
M1	RKS-G4028-L3-4GS-HV-T	---	---	---
M2	RM-G4000-8TX	TBBID0000004	V1.0.0	---
M3	RM-G4000-8TX	TBBID0000006	V1.0.0	---

1 - 3 of 3

UI Setting	Description
<b>Slot</b>	Shows the slot the module is installed in.

UI Setting	Description
<b>Module Name</b>	Shows the name of the module this entry is for.
<b>Serial Number</b>	Shows the serial number of the module.
<b>Product Revision</b>	Shows the product revision of the module.
<b>Status</b>	Shows the status of the module.

## Network Status

### Menu Path: [Diagnostics](#) > [Network Status](#)

This section lets you view the network status.

This section includes these pages:

- Network Statistics
- LLDP
- ARP Table

### About Network Statistics

Network Statistics provides monitoring tools that give you a real-time view of traffic flowing through the device.

This information typically includes:

- **Packet Counter:** The number of data packets being transmitted and received within a specific period of time, providing a crucial metric for assessing the activity and load on a network's infrastructure.
- **Bandwidth Utilization:** The percentage of the total bandwidth currently being used for data transmission.

### Network Statistics

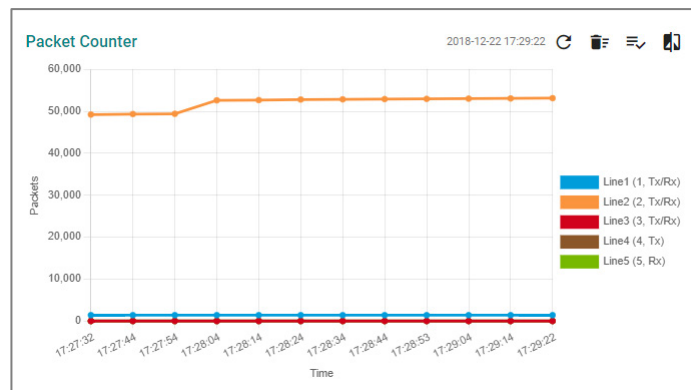
#### Menu Path: [Diagnostics](#) > [Network Status](#) > [Network Statistics](#)

This page lets you see the real-time packet and bandwidth status for your device.

## Network Status Display

You can switch between **Packet Counter** and **Bandwidth Utilization** views by clicking on the **Display Settings** (☰) icon on the top-right.

- **Packet Counter:** This view shows how many packets are being handled over time. This view updates every 5 seconds.
- **Bandwidth Utilization:** This view shows bandwidth utilization over time. This view updates every 3 seconds.



UI Setting	Description
<b>Refresh</b> (↻)	Updates statistics immediately without waiting for the refresh interval.
<b>Reset the Statistics Graph</b> (☰) (For Packet Counter display only)	Clears the display and resets display settings back to defaults.
<b>Display Settings</b> (☰)	Opens <b>Display Settings</b> , which allows you to switch between <b>Packet Counter</b> and <b>Bandwidth Usage</b> view, and add lines based on user-defined criteria.
<b>Compare Data</b> (📏) (For Packet Counter display only)	Compare data by selecting a benchmark line and time and a comparison line and time.

## Display Settings

**Display Settings**

Display Mode \*  
 Packet Counter ▾

Line 1 Monitoring Port \*      Line 1 Sniffer \*  
 1/1 ▾                              Tx/Rx ▾

Line 2 Monitoring Port \*      Line 2 Sniffer \*  
 1/2 ▾                              Tx/Rx ▾

Line 3 Monitoring Port \*      Line 3 Sniffer \*  
 1/3 ▾                              Tx/Rx ▾

Line 4 Monitoring Port \*      Line 4 Sniffer \*  
 1/4 ▾                              Tx ▾

Line 5 Monitoring Port \*      Line 5 Sniffer \*  
 2/1 ▾                              Rx ▾

CANCEL    APPLY

UI Setting	Description	Valid Range	Default Value
<b>Display Mode</b>	Select whether to show the <b>Packet Counter</b> or the <b>Bandwidth Usage</b> display.	Packet Counter / Bandwidth Usage	Packet Counter
<b>Line 1-5 Monitoring Port</b>	Select which port to monitor for the line.	Drop-down list of ports	Line 1: 1/1 Line 2: 1/2 Line 3: 1/3 Line 4: 1/4 Line 5: 2/1
<b>Line 1-5 Sniffer (If Display Mode is Packet Counter)</b>	Select which type of traffic to monitor for the line. <ul style="list-style-type: none"> <li>• <b>Tx/Rx</b>: Monitor both transmit and receive traffic.</li> <li>• <b>Tx</b>: Only monitor transmit traffic.</li> <li>• <b>Rx</b>: Only monitor receive traffic.</li> </ul>	Tx/Rx / Tx / Rx	Line 1: Tx/Rx Line 2: Tx/Rx Line 3: Tx/Rx Line 4: Tx Line 5: Rx

## Compare Data Settings

If you click on the **Compare icon** (🔍) for the **Packet Counter** display, this dialog will appear.

After making your selections, a table will appear that compares various packet statistics between the benchmark and comparison data.

- ↑ : Shows that the benchmark line number is **higher** than the comparison line.
- ⚖️ : Shows that the benchmark line number is **equal** to the comparison line.
- ↓ : Shows that the benchmark line number is **lower** than the comparison line.

**Compare Data**

Benchmark \*      Benchmark Line - Time \*

Comparison \*      Comparison Line - Time \*

CLOSE

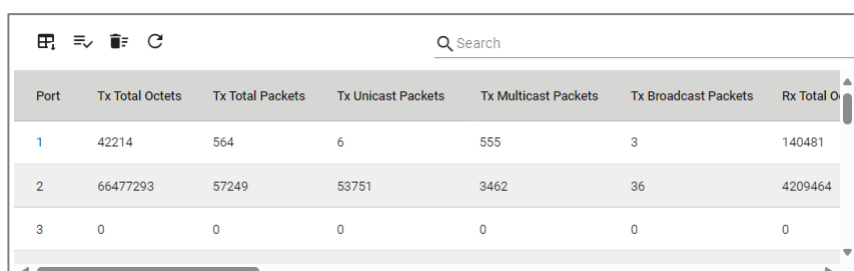
## Comparison Table

Tx Total Octets	37755097	↑	↓
Tx Total Packets	34751	↑	↓
Tx Unicast Packets	31911	↑	↓
Tx Multicast Packets	2807	↑	↓
Tx Broadcast Packets	33	↑	↓
Rx Total Octets	2831394	↑	↓
Rx Total Packets	16518	↑	↓
Rx Unicast Packets	14055	↑	↓
Rx Multicast Packets	2525	↑	↓
Rx Broadcast Packets	-62	↓	↓
Rx Pause Packets	0	⚖️	↓
Collision Packets	0	⚖️	↓
Late Collision Packets	0	⚖️	↓
Excessive Collision Packets	0	⚖️	↓

UI Setting	Description	Valid Range	Default Value
<b>Benchmark</b>	Specify which line to use as the benchmark.	Drop-down list of monitored port and sniffer combinations	N/A
<b>Benchmark Line - Time</b>	Select a timestamp to determine which benchmark data to use.	Drop-down list of timestamps	N/A
<b>Comparison</b>	Specify which line to use as the comparison.	Drop-down list of monitored port and sniffer combinations	N/A
<b>Comparison Line - Time</b>	Select a timestamp to determine which comparison data to use.	Drop-down list of timestamps	N/A

## Network Statistics Table

This table shows various packet statistics for each port.

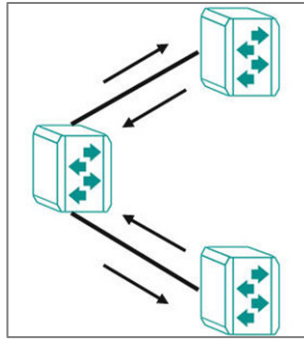


Port	Tx Total Octets	Tx Total Packets	Tx Unicast Packets	Tx Multicast Packets	Tx Broadcast Packets	Rx Total Octets
1	42214	564	6	555	3	140481
2	66477293	57249	53751	3462	36	4209464
3	0	0	0	0	0	0

## About LLDP

Link Layer Discovery Protocol (LLDP) is an OSI Layer 2 protocol defined by IEEE 802.11AB. LLDP standardizes the self-identification advertisement method, and allows each networking device to periodically send its system and configuration information to its neighbors. Because of this, all LLDP devices are kept informed of each other's status and configurations. With SNMP, this information can be transferred to Moxa's MXview One for auto-topology and network visualization.

From the device's web interface, you can enable or disable LLDP, and set the LLDP transmit interval. In addition, you can view each switch's neighbor list, which is reported by its network neighbors. Most importantly, enabling the LLDP function allows Moxa's MXview One to automatically display the network's topology and system setup details, such as VLAN and Trunking for the entire network.



## LLDP

### Menu Path: [Diagnostics](#) > [Network Status](#) > [LLDP](#)

This page lets you configure Link Layer Discovery Protocol (LLDP) for your device.

This page includes these tabs:

- Settings
- Status
- Neighbor Status

### LLDP - Settings

#### Menu Path: [Diagnostics](#) > [Network Status](#) > [LLDP - Settings](#)

This page lets you configure Link Layer Discovery Protocol (LLDP) settings.



## LLDP - Settings

LLDP \* 🔔

Enabled ▼

---

LLDP Version \*

v1(2005) ▼

---

Transmit Interval *	Notification Interval *	Tx Delay *
30	5	2
5 - 32768 sec.	5 - 3600 sec.	1 - 8192 sec.

Reinitialization Delay *	Holdtime Multiplier *
2	4
1 - 10 sec.	2 - 10 times

Chassis ID Subtype \*

Port-Component ▼ Chassis ID \* \_\_\_\_\_

APPLY

UI Setting	Description	Valid Range	Default Value
<b>LLDP</b>	Enable or disable Link Layer Discovery Protocol (LLDP).	Enabled / Disabled	Enabled
<b>LLDP Version</b>	Shows the LLDP version.	v1(2005)	v1(2005)
<b>Transmit Interval</b>	Specify how long in seconds the interval will be in between sending LLDP messages.	5 to 32768	30
<b>Notification Interval</b>	Specify how long in seconds the interval will be in between sending notifications.	5 to 3600	5
<b>Tx Delay</b>	Specify how long in seconds the interval will be in between successive LLDP frame transmissions initiated by changes.	1 to 8192	2
<b>Reinitialization Delay (Only in Advanced Mode)</b>	Specify how long in seconds the delay will be before reinitializing an LLDP packet transmission.	1 to 10	2

UI Setting	Description	Valid Range	Default Value
<b>Holdtime Multiplier</b> <b>(Only in Advanced Mode)</b>	Specify how long in seconds the receiving device will hold an LLDP packet before discarding it.	2 to 10	4
<b>Chassis ID Subtype</b>	Specify the Chassis ID subtype of the device.	Chassis-Component / If-Alias / Port-Component / MAC-Address / Network-Address / If-Name / Local	MAC-Address
<b>Chassis ID</b> <b>(If Chassis ID Subtype is Chassis-Component, Port-Component, or Local)</b>	Specify the Chassis ID.  <div style="background-color: #f0f0f0; padding: 5px;"> <p><b>Note</b></p> <p>The MAC address of the default VLAN is often used for the Chassis ID.</p> </div>	1 to 255 characters	N/A

## LLDP Port List

Port	Port Status
1/1	Tx and Rx
1/2	Tx and Rx
1/3	Tx and Rx
1/4	Tx and Rx
2/1	Tx and Rx
2/2	Tx and Rx

UI Setting	Description
<b>Port</b>	Shows the port number the entry is for.
<b>Port Status</b>	Show the status of what data is being transmitted for the port.

## LLDP - Edit Port Settings

### Menu Path: Diagnostics > Network Status > LLDP - Settings

Clicking the **Edit** (✎) icon for a port on the **Diagnostics > Network Status > LLDP - Settings** page will open this dialog box. This dialog lets you configure the LLDP settings for the port.

Click **APPLY** to save your changes.

UI Setting	Description	Valid Range	Default Value
<b>Port Status</b>	Specify the port status for transmitting data.	Tx and Rx / Tx Only / Rx Only	Tx and Rx
<b>Subtype</b>	Specify the Chassis ID subtype for the port.	Chassis-Component / If-Alias / Port-Component / MAC-Address / Network-Address / If-Name / Local	If-Alias
<b>Basic Transmit TLVs</b>	Select the basic information to use for the TLV. You can select multiple options.	Port Description / System Name / System Description	Port Description, System Name
<b>802.1 Transmit TLVs</b>	Select the 802.1 information to use for the TLV. You can select multiple options.	Port VLAN ID / VLAN Name	N/A
<b>802.3 Transmit TLVs</b>	Select the 802.3 information to use for the TLV. You can select multiple options.	Link Aggregation Statistics / Maximum Frame Size	N/A

UI Setting	Description	Valid Range	Default Value
<b>Copy configurations to ports</b>	Select the ports you want to copy this configuration to.	Drop-down list of ports	N/A

## LLDP - Status

**Menu Path: Diagnostics > Network Status > LLDP - Status**

This page lets you see the status of LLDP on your device.

### Local Information

Local Information
LLDP Enabled
LLDP Version v1(2005)
Chassis ID Subtype MAC-Address
Chassis ID 00:90:e8:af:4b:17
System Capability Bridge, Router
Interface ID / Management Address 130 / 192.168.127.253

UI Setting	Description
<b>LLDP</b>	Shows whether LLDP is enabled.
<b>LLDP Version</b>	Shows the LLDP version.
<b>Chassis ID Subtype</b>	Shows the chassis ID subtype.
<b>Chassis ID</b>	Shows the chassis ID.
<b>System Capacity</b>	Shows the system capacity.
<b>Interface ID / Management Address</b>	Shows the interface ID and the management IP address.

## Local Timer

Local Timer
Transmit Interval
30 (sec.)
Notification Interval
5 (sec.)
Tx Delay
2 (sec.)
Reinitialization Delay
2 (sec.)
Holdtime Multiplier
4 (times)

UI Setting	Description
<b>Transmit Interval</b>	Shows the interval between regular LLDP packet transmissions.
<b>Notification Interval</b>	Shows the interval between sending notifications.
<b>Tx Delay</b>	Shows the delay period between successive LLDP frame transmissions initiated by changes.
<b>Reinitialization Delay</b>	Shows the delay an LLDP port waits before reinitializing an LLDP packet transmission.
<b>Holdtime Multiplier</b>	Shows the amount of time that the receiving device will hold an LLDP packet before discarding it.

## Remote Table Statistics

### Remote Table Statistics

Last Change Time (ms)  
**1499300**

Inserts  
**2**

Drops  
**0**

Delete  
**1**

Ageouts  
**0**

UI Setting	Description
<b>Last Change Time (ms)</b>	Shows how long ago in milliseconds the remote table was last changed.
<b>Inserts</b>	Shows how many inserts have occurred.
<b>Drops</b>	Shows how many drops have occurred.
<b>Delete</b>	Shows how many deletes have occurred.
<b>Ageouts</b>	Shows how many ageouts have occurred.

## LLDP Port Status

To view the detailed LLDP status for a specific port, click the **detailed information** (i) icon for the port.

🔄 🏠
🔍 Search

Port	Tx Status	Rx Status																							
❗	1/1	Enabled	Enabled																						
<div style="border-left: 1px solid #ccc; padding-left: 10px;"> <p><b>Port Local Interface</b></p> <table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 33%;">Port ID SubType <b>If-Alias</b></td> <td style="width: 33%;">Port ID <b>Eth1/1</b></td> <td style="width: 34%;">Port Description <b>Ethernet Interface Port 01 - 1000FX,miniGBIC</b></td> </tr> </table> <p><b>Extended 802.1 TLV</b></p> <table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 33%;">Port VLAN ID <b>1</b></td> <td style="width: 33%;">VLAN ID / Name <b>1 / ---</b></td> <td style="width: 34%;"></td> </tr> </table> <p><b>Extended 802.3 TLV</b></p> <table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 33%;">Link Aggregation Status <b>Disabled</b></td> <td style="width: 33%;">Aggregated Port ID <b>0</b></td> <td style="width: 34%;">Maximum Frame Size <b>9216</b></td> </tr> </table> <p><b>Port Traffic Statistics</b></p> <table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 33%;">Total Frames Out <b>0</b></td> <td style="width: 33%;">Total Entries Aged <b>0</b></td> <td style="width: 34%;">Total Frames In <b>0</b></td> </tr> <tr> <td>Total Frames Received In Error <b>0</b></td> <td>Total Frames Discarded <b>0</b></td> <td>Total TLVs Unrecognized <b>0</b></td> <td>Total TLVs Discarded <b>0</b></td> </tr> </table> <p><b>Extended Ethernet/IP TLV</b></p> <table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 33%;">Vendor ID <b>991</b></td> <td style="width: 33%;">Device Type <b>44</b></td> <td style="width: 34%;">Product Code <b>8963</b></td> </tr> <tr> <td>Major Revision <b>1</b></td> <td>Minor Revision <b>0</b></td> <td>Serial Number <b>1119503</b></td> </tr> </table> </div>				Port ID SubType <b>If-Alias</b>	Port ID <b>Eth1/1</b>	Port Description <b>Ethernet Interface Port 01 - 1000FX,miniGBIC</b>	Port VLAN ID <b>1</b>	VLAN ID / Name <b>1 / ---</b>		Link Aggregation Status <b>Disabled</b>	Aggregated Port ID <b>0</b>	Maximum Frame Size <b>9216</b>	Total Frames Out <b>0</b>	Total Entries Aged <b>0</b>	Total Frames In <b>0</b>	Total Frames Received In Error <b>0</b>	Total Frames Discarded <b>0</b>	Total TLVs Unrecognized <b>0</b>	Total TLVs Discarded <b>0</b>	Vendor ID <b>991</b>	Device Type <b>44</b>	Product Code <b>8963</b>	Major Revision <b>1</b>	Minor Revision <b>0</b>	Serial Number <b>1119503</b>
Port ID SubType <b>If-Alias</b>	Port ID <b>Eth1/1</b>	Port Description <b>Ethernet Interface Port 01 - 1000FX,miniGBIC</b>																							
Port VLAN ID <b>1</b>	VLAN ID / Name <b>1 / ---</b>																								
Link Aggregation Status <b>Disabled</b>	Aggregated Port ID <b>0</b>	Maximum Frame Size <b>9216</b>																							
Total Frames Out <b>0</b>	Total Entries Aged <b>0</b>	Total Frames In <b>0</b>																							
Total Frames Received In Error <b>0</b>	Total Frames Discarded <b>0</b>	Total TLVs Unrecognized <b>0</b>	Total TLVs Discarded <b>0</b>																						
Vendor ID <b>991</b>	Device Type <b>44</b>	Product Code <b>8963</b>																							
Major Revision <b>1</b>	Minor Revision <b>0</b>	Serial Number <b>1119503</b>																							
❗	1/2	Enabled	Enabled																						
❗	1/3	Enabled	Enabled																						
❗	1/4	Enabled	Enabled																						
❗	2/1	Enabled	Enabled																						
❗	2/2	Enabled	Enabled																						

UI Setting	Description
<b>Port</b>	Shows the port number the entry is for.
<b>Tx Status</b>	Shows whether LLDP is enabled for transmit traffic.
<b>Rx Status</b>	Shows whether LLDP is enabled for receive traffic.

## menu reference LLDP - Neighbor Status

### LLDP - Neighbor Status

**Menu Path:** [Diagnostics](#) > [Network Status](#) > [LLDP - Neighbor Status](#)

This page lets you see the neighbor status of LLDP.

### Neighbor Status

Local Port	System Capability	Neighbor Port ID	Neighbor Chassis ID	Port Description	System Name	Hold Time
3/3	---	---	---	---	---	---
3/4	Router	2	00:90:e8:00:00:05	100TX	NAT Router	---
3/5	---	---	---	---	---	---
3/6	---	---	---	---	---	---
3/7	---	---	---	---	---	---
3/8	Router	5	00:90:e8:a9:ed:2b	100TX	Firewall/ETBN Router 05518	---
4/1	---	---	---	---	---	---

1 - 28 of 28

UI Setting	Description
<b>Local Port</b>	Shows the number of the port connected to the neighbor.
<b>System Capability</b>	Shows the system capability of the neighbor.
<b>Neighbor Port ID</b>	Shows the neighbor's port ID for the interface this device is connected to.
<b>Neighbor Chassis ID</b>	Shows the unique ID (typically the MAC address) used to identify the neighbor device.
<b>Port Description</b>	Shows the neighbor's port description for the interface this device is connected to.
<b>System Name</b>	Shows the hostname of the neighbor device.
<b>Hold Time</b>	Shows the amount of time that the receiving device will hold an LLDP packet before discarding it.



## About ARP Tables

The **ARP Table (Address Resolution Protocol Table)** is a database maintained by Ethernet switches. It acts like a translator that maps Media Access Control (MAC) addresses to their corresponding IP addresses. Network devices communicate using MAC addresses, which are unique hardware identifiers. However, routing between devices often relies on IP addresses, so ARP tables are used to bridge this gap.

## ARP Table

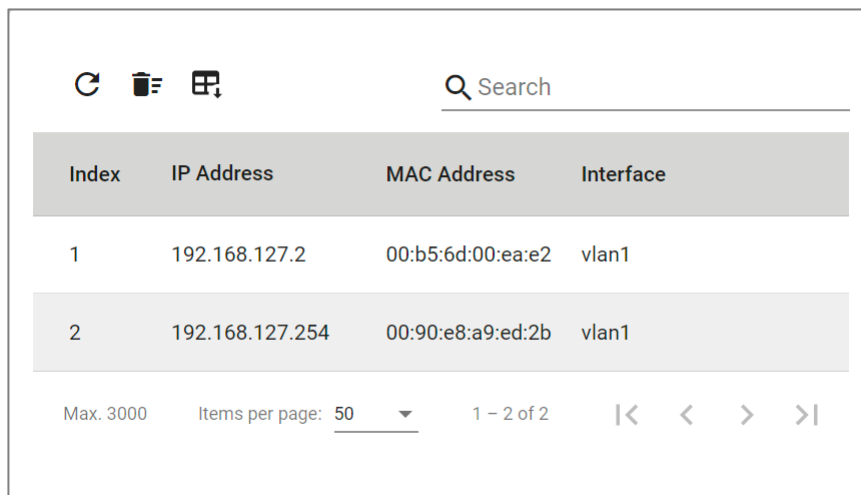
**Menu Path: Diagnostics > Network Status > ARP Table**

This page lets you see the device's Address Resolution Protocol (ARP) table.

### Limitations

The ARP table can show up to 3000 entries.

## ARP Table



Index	IP Address	MAC Address	Interface
1	192.168.127.2	00:b5:6d:00:ea:e2	vlan1
2	192.168.127.254	00:90:e8:a9:ed:2b	vlan1

Max. 3000    Items per page: 50    1 - 2 of 2

UI Setting	Description
<b>Index</b>	Shows the index of the device entry.
<b>IP Address</b>	Shows the IP address used for the device.

UI Setting	Description
<b>MAC Address</b>	Shows the MAC address of the device.
<b>Interface</b>	Shows the interface the device is connecting through.

## Tools

### Menu Path: [Diagnostics](#) > [Tools](#)

This page lets you use various tools to help troubleshoot network issues.

This page includes these tabs:

- Port Mirroring
- Ping

## About Port Mirroring

Port Mirroring is used to monitor data being transmitted through specific ports. This is done by setting up mirror ports to receive the same data being transmitted to, from, or both to and from the ports being monitored. Using mirror ports allows network administrators to sniff the observed ports to keep tabs on network activity.

## Port Mirroring In Depth

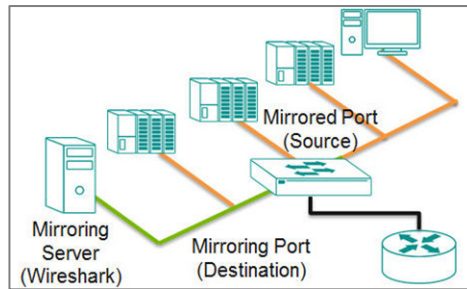
There are two ways to use Port Mirroring on this device:

- **SPAN (Switched Port Analyzer):** Mirrors data from monitored ports to multiple terminal ports on the same switch.
- **RSPAN (Remote Switched Port Analyzer):** Mirrors data from monitored ports on one switch to multiple terminal ports on other switches.

### SPAN

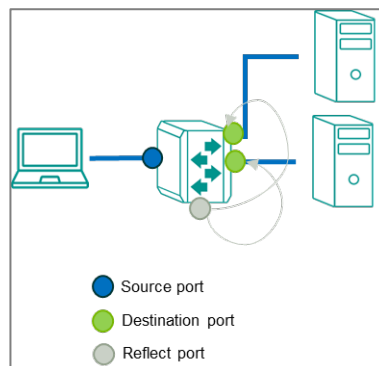
**SPAN** can be configured to copy packets from various ports to a single port or multiple ports, so that users can check if there are problems occurring in these ports.

For example, the following figure demonstrates how packets transmitted through the four mirrored ports (marked in orange) are copied (mirrored) to a single mirroring port (marked in green). These packets will be sent to a monitoring computer where software is used to check for issues with the packets. This is useful for troubleshooting or monitoring network data transmissions for debugging or security purposes.



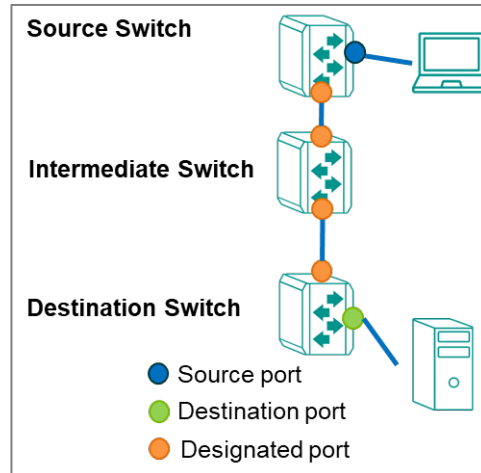
Ingress, egress, or both ingress and egress traffic can be mirrored one or more destination ports.

If you want to mirror traffic to multiple destination ports, than a reflect port needs to be assigned and the destination ports need to be in the same VLAN as the reflect port.



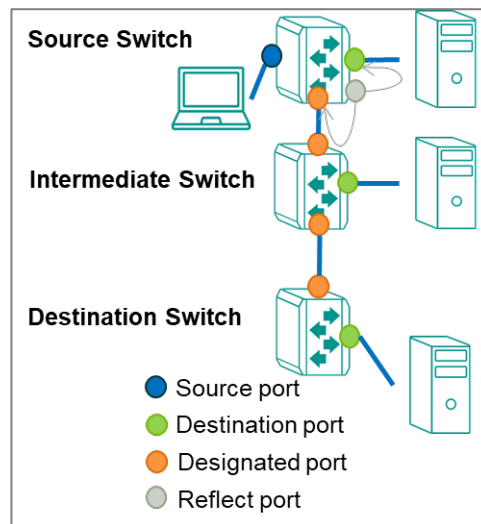
## RSPAN

**RSPAN** can be configured to copy packets from one or more ports from one or more source switches through intermediate switches to one or more ports on destination switches. The PC or monitoring server can be connected to destination ports on the destination switch to receive a copy of the original traffic being monitored. For example, the following figure demonstrates how packets transmitted to a source port (marked in blue) are copied (mirrored) through an intermediate switch to one or more destination ports (marked in green). Source traffic can be copied through multiple intermediate switches to single or multiple destination switches.



Ingress, egress, or both ingress and egress traffic of the source port(s) can be mirrored to one or more destination ports on destination switches.

If you want to mirror traffic to destination ports on the source switch, a reflect port needs to be assigned. Destination ports in source switch, intermediate switch(es), and destination switch(es) need to be in the same VLAN as the reflect port.



- You can set source ports to be from one or more RSPAN source switches. If one of the destination ports is on a source switch, a reflect port needs to be assigned.
- You can configure an RSPAN VLAN for monitored traffic to be labeled with a RSPAN VLAN tag and send monitored traffic to an RSPAN destination switch via trunk ports.
- You can configure ports to join an RSPAN VLAN, these ports will be destination ports to receive monitored traffic.

- You can connect a monitoring computer to a destination port to receive monitoring traffic for software analysis or diagnostics.

## Port Mirroring

### Menu Path: Diagnostics > Tools > Port Mirroring

This page lets you configure port mirroring for your device.

This page includes these tabs:

- General
- SPAN
- RSPAN

### Port Mirroring - General

#### Menu Path: Diagnostics > Tools > Port Mirroring - General

This page lets you enable or disable port mirroring for your device.

The screenshot shows a web interface for 'Port Mirroring'. At the top, there are three tabs: 'General', 'SPAN', and 'RSPAN'. The 'General' tab is selected. Below the tabs, there is a dropdown menu labeled 'Port Mirroring \*' with 'Enabled' selected. Below the dropdown is a green 'APPLY' button.

UI Setting	Description	Valid Range	Default Value
<b>Port Mirroring</b>	Enable or disable port mirroring to facilitate the creation of SPAN or RSPAN sessions.	Enabled / Disabled	Enabled

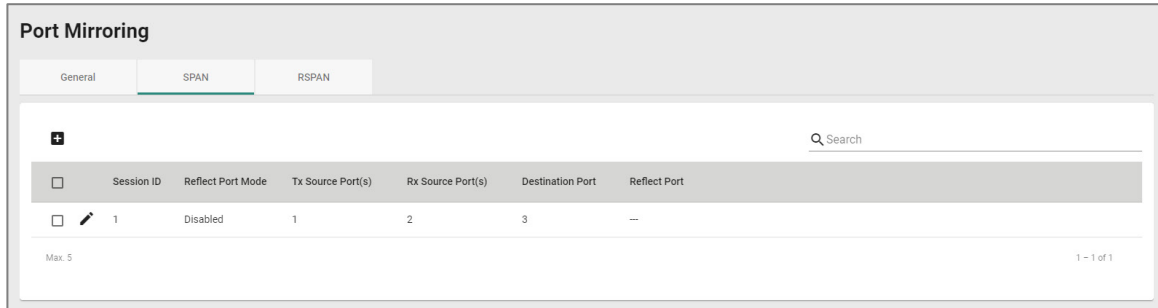
## SPAN

### Menu Path: Diagnostics > Tools > Port Mirroring - SPAN

This page lets you view and configure your device's SPAN settings.

## 🔒 Limitations

You can create up to 5 SPAN entries.



## UI Setting Description

**Session ID** Shows the session ID the entry is for.

### 📌 Note

SPAN and RSPAN share 7 sessions, SPAN uses 1 to 5, and RSPAN uses 6 and 7.

**Reflect Port Mode** Shows whether Reflect Port Mode is enabled.

**Tx Source Port(s)** Shows the Tx source ports for the session.

**Rx Source Port(s)** Shows the Rx source ports for the session.

**Destination Port** Shows the destination port for the session.

**Reflect Port** Shows the reflect port for the session.

## Creating a SPAN Session

### Menu Path: [Diagnostics](#) > [Tools](#) > [Port Mirroring - SPAN](#)

Clicking the **Add** (🛠️) icon on the **Diagnosis > Port Mirroring - SPAN** page will open this dialog box. This dialog lets you create a SPAN session.

Click **CREATE** to save your changes and add the new session.

### Create Session

Session ID \* ▼

---

Reflect Port Mode \* ▼

---

Tx Source Port(s) ▼      Rx Source Port(s) ▼

---

Destination Port \* ▼

---

Either the TX or RX source ports need to be selected.

CANCEL
CREATE

UI Setting	Description	Valid Range	Default Value
<b>Session ID</b>	Select the session ID to use for the session. <div style="background-color: #f0f0f0; padding: 5px; margin-top: 10px;"> <p><b>Note</b></p> <p>SPAN and RSPAN share 7 sessions, SPAN uses 1 to 5, and RSPAN uses 6 and 7.</p> </div>	1 to 5	N/A
<b>Reflect Port Mode</b>	Enable or disable Reflect Port Mode. <ul style="list-style-type: none"> <li><b>Enabled:</b> You can configure a reflect port to mirror packets to multiple destination ports.</li> <li><b>Disabled:</b> Packets will be mirrored to a single destination port.</li> </ul>	Enabled / Disabled	N/A
<b>Tx Source Port</b>	Specify a port to monitor data packets being sent through it. <div style="background-color: #f0f0f0; padding: 5px; margin-top: 10px;"> <p><b>Note</b></p> <p>Avoid selecting source ports that are in the same VLAN as the reflect port.</p> </div>	Drop-down list of ports	N/A
<b>Rx Source Port</b>	Specify a port to monitor data packets being received through it. <div style="background-color: #f0f0f0; padding: 5px; margin-top: 10px;"> <p><b>Note</b></p> <p>Avoid selecting source ports that are in the same VLAN as the reflect port.</p> </div>	Drop-down list of ports	N/A

UI Setting	Description	Valid Range	Default Value
<b>Reflect Port</b>	Specify this port as the reflect port for Reflect Port Mode to mirror packets to multiple destination ports.  <div style="background-color: #f0f0f0; padding: 5px; margin: 5px 0;"> <p><b>Note</b></p> <p>This port will be specifically reserved for reflect port use, please do not configure it for other uses.</p> </div> <div style="background-color: #f0f0f0; padding: 5px; margin: 5px 0;"> <p><b>Note</b></p> <p>Avoid selecting reflect ports that are in the management VLAN.</p> </div>	Drop-down list of ports	N/A
<b>Destination Port</b>	Specify the destination port to use for the session.	Drop-down list of ports	N/A

## RSPAN

### Menu Path: [Diagnostics](#) > [Tools](#) > [Port Mirroring - RSPAN](#)

This page lets you view and configure your device's RSPAN settings.



### 🔔 Limitations

You can create up to 2 RSPAN entries.

## RSPAN Intermediate Settings

### Port Mirroring

- General
- SPAN
- RSPAN**

#### RSPAN Intermediate Settings

Make sure that any ports used for RSPAN communication are added to the appropriate RSPAN VLAN.

RSPAN Intermediate Role \*  
Disabled ▾

RSPAN Intermediate 1st VLAN ID ▾ RSPAN Intermediate 2nd VLAN ID ▾

**APPLY**

UI Setting	Description	Valid Range	Default Value
<b>RSPAN Intermediate Role</b>	Enable this if the device is in an intermediate role. Disable this if the device is in a source or destination role.	Enabled / Disabled	Disabled
<b>RSPAN Intermediate 1st/2nd VLAN ID</b>	Specify the VLAN ID to use as the RSPAN intermediate VLAN ID.  <b>Note</b> The management VLAN ID cannot be used as an RSPAN intermediate VLAN ID.  Two RSPAN Intermediate VLAN are supported after v5.x. If you downgrade firmware version to version before v5.x. Only 1st VLAN ID will be reserved in the configuration.	Drop-down list of VLAN IDs	N/A

## RSPAN Session List

<div style="float: right;">Q Search</div>								
<input type="checkbox"/>	Session ID	Reflect Port Mode	RSPAN Type	RSPAN VLAN ID	Tx Source Port(s)	Rx Source Port(s)	Destination Port(s) or Designated Port	Reflect Port
<input type="checkbox"/>	6	Disabled	Source	5	--	--	Designated Port: G2	--

Max. 2 1 - 1 of 1

UI Setting	Description
<b>Session ID</b>	Shows the session ID the entry is for.
	<div style="background-color: #f0f0f0; padding: 5px;"> <p> <b>Note</b> SPAN and RSPAN share 7 sessions, SPAN uses 1 to 5, and RSPAN uses 6 and 7.</p> </div>
<b>Reflect Port Mode</b>	Shows whether Reflect Port Mode is enabled for the session.
<b>RSPAN Type</b>	Shows Source if the device role is an RSPAN source switch. Shows Destination if the device role is an RSPAN destination switch.
<b>RSPAN VLAN ID</b>	Shows the VLAN ID used for the RSPAN.
<b>Tx Source Port</b>	Shows the ports being monitored for Tx packets being sent out.
<b>Rx Source Port</b>	Shows the ports being monitored for Rx packets coming in.
<b>Designated Port</b>	Shows the port set as the designated port.
<b>Reflect Port</b>	Shows the port set as the Reflect Port for Reflect Port Mode to mirror packets to the designated ports.

## Creating an RSPAN Session

### Menu Path: [Diagnostics](#) > [Tools](#) > [Port Mirroring - RSPAN](#)

Clicking the **Add (+)** icon on the **Diagnostics > Tools > Port Mirroring - RSPAN** page will open this dialog box. This dialog lets you create an RSPAN session.


Click **CREATE** to save your changes and add the new session.

### Create Session

Session ID \*

Reflect Port Mode \*


RSPAN Type \*





RSPAN VLAN ID \*  

Tx Source Port(s)  Rx Source Port(s)

Designated Port \*

Either the TX or RX source ports need to be selected.

UI Setting	Description	Valid Range	Default Value
<b>Session ID</b>	Select the session ID to use for the session.  <div style="background-color: #f0f0f0; padding: 5px;"> <p> <b>Note</b> SPAN and RSPAN share 7 sessions, SPAN uses 1 to 5, and RSPAN uses 6 and 7.</p> </div>	6 / 7	N/A
<b>Reflect Port Mode</b>	Enable or disable Reflect Port Mode. <ul style="list-style-type: none"> <li><b>Enable:</b> You can configure a reflect port to mirror packets to destination port(s) in source switch.</li> <li><b>Disable:</b> Packets will be only mirrored to designated port.</li> </ul>	Enabled / Disabled	N/A

UI Setting	Description	Valid Range	Default Value
<b>RSPAN Type</b>	<p>Select the RSPAN type to use for the session.</p> <ul style="list-style-type: none"> <li><b>Source:</b> The device will act as an RSPAN source switch.</li> <li><b>Destination:</b> The device will act as an RSPAN destination switch.</li> </ul>	Source / Destination	N/A
<b>RSPAN VLAN ID</b>	<p>Select the VLAN ID to use as the RSPAN VLAN ID. Only existing VLAN IDs can be selected.</p> <div style="background-color: #f0f0f0; padding: 5px; margin-top: 10px;"> <p> <b>Note</b></p> <p>Using the management VLAN or VLAN assignment-configured for RSPAN is not recommended.</p> </div>	Drop-down list of VLAN IDs	N/A
<b>Tx Source Port</b>	<p>Select the ports you want to monitor for Tx packets being sent out.</p> <div style="background-color: #f0f0f0; padding: 5px; margin-top: 10px;"> <p> <b>Note</b></p> <p>Avoid selecting source ports that are in the RSPAN VLAN.</p> </div>	Drop-down list of ports	N/A
<b>Rx Source Port</b>	<p>Select the ports you want to monitor for Rx packets coming in.</p> <div style="background-color: #f0f0f0; padding: 5px; margin-top: 10px;"> <p> <b>Note</b></p> <p>Avoid selecting source ports that are in the RSPAN VLAN.</p> </div>	Drop-down list of ports	N/A
<b>Designated Port</b>	<p>Select the port to use as the designated port.</p>	Drop-down list of ports	N/A
<b>Reflect Port</b>	<p>Select the port to use as the reflect port for Reflect Port Mode to mirror packets to multiple designated ports.</p> <div style="background-color: #f0f0f0; padding: 5px; margin-top: 10px;"> <p> <b>Note</b></p> <p>This port is specifically reserved for reflect port use, please do not configure it for other use.</p> </div>	Drop-down list of ports	N/A

## Ping

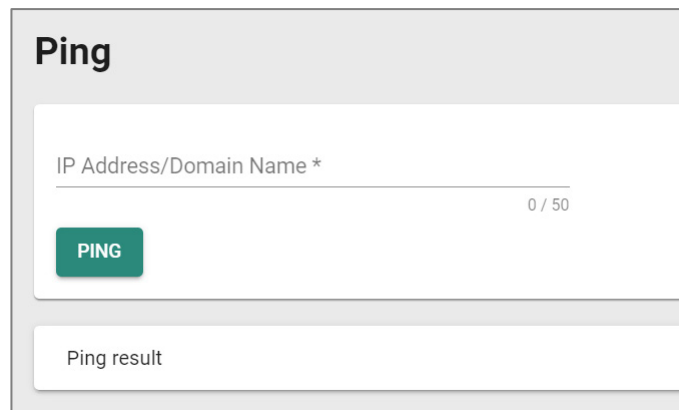
Ping lets you use the ping command through the device for a simple, but powerful tool for troubleshooting network problems. The unique feature of this is that even though the

ping command is entered in your browser window, the actual ping command will be sent from the Moxa device itself.

## Ping

### Menu Path: [Diagnostics](#) > [Tools](#) > [Ping](#)

This page lets you use the ping function, which is useful for troubleshooting network problems.



UI Setting	Description	Valid Range	Default Value
<b>IP Address/Domain Name</b>	Specify the IP address or domain name you want to ping, then click the <b>PING</b> button. The ping result will be displayed below.	Valid IP address or domain name up to 50 characters	N/A

## Event Logs and Notifications

### Menu Path: [Diagnostics](#) > [Event Logs and Notifications](#)

This section lets you set up and view your device's event logs and notifications.

This section includes these pages:

- Event Logs
- Event Notifications
- Syslog
- SNMP Trap/Inform

- Email Settings
- Relay Alarm

## About Event Logs

Event logs automatically record important events that happen on the network connected to a switch. They are useful when troubleshooting network issues.

These events can include:

- **Changes in connection status:** This could be a cable being plugged in or unplugged, a device joining or leaving the network, or a port going up or down.
- **Errors:** The switch might detect issues like data corruption, excessive traffic, or problems with specific ports.
- **Security events:** Some switches can log attempts to access the switch itself or suspicious activity on the network.

## Event Logs

**Menu Path:** [Diagnostics](#) > [Event Logs and Notifications](#) > [Event Logs](#)

This page lets you browse and export your device's various event logs.

This page includes these tabs:

- Event Logs
- Oversize Action
- Backup

### Event Logs - Event Logs

**Menu Path:** [Diagnostics](#) > [Event Logs and Notifications](#) > [Event Logs - Event Logs](#)

This page lets you view your device's event logs.

## 🔌 Limitations

The system log can record up to 10000 events.

## Actions

- Click the **Refresh icon** (🔄) to refresh the logs.
- Click the **Clear System Log icon** (🗑️) to delete all logs.
- Click the **Export icon** (📄) to export all logs to a file.

Event Logs						
Event Logs	Oversize Action	Backup				
🔄	🗑️	📄	🔍 Search			
Index	Bootup Number	Severity	Timestamp	Uptime	Message	
1	461	Notice	2024-04-10 03:51:21	9d6h34m42s	[Account:admin] logged out.	
2	461	Notice	2024-04-10 03:51:21	9d6h34m42s	[Account:admin] successfully logged in via local.	
3	461	Notice	2024-04-10 03:48:13	9d6h31m34s	[Account:admin] successfully logged in via local.	
4	461	Notice	2024-04-10 03:30:57	9d6h14m18s	[Account:admin] logged out.	
5	461	Notice	2024-04-10 03:27:26	9d6h10m47s	[Account:admin] logged out.	
6	461	Notice	2024-04-10 03:27:26	9d6h10m47s	[Account:admin] successfully logged in via local.	
7	461	Notice	2024-04-10 03:01:06	9d5h44m28s	[Account:admin] successfully logged in via local.	
8	461	Notice	2024-04-10 02:49:16	9d5h32m38s	[Account:admin] logged out.	
9	461	Notice	2024-04-10 02:28:57	9d5h12m19s	Configuration [dhcpRelay] changed by admin.	
10	461	Notice	2024-04-10 02:28:03	9d5h11m24s	Configuration [mlexport] changed by admin.	

UI Setting	Description
------------	-------------

<b>Index</b>	Shows the index of the event.
--------------	-------------------------------

<b>Bootup Number</b>	Shows the total number of times the device has been powered on. The number increases by 1 every time the device is powered on.
----------------------	--

<b>Severity</b>	Shows the severity categorization of the event.
-----------------	---

<b>Timestamp</b>	Shows the time of the event, including the date, time, and UTC time zone adjustment.
------------------	--

<b>Uptime</b>	Shows the uptime of the device after it is powered on.
---------------	--

<b>Message</b>	Shows additional information about the event, based on the type of event. The username of the account will also be recorded for the following events: <b>Login Success</b> , <b>Login Fail</b> , <b>User Logout</b> .
----------------	---

## Event Logs - Oversize Action

### Menu Path: Diagnostics > Event Logs and Notifications > Event Logs - Oversize Action

This page lets you configure the system's oversize action when the event log reaches its maximum number of entries.

### Oversize Action

The screenshot shows the 'Event Logs' configuration page with the 'Oversize Action' tab selected. The 'Oversize Action' dropdown is set to 'Overwrite the oldest event log'. The 'Capacity Warning' dropdown is set to 'Disabled'. The 'Warning Threshold' is set to '80', with a range indicator below it showing '50 - 100 %'. An 'APPLY' button is located at the bottom of the configuration area.

UI Setting	Description	Valid Range	Default Value
<b>Oversize Action</b>	Select the action to take when the event log reaches its maximum number of entries. <ul style="list-style-type: none"><li>• <b>Overwrite the oldest event log:</b> New events will overwrite the oldest events.</li><li>• <b>Stop recording event log:</b> No new events will be recorded. This will also disable port monitoring.</li></ul>	Overwrite the oldest event log / Stop recording event log	Overwrite the oldest event log
<b>Capacity Warning</b>	Enable or disable capacity warnings.	Enabled / Disabled	Disabled
<b>Warning Threshold</b>	Set the warning threshold as a percentage. When <b>Capacity Warning</b> is enabled, a warning event log will be triggered when the event log reaches this threshold.	50% to 100%	80%



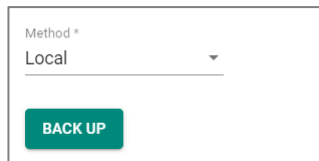
## Event Logs - Backup

**Menu Path: Diagnostics > Event Logs and Notifications > Event Logs - Backup**

This page lets you back up the event logs through various methods.

### Event Logs - Backup Settings - Local

If **Method** is set to **Local**, these settings will appear. Click **BACK UP** to save the event logs to your local computer.



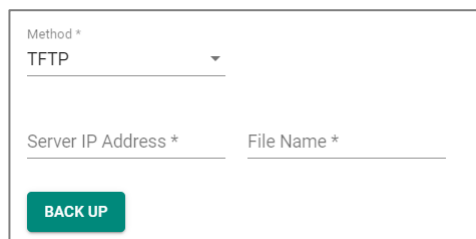
Method \*  
Local

BACK UP

UI Setting	Description	Valid Range	Default Value
<b>Method</b>	Select a method for backing up event logs.	Local / TFTP / SFTP / USB	Local

### Event Logs - Backup Settings - TFTP

If **Method** is set to **TFTP**, these settings will appear. Click **BACK UP** to save the event log to the specified TFTP server.



Method \*  
TFTP

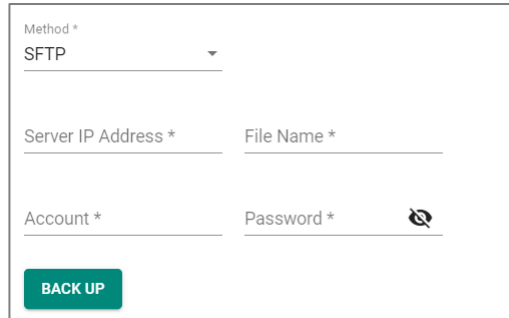
Server IP Address \*      File Name \*

BACK UP

UI Setting	Description	Valid Range	Default Value
<b>Method</b>	Select a method for backing up event logs.	Local / TFTP / SFTP / USB	Local
<b>Server IP Address</b>	Specify the IP address of the TFTP server to upload the event logs to.	Valid IP address	N/A
<b>File Name</b>	Specify a file name to use for the event logs file.	File name can only contain A-Z, a-z, 0-9 or the symbols -._().	N/A

## Event Logs - Backup Settings - SFTP

If **Method** is set to **SFTP**, these settings will appear. Click **BACK UP** to save the event log to the specified SFTP server.



UI Setting	Description	Valid Range	Default Value
<b>Method</b>	Select a method for backing up event logs.	Local / TFTP / SFTP / USB	Local
<b>Server IP Address</b>	Specify the IP address of the SFTP server to upload the event logs to.	Valid IP address	N/A
<b>File Name</b>	Specify a file name to use for the event logs file.	File name can only contain A-Z, a-z, 0-9 or the symbols -._().	N/A
<b>Account</b>	Enter the SFTP server account name to use to connect to the SFTP server.	N/A	N/A
<b>Password</b>	Enter the SFTP server account password to use to connect to the SFTP server.	N/A	N/A

## Event Logs - Backup Settings - USB

If **Method** is set to **USB**, these settings will appear. Click **BACK UP** to save the event log to an ABC-02 configuration tool connected to your device's USB port.

### Note

To use this feature, USB Function must be enabled in System > Management Interface > Hardware Interface.

UI Setting	Description	Valid Range	Default Value
<b>Method</b>	Select a method for backing up event logs.	Local / TFTP / SFTP / USB	Local

### Event Logs - Backup Settings - microSD

If **Method** is set to **microSD**, these settings will appear. Click **BACK UP** to save the event log to a microSD card inserted into your device's microSD slot.

#### Note

To use this feature, microSD Function must be enabled in System > Management Interface > Hardware Interfaces.

UI Setting	Description	Valid Range	Default Value
<b>Method</b>	Select a method for backing up event logs.	Local / TFTP / SFTP / USB	Local

### Auto Event Log Backup

When **Automatically Back Up** is enabled, when the event log is full, the earliest 1000 event logs will be backed up to an inserted ABC-02 configuration tool or microSD card and then deleted from the device.

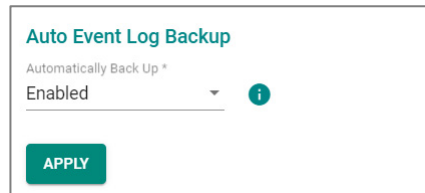
**Note**

To use an ABC-02 configuration tool, USB Function must be enabled in System > Management Interface > Hardware Interface.

To use a microSD card, microSD Function must be enabled in System > Management Interface > Hardware Interfaces.

**Note**

If both an ABC-02 configuration tool and a microSD card are inserted into the device, the ABC-02 configuration tool will be used.



UI Setting	Description	Valid Range	Default Value
<b>Automatically Back Up</b>	Enable or disable automatic backup of your event logs.	Enabled / Disabled	Enabled

## About Event Notifications

Event Notifications act like an alert system for the network. They allow you to be proactively notified when important events occur on the device or for other network devices connected to it.

### Event Notifications

**Menu Path: Diagnostics > Event Logs and Notifications > Event Notifications**

This page lets you configure notifications for various kinds of events.

This page includes these tabs:

- System and Functions
- Port

## Event Notifications - System and Functions


### Menu Path: Diagnostics > Event Logs and Notifications > Event Notifications - System and Functions

This page lets you configure notification settings for various system events related to the overall functions of the device. Each event can be configured independently with different warning methods and severity classifications.

### Event Notifications List


Group	Event Name	Enabled	Severity	Registered Action
General	Cold start	Enabled	Critical	Trap, Email
General	Warm start	Enabled	Notice	Trap, Email
General	Configuration changed	Enabled	Notice	Trap, Email
General	Login success	Enabled	Notice	Trap, Email
General	Login failed	Enabled	Warning	Trap, Email
General	Login lockout	Enabled	Warning	Trap, Email
General	Account settings changed	Enabled	Notice	Trap, Email
General	Configuration imported	Enabled	Notice	Trap, Email
General	SSL certification changed	Enabled	Notice	Trap, Email
General	Log capacity threshold	Enabled	Warning	Trap, Email
General	Password changed	Enabled	Notice	Trap, Email
General	Power On->Off	Enabled	Notice	Trap, Email
General	Power Off->On	Enabled	Notice	Trap, Email
Switching	Topology changed	Enabled	Warning	Trap, Email
Switching	Coupling changed	Enabled	Warning	Trap, Email
Switching	Master changed	Enabled	Warning	Trap, Email
Switching	Master mismatch	Enabled	Warning	Trap, Email

UI Setting	Description
<b>Group</b>	Shows which group this event belongs to.
<b>Event Name</b>	Shows the name of the event. Refer to <a href="#">Event Log Descriptions</a> for more details.
<b>Enabled</b>	Shows whether event notifications are enabled for this kind of event.

UI Setting	Description
<b>Severity</b>	Shows the severity assigned to the event. Refer to the <a href="#">Severity Level List</a> for more details.
<b>Registered Action</b>	Shows which action will be taken for this kind of event. <b>Trap:</b> A notification is sent to the Trap server when the event is triggered. <b>Email:</b> A notification is sent to the email server defined in the <a href="#">Email Settings</a> section. <b>Relay:</b> A notification is sent through the relay interface, if the device has one, when the event is triggered.
	<p> <b>Note</b></p> <p>The types of actions available may vary depending on the event type and the device model.</p>

## Editing an Event Notification

### Menu Path: [Diagnostics](#) > [Event Logs and Notifications](#) > [Event Notifications - System and Functions](#)

Clicking the **Edit** () icon for an entry on the **Diagnostics > Event Logs and Notifications > Event Notifications - System and Functions** page will open this dialog box. This dialog lets you change the notification settings for the selected event.

Click **APPLY** to save your changes.

**Edit This Event Notification**

Event Name  
Cold start

---

Enabled \*  
Enabled ▼

Registered Action  
Trap, Email ▼

CANCEL APPLY

UI Setting	Description	Valid Range	Default Value
<b>Event Name (View-only)</b>	Shows the name of the event. Refer to <a href="#">Event Log Descriptions</a> for more information.	(Fixed)	(Fixed)

UI Setting	Description	Valid Range	Default Value
<b>Enabled</b>	Enable or disable notifications for this event.	Enabled / Disabled	Enabled
<b>Registered Action</b>	Select which actions to take when the event occurs. Multiple actions may be selected. <ul style="list-style-type: none"> <li>• <b>Trap:</b> A notification will be sent to the Trap server.</li> <li>• <b>Email:</b> A notification email will be sent to the email server defined in the <a href="#">Email Settings</a> section.</li> <li>• <b>Relay:</b> An alarm notification will be triggered through the relay output of the device, if your device is equipped with one.</li> </ul>	Trap / Email / Relay	Trap, Email

## Event Notifications - Port

### Menu Path: [Diagnostics](#) > [Event Logs and Notifications](#) > [Event Notifications - Port](#)

This page lets you configure notification settings for various events related to your device's physical ports. Each port can be configured independently with different warning methods and severity classifications.

When a port event is triggered, the FAULT LED on your device will also light up if your device has one.

Event Name	Enable	Severity	Registered Action	Registered Port
Port On	Enabled	Notice	Trap, Email	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, G1, G2, G3, G4, G5, G6, G7, G8
Port Off	Enabled	Notice	Trap, Email	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, G1, G2, G3, G4, G5, G6, G7, G8
Port shut down by Port Security	Enabled	Warning	Trap, Email	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, G1, G2, G3, G4, G5, G6, G7, G8
Port shut down by Rate Limit	Enabled	Warning	Trap, Email	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, G1, G2, G3, G4, G5, G6, G7, G8
Port recovered by Rate Limit	Enabled	Warning	Trap, Email	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, G1, G2, G3, G4, G5, G6, G7, G8

UI Setting	Description
<b>Event Name</b>	Shows the name of the port event.
<b>Enable</b>	Shows whether event notifications are enabled for this kind of event.
<b>Severity</b>	Shows the severity assigned to the event. Refer to the <a href="#">Severity Level List</a> for more details.
<b>Registered Action</b>	Shows which action will be taken for this kind of event. <b>Trap:</b> A notification is sent to the Trap server when the event is triggered. <b>Email:</b> A notification is sent to the email server defined in the <a href="#">Email Settings</a> section. <b>Syslog:</b> An event log is recorded to the Syslog server defined in the <a href="#">Syslog</a> section. <b>Relay:</b> A notification is sent through the relay interface, if the device has one, when the event is triggered.
<b>Registered Port</b>	Shows the ports that use the registered action.

## Editing a Port Event Notification

**Menu Path: Diagnostics > Event Logs and Notifications > Event Notifications - Port**

Clicking the **Edit** (✎) icon for a port on the **Diagnostics > Event Logs and Notifications > Event Notifications - Port** page will open this dialog box. This dialog lets you change the notification settings for the selected port.

Click **APPLY** to save your changes.

**Edit This Event Notification**

Event Name  
Port On

---

Enabled \*  
Enabled ▾

---

Registered Action  
Trap, Email ▾

---

Registered Port  
All Ports ▾

CANCEL APPLY



UI Setting	Description	Valid Range	Default Value
<b>Event Name (View-only)</b>	Shows the name of the port event.	(Fixed)	(Fixed)
<b>Enabled</b>	Enable or disable notifications for this event.	Enabled / Disabled	Enabled
<b>Registered Action</b>	Select which actions to take when the event occurs. Multiple actions may be selected. <ul style="list-style-type: none"> <li>• <b>Trap:</b> A notification will be sent to the Trap server.</li> <li>• <b>Email:</b> A notification email will be sent to the email server defined in the <a href="#">Email Settings</a> section.</li> <li>• <b>Relay:</b> An alarm notification will be triggered through the relay output of the device, if your device is equipped with one.</li> </ul>	Trap / Email / Relay	Trap, Email
<b>Registered Port</b>	Specify the ports that will use the registered action.	Drop-down list of ports	All Ports

## Syslog

Syslog allows you to centralize event logs on a dedicated server. This provides a more comprehensive record of network activity compared to the limited storage on an individual device, aiding in troubleshooting and security analysis.

When an event occurs, an event notification can be sent as a syslog UDP packet to specified syslog servers. Each syslog server can be enabled individually.

Administrators can manually import self-signed certificates for syslog client services. However, they should check the root certificate and validity of the signature before importing, according to the organization's security procedures and requirements. After importing a certificate, the administrator should check if the certificate has been revoked and if so, the certificate must be replaced. When the device sends an imported certificate to the syslog server, the syslog server will attempt to verify the certificate against the approved certificate pool on the server.


## Syslog

**Menu Path: [Diagnostics](#) > [Event Logs and Notifications](#) > [Syslog](#)**

This page lets you manage your device's Syslog.

This page includes these tabs:

- General
- Authentication

 **Note**

In order to ensure the security of your network, we recommend the following:


- The encryption algorithm of keys should be selected based on internationally recognized and proven security practices and recommendations.
- The lifetime of certificates generated for syslog client services should be short and in accordance with the organization's security procedures and requirements.
- For security reasons, it is recommended to send event logs to a centralized syslog server for continuous network event monitoring.

## Syslog - General

**Menu Path: [Diagnostics](#) > [Event Logs and Notifications](#) > [Syslog - General](#)**

This page lets you configure the Syslog server settings.

## Syslog Settings

 **Note**

If the syslog server cannot receive previous logs, it is possible that the receiving port of the syslog server is not ready. We suggest you enable the Linkup Delay function to delay the log delivery time.

## Syslog

General

Authentication

Syslog \*  
Disabled ▼

Syslog Server 1 \*  
Disabled ▼

Authentication \*  
Disabled ▼

IP Address/ Domain Na...

UDP Port  
514

1 - 65535

Syslog Server 2 \*  
Disabled ▼

Authentication \*  
Disabled ▼

IP Address/ Domain Na...

UDP Port  
514

1 - 65535

Syslog Server 3 \*  
Disabled ▼

Authentication \*  
Disabled ▼

IP Address/ Domain Na...

UDP Port  
514

1 - 65535

APPLY

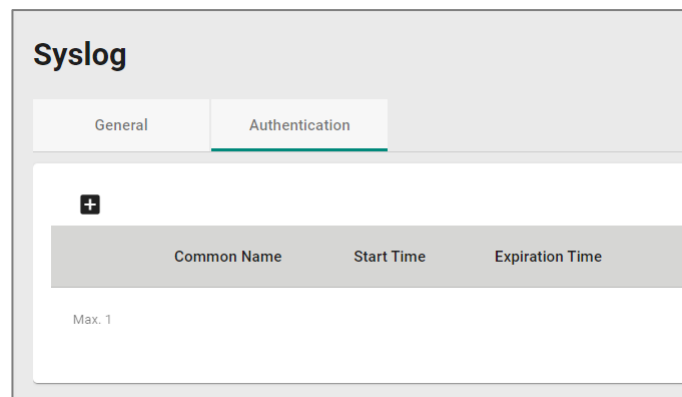
UI Setting	Description	Valid Range	Default Value
<b>Syslog</b>	Enable or disable the syslog logging for your device.	Enabled / Disabled	Disabled
<b>Syslog Server 1/2/3</b>	Enable or disable the specified syslog server.	Enabled / Disabled	Disabled
<b>Authentication</b>	Select whether to authenticate via TLS or disable authentication. <div style="background-color: #f0f0f0; padding: 10px; margin-top: 10px;"> <p><b>Note</b></p> <p>To enable TLS, a certificate and key set must be created first on the "Authentication" tab.</p> </div>	Disabled / TLS	Disabled
<b>IP Address/ Domain Name</b>	Enter the IP address or domain name of the related syslog server.	Valid IP address or domain name	N/A
<b>UDP Port</b>	Specify the UDP port of the related syslog server.	1 to 65535	514

## Syslog - Authentication

### Menu Path: [Diagnostics > Event Logs and Notifications > Syslog - Authentication](#)

This page lets you manually import self-signed certificates for syslog client services.

### Syslog Certificate List



UI Setting	Description
<b>Common Name</b>	Shows the name of the imported certificate and keys.
<b>Start Time</b>	Shows the start time of the imported certificate and keys.
<b>Expiration Time</b>	Shows the expiration time of the imported certificate and keys.

### Adding a Syslog Certificate and Key Set

### Menu Path: [Diagnostics > Event Logs and Notifications > Syslog - Authentication](#)

This page lets you add a client certificate and key for Syslog authentication.




Click **CREATE** to save your changes.

**Add a Certificate and Key Set**

Client Certificate \*

Client Key \*

CA Key \*

UI Setting	Description	Valid Range	Default Value
<b>Client Certificate</b>	Click the folder  icon and select a client certificate file from your computer to import.	N/A	N/A
<b>Client Key</b>	Click the folder  icon and select a client key file from your computer to import.	N/A	N/A
<b>CA Key</b>	Click the folder  icon and select a CA certificate file from your computer to import.	N/A	N/A

## About SNMP Trap/Inform

SNMP Trap allows an SNMP agent to notify the NMS of a significant event.

Your device supports two SNMP modes: **Trap** mode and **Inform** mode.

SNMP Trap/Inform allows your switch to actively send real-time notifications about critical events to network management systems. This proactive alerting can help identify and address network issues faster, improving overall network health and uptime.

### SNMP Trap/Inform

**Menu Path: Diagnostics > Event Logs and Notifications > SNMP Trap/Inform**

This page lets you configure the SNMP Trap/Inform notification feature.

This page includes these tabs:

- General
- SNMP Trap/Inform Accounts

## SNMP Trap/Inform - General

### Menu Path: [Diagnostics > Event Logs and Notifications > SNMP Trap/Inform - General](#)

This page lets you configure the SNMP Trap/Inform settings of your device.

Click **APPLY** to save your changes.

## SNMP Trap/Inform Recipients

Recipient IP Address/ Domain Name	Mode	Trap Community
-----------------------------------	------	----------------

Max. 2

UI Setting	Description
<b>Recipient IP Address/ Domain Name</b>	Shows the IP address or the name of the recipient trap server that will receive notifications.
<b>Mode</b>	Shows the mode used for SNMP notifications.
<b>Trap Community</b>	Shows the community string used for authentication.

## Creating an SNMP Trap/Inform Host

### Menu Path: [Diagnostics > Event Logs and Notifications > SNMP Trap/Inform - General](#)

Clicking the **Add (+)** icon on the **Diagnostics > Event Logs and Notifications > SNMP Trap/Inform - General** page will open this dialog box. This dialog lets you add an SNMP Trap/Inform server.

Click **CREATE** to save your changes and add the new server.

**Create a Host**

Recipient IP Address/ Domain Name \*  
0 / 32

Mode \*  
▼

Trap Community \*  
Minimum 4 characters 0 / 32

CANCEL CREATE

UI Setting	Description	Valid Range	Default Value
<b>Recipient IP Address/ Domain Name</b>	Specify the IP address or the name of the recipient trap server that will receive notifications.	Valid IP address or domain name, 0 to 32 characters	N/A
<b>Mode</b>	<p>Select a mode to use for SNMP notifications. Trap notifications are sent without requesting an acknowledgement from the recipient. Inform notifications will request an acknowledgement from the recipient, and will retry sending the notification if the acknowledgement is not received.</p> <p><b>Trap V1:</b> Use Trap V1 for SNMP notifications.</p> <p><b>Trap V2c:</b> Use Trap V2 for SNMP notifications.</p> <p><b>Inform V2c:</b> Use Inform V2 for SNMP notifications.</p> <p><b>Trap V3:</b> Use Trap V3 for SNMP notifications.</p> <p><b>Inform V3:</b> Use Inform V3 for SNMP notifications.</p>	Trap V1 / Trap V2 / Inform V2 / Trap V3 / Inform V3	N/A
<b>Trap Community</b>	Specify the community string that will be used for authentication.	4 to 32 characters	N/A

## SNMP Inform Settings

### Note

These settings only apply to SNMP Trap/Inform entries that have Trap Mode set to Inform V2c or Inform V3.

UI Setting	Description	Valid Range	Default Value
<b>Inform Retries</b>	Specify the number of times to retry sending an inform notification.	1 to 99	3
<b>Inform Timeout</b>	Specify the amount of time in seconds to wait to wait for an acknowledgement before trying to resend an inform notification.	1 to 300	10

## SNMP Trap/Inform Accounts

**Menu Path: Diagnostics > Event Logs and Notifications > SNMP Trap/Inform - SNMP Trap/Inform Accounts**

This page lets you configure an SNMP trap account for your device.

### Limitations

You can configure up to 1 SNMP trap account.

UI Setting	Description
<b>Username</b>	Shows the username for the SNMP trap account.



UI Setting	Description
<b>Authentication Type</b>	Shows which authentication method is used for the account.
<b>Encryption Method</b>	Shows which encryption method is used for the account.

## Creating an SNMP Trap Account

### Menu Path: [Diagnostics](#) > [Event Logs and Notifications](#) > [SNMP Trap/Inform - SNMP Trap/Inform Accounts](#)

Clicking the **Add** (+) icon on the **Diagnostics > Event Logs and Notifications > SNMP Trap/Inform - SNMP Trap/Inform Accounts** page will open this dialog box. This dialog lets you add an SNMP trap account for your device.

Click **CREATE** to save your changes and add the new account.

**Create an SNMP Trap Account**

Username \*  
Minimum 4 characters 0 / 32

Authentication Type \*  
MD5 Authentication Password \* Minimum 8 characters 0 / 64

Encryption Method \*  
DES Encryption Key \* Minimum 8 characters 0 / 64

CANCEL CREATE

UI Setting	Description	Valid Range	Default Value
<b>Username</b>	Specify a username for the SNMP Trap account.	4 to 32 characters	N/A
<b>Authentication Type</b>	Select which authentication method to use for the account.	None / MD5 / SHA / SHA-256 / SHA-512	None
<b>Authentication Key (if Authentication Type is MD5 or SHA)</b>	Specify an authentication key to use for the account.	8 to 64 characters	N/A
<b>Encryption Method</b>	Disable encryption or select which encryption method to use for the account.	Disabled / DES / AES	Disabled

UI Setting	Description	Valid Range	Default Value
<b>Encryption Key</b> (if Encryption Method is DES or AES)	Specify an encryption password for the account.	8 to 64 characters	N/A

## Deleting an SNMP Trap Account

**Menu Path: Diagnostics > Event Logs and Notifications > SNMP Trap/Inform - SNMP Trap/Inform Accounts**

You can delete an account by clicking its **Delete** (🗑️) icon.

## Editing an SNMP Trap Account

**Menu Path: Diagnostics > Event Logs and Notifications > SNMP Trap/Inform - SNMP Trap/Inform Accounts**

Clicking the **Edit** (✎) icon for an account on the **Diagnostics > Event Logs and Notifications > SNMP Trap/Inform - SNMP Trap/Inform Accounts** page will open this dialog box. This dialog lets you edit the account's settings.

Click **APPLY** to save your changes.

**Edit This SNMP Trap Account**

Username \*  
User1  
Minimum 4 characters 5 / 32

Authentication Type \*  
MD5 CHANGE PASSWORD ⓘ

Encryption Method \*  
DES CHANGE ENCRYPTION KEY

CANCEL APPLY

UI Setting	Description	Valid Range	Default Value
<b>Username</b>	Specify a username for the SNMP Trap account.	4 to 32 characters	N/A

UI Setting	Description	Valid Range	Default Value
<b>Authentication Type</b>	Select which authentication method to use for the account.  Click <b>CHANGE PASSWORD</b> to specify a new authentication password for the account.	None / MD5 / SHA / SHA-256 / SHA-512	None
<b>Encryption Method</b>	Disable encryption or select which encryption method to use for the account.  Click <b>CHANGE ENCRYPTION KEY</b> to specify a new encryption key for the account.	Disabled / DES / AES	Disabled

## About Email Settings

Email Settings lets you configure email notifications for important events. This lets you receive alerts directly in your inbox, providing a convenient way to stay informed about critical network issues.

### Email Settings

**Menu Path:** [Diagnostics](#) > [Event Logs and Notifications](#) > [Email Settings](#)


This page lets you configure your device's email notification settings. You can specify which mail server and account to use, and which email addresses to send email notifications to.

Click **APPLY** to save your changes.

### Email Settings

Server IP Address \*  
0.0.0.0

TCP Port \*  
25  
1 - 65535

Username Password   
0 / 60 0 / 60

TLS \*  
Disabled

Sender Address \*  
admin@localhost.com  
19 / 63

1st Recipient Email Add... 2nd Recipient Email Ad... 3rd Recipient Email Add...  
0 / 63 0 / 63 0 / 63

4th Recipient Email Add... 5th Recipient Email Add...  
0 / 63 0 / 63

**APPLY**

UI Setting	Description	Valid Range	Default Value
<b>Server IP Address</b>	Specify the IP address of the email server.	Valid IP address	N/A
<b>TCP Port</b>	Specify the TCP port of the email server.	1 to 65535	25
<b>Username</b>	Specify the username used to log in to the email server.	0 to 60 characters	N/A
<b>Password</b>	Specify the password used to log in to the email server.	0 to 60 characters	N/A
<b>TLS</b>	Enable or disable TLS (Transport Layer Security).	Enabled / Disabled	Disabled
<b>Sender Address</b>	Specify the sender email address to use for email notifications.	1 to 63 characters	N/A
<b>1st/2nd/3rd/4th/5th Recipient Email Address</b>	Enter an email address to send email notifications to. You can set up to 5 email addresses to send email notifications to.	0 to 63 characters	N/A

## Relay Alarm

**Menu Path:** [Diagnostics](#) > [Event Logs and Notifications](#) > [Relay Alarm](#)

This page lets you see the status of the relay alarm and configure related settings.

### Relay Alarm Cut-Off Status

#### Relay Alarm Cut-Off

↻
🔍 Search

	Name	Status
🔊	Relay	Open

UI Setting	Description
<b>Name</b>	Shows the name of the relay.
<b>Status</b>	Shows whether the relay is currently open or closed.

#### Relay Alarm Settings

Fault LED Display \*

Disabled ▼

APPLY

UI Setting	Description	Valid Range	Default Value
<b>Fault LED Display</b>	Enable or disable whether the fault LED on the device will turn on if the relay alarm is triggered.	Enabled / Disabled	Disabled

# Industrial Application

## Menu Path: Industrial Application

This section lets you manage settings related to specific industrial applications.

This section includes these pages:

- IEC 61850
- Modbus TCP
- EtherNet/IP
- PROFINET

## Industrial Application - User Privileges

Privileges to settings are granted to the different authority levels as follows. Refer to [System > Account Management > User Accounts](#) for more information on user accounts.

Settings	Admin	Supervisor	User
<b>IEC 61850</b>			
<b>MMS</b>	R/W	R/W	R
<b>GOOSE Check</b>	R/W	R/W	R
<b>Modbus TCP</b>	R/W	R/W	R
<b>EtherNet/IP</b>	R/W	R/W	R
<b>PROFINET</b>	R/W	R/W	R

## IEC 61850

### Menu Path: Industrial Application > IEC 61850

This section lets you manage features related to IEC 61850.

This section includes these pages:

- MMS
- GOOSE Check

## MMS

A Manufacturing Message Specification (MMS) server allows Ethernet switches to be controlled, monitored, and managed via a Power SCADA system without the need for any additional network management software. MMS clients can receive data objects sent from a server, such as IEDs receiving data objects from a SCADA, or a SCADA receiving objects from a switch.

This device supports MMS protocol and can act as an MMS server.

### Connecting With an MMS Server

To connect with an MMS server, the following key parameters need to be set:

#### 1. IP Address and Port

- IP Address:** The network address of the MMS server.
- Port Number:** Typically, MMS communication uses **port 102**, though this can vary depending on the server configuration.

#### 2. Remote AP ID (Application Process Identifier)

- A unique identifier used in MMS communication to identify a specific application process on a remote device, such as an MMS server or an IED. The Remote AP ID typically includes the **AP Title** (Application Process Title) and **AE Qualifier** (Application Entity Qualifier). Together, these form the full identifier for the application process on the remote system.

#### 3. Local AP ID (Application Process Identifier)

- A unique identifier used in MMS and OSI-based communication to identify the application process on your client device during communication.

#### 4. OSI Layer Parameters

Since MMS is based on the OSI model, specific OSI parameters are needed:

- PSEL (Presentation Selector)**

- b. **SSEL (Session Selector)**
- c. **TSEL (Transport Selector)** These selectors define how data is routed at different layers of the OSI model.

Parameter	Setting recommended
<b>Remote P Selector</b>	No limitation
<b>Remote S Selector</b>	1
<b>Remote T Selector</b>	No limitation
<b>Local P Selector</b>	1
<b>Local S Selector</b>	1
<b>Local T Selector</b>	1

5. **Authentication Information Such as Certificate-based Authentication** Refer to [MMS - Security](#) for more information about security settings.

## MMS

### Menu Path: Industrial Application > IEC 61850 > MMS

This page configure the device to act as an MMS server.

This page includes these tabs:

- General
- Security

### MMS - General

#### Menu Path: Industrial Application > IEC 61850 > MMS - General

This page lets you configure general MMS server settings for your device.



## MMS Settings

MMS \*  
Disabled ▼

---

IED Name \*  
RKSG4028L34GSHVT

16 / 20

APPLY

UI Setting	Description	Valid Range	Default Value
<b>MMS</b>	Enable or disable the MMS server for your device.	Enabled / Disabled	Disabled
<b>IED Name</b>	Specify the IED name for your device.	0 to 20 characters	The name of your product model

## CID File Settings

You can click the EXPORT CID FILE button to export and download the current CID file.

### CID File Settings

🔍 Search

	Report Control Block	Data Change	Data Update	Quality Change	Integrity	Buffer Time	Integrity Period
	urcbLnkSt	Enabled	Disabled	Disabled	Enabled	1000	5000
	brcbLnkSt	Enabled	Disabled	Disabled	Enabled	1000	5000
	urcbSysSt	Enabled	Disabled	Disabled	Enabled	1000	5000
	brcbSysSt	Enabled	Disabled	Disabled	Enabled	1000	5000

1 – 4 of 4

EXPORT CID FILE

UI Setting	Description
<b>Report Control Block</b>	Shows which report control block the entry is for. <ul style="list-style-type: none"> <li>• <b>urcbLnkSt:</b> Unbuffered Report Control Block Link Status</li> <li>• <b>brcbLnkSt:</b> Buffered Report Control Block Link Status</li> <li>• <b>urcbSysSt:</b> Unbuffered Report Control Block System Status</li> <li>• <b>brcnSysSt:</b> Buffered Report Control Block System Status</li> </ul>
<b>Data Change</b>	Shows whether report generation when there is a data change event is enabled.
<b>Data Update</b>	Shows whether report generation when there is a data update event is enabled.
<b>Quality Change</b>	Shows whether report generation when there is a quality change event is enabled.
<b>Integrity</b>	Shows whether integrity report generation is enabled for the report control block.
<b>Buffer Time</b>	Shows the interval in milliseconds for buffering internal notifications caused by a data change (dchg), quality change (qchg), or data update (dupd) by the report control block for inclusion into a single report.
<b>Integrity Period</b>	Shows the amount of time in milliseconds that should pass between creating integrity reports.

## Edit Report Control Block

### Menu Path: Industrial Application > IEC 61850 > MMS - General

Clicking the **Edit** (✎) icon for a report control block on the **Industrial Application > IEC 61850 > MMS - General** page will open this dialog box. This dialog lets you configure what reports are sent by the report control block.

Click **APPLY** to save your changes.

### Edit urcbLnkSt

Data Change \*  
 Enabled ▼

---

Data Update \*  
 Disabled ▼

---

Quality Change \*  
 Disabled ▼

---

Integrity \*  
 Enabled ▼

---

Buffer Time \*  
 1000  
 1 - 4294967295 ms

Integrity Period \*  
 5000  
 1 - 4294967295 ms

CANCEL APPLY

UI Setting	Description	Valid Range	Default Value
<b>Data Change</b>	<p>Enable or disable report generation when there is a data change event.</p> <p>A data change (dhcg) relates to a change in a value of a data attribute.</p>	Enabled / Disabled	Enabled
<b>Data Update</b>	<p>Enable or disable report generation when there is a data update event.</p> <p>A data-update (dupd) relates to any update or freeze in a value of a data attribute. Compared to a data change, a data update does not require the data attribute value to change; it includes updating a data attribute with the same value.</p>	Enabled / Disabled	Disabled

UI Setting	Description	Valid Range	Default Value
<b>Quality Change</b>	Enable or disable report generation when there is a quality change event.  Quality-change (qchg) relates to a change in the quality value of a data attribute.	Enabled / Disabled	Disabled
<b>Integrity</b>	Enable or disable integrity report generation for the report control block.  When integrity reports are enabled, the report control block will periodically (based on the <b>Integrity Period</b> ) generate a report with the values of all members of the referenced data set.	Enabled / Disabled	Enabled
<b>Buffer Time</b>	Specify the buffer time in milliseconds.  The Buffer Time (BufTm) specifies the interval for buffering internal notifications caused by a data change (dchg), quality change (qchg), or data update (dupd) by the report control block for inclusion into a single report.	1 to 4294967295	1000
<b>Integrity Period</b>	Specify the integrity period in milliseconds.  The attribute Integrity Period (IntgPd) indicates the amount of time that should pass between creating integrity reports.	1 to 4294967295	5000

## MMS - Security

### Menu Path: Industrial Application > IEC 61850 > MMS - General

This page lets you manage CID file certification information.

### T-Profile Certificate Information

T-Profile Certificate Information	
CA Name	moxa
Expiration Date	22000806065419Z

UI Setting	Description
<b>CA Name</b>	Shows the name of the CA for the T-Profile certificate.

UI Setting	Description
<b>Expiration Date</b>	Shows when the T-Profile certificate will expire. The date format is YYYYMMDDhhmmss (year, month, date, hour, minute, second) in UTC time.

## A-Profile Certificate Information

**A-Profile Certificate Information**

CA Name  
**moxa**

Expiration Date  
**22000806065419Z**

UI Setting	Description
<b>CA Name</b>	Shows the name of the CA for the A-Profile certificate.
<b>Expiration Date</b>	Shows when the A-Profile certificate will expire. The date format is YYYYMMDDhhmmss (year, month, date, hour, minute, second) in UTC time.

## T-Profile Security

After making your changes, click **APPLY** to save your changes.

You can click **EXPORT SERVER CA** or **EXPORT SERVER CERTIFICATE** to export and download the file to your local computer.

**T-Profile Security**

T-Profile Security \*

Disabled ▼

---

Import Client CA 📁

---

Import Client Certificate 📄

---

APPLY
EXPORT SERVER CA
EXPORT SERVER CERTIFICATE

UI Setting	Description	Valid Range	Default Value
<b>T-Profile Security</b>	Enable or disable T-Profile security.	Enabled / Disabled	Disabled
<b>Import Client CA</b>	Import a client CA file from your local computer.	Valid CA file	N/A
<b>Import Client Certificate</b>	Import a client certificate file from your local computer	Valid client certificate file	N/A

## A-Profile Security

After making your changes, click **APPLY** to save your changes.

You can click **EXPORT SERVER CA** or **EXPORT SERVER CERTIFICATE** to export and download the file to your local computer.

### A-Profile Security

A-Profile Security \*

Disabled ▼

---

Import Client CA 📁

---

Import Client Certificate 📁

---

APPLY
EXPORT SERVER CA
EXPORT SERVER CERTIFICATE

UI Setting	Description	Valid Range	Default Value
<b>A-Profile Security</b>	Enable or disable A-Profile security.	Enabled / Disabled	Disabled
<b>Import Client CA</b>	Import a client CA file from your local computer.	Valid CA file	N/A
<b>Import Client Certificate</b>	Import a client certificate file from your local computer	Valid client certificate file	N/A

## About GOOSE Check

GOOSE (Generic Object Oriented Substation Event) packet communication is invisible via Ethernet to substation engineers. It is difficult for substation engineers to troubleshoot when GOOSE communication fails through Ethernet.

GOOSE Check is a proprietary Moxa feature which provides various GOOSE attributes in switches, including:

- **GOOSE monitoring table** for users to diagnose communication problems in the system design or system operating phase based on this dynamic information.
- **GOOSE Lock**, which provides an allowlist for GOOSE packets and configurable actions for when when GOOSE packet tampering is detected. Both functions help protect the network from unexpected or invalid GOOSE packets, whether due to incorrect operation or due to an attack.

## GOOSE Check In Depth

GOOSE Check snoops the GOOSE messages passing through the device and shows the communication status of GOOSE messages.

GOOSE Check provides a monitoring table for users to check if GOOSE packets recorded in the monitoring list are consistent with the registered and valid GOOSE streams transmitted over the network.

There are two types of GOOSE entries in the monitoring table:

- **Static:** These are manually defined by user and are kept as records in the monitoring table even if the device reboots or reaches the maximum number of messages.
- **Dynamic:** These entries are automatically learned from ingress GOOSE packets.

## GOOSE Lock In Depth

Enabling GOOSE Lock will lock down the current GOOSE monitoring table, and dynamic entry updates will be stopped. GOOSE entries shown in the table will be treated as an allowlist; ingress GOOSE packets will be dropped if they are not in the current GOOSE monitoring table. The purpose of GOOSE Lock is to protect the network from unregistered or invalid GOOSE packets caused by incorrect operation or attacks.

GOOSE Lock also allows users to specify the action to take when tampered GOOSE packets are detected. Traffic can be allowed after logging the event, the packets can be dropped, or the port can be shut down.

## GOOSE Check

**Menu Path: Industrial Application > IEC 61850 > GOOSE Check**

This page lets you manage the GOOSE check feature for your device.

This page includes these tabs:

- Settings
- Status

### GOOSE Check - Settings

**Menu Path: Industrial Application > IEC 61850 > GOOSE Check - Settings**

This page lets you configure GOOSE check for your device.

### GOOSE Check Settings

UI Setting	Description	Valid Range	Default Value
<b>GOOSE Check</b>	Enable or disable <b>GOOSE Check</b> on the device.	Enabled / Disabled	Disabled



UI Setting	Description	Valid Range	Default Value
<b>GOOSE Lock</b> (If GOOSE Check is Enabled)	Enable or disable <b>GOOSE Lock</b> . When enabled, packets that are not shown in the monitoring table will be dropped.	Enabled / Disabled	Disabled
<b>Tampered Response</b> (If GOOSE Check is Enabled)	Select the action to take if a GOOSE check detects tampering. <ul style="list-style-type: none"> <li>• <b>No Action:</b> No action will be taken for tampered packets, but an event will still be recorded.</li> <li>• <b>Drop:</b> All tampered packets will be dropped. Other traffic will be handled normally.</li> <li>• <b>Port Disable:</b> The relevant port will be disabled.</li> </ul>	No Action / Drop / Port Disable	No Action

### GOOSE Check Monitoring List

+		
<input type="checkbox"/>	APP ID	GOOSE Address (DA)
<input type="checkbox"/>	0x0012	01:0C:CD:01:23:44
Max. 100 of Monitoring table		

UI Setting	Description
<b>APP ID</b>	Shows the GOOSE application identifier for the GOOSE message.
<b>GOOSE Address (DA)</b>	Shows the destination MAC address for the GOOSE message.

## Creating a GOOSE Check Monitoring Entry

**Menu Path: Industrial Application > IEC 61850 > GOOSE Check - Settings**

Clicking the **Add (+)** icon on the **Industrial Application > IEC 61850 > GOOSE Check - Settings** page will open this dialog box. This dialog lets you add a GOOSE check monitoring entry.

Click **CREATE** to save your changes and add the new entry.

### Create Statis GOOSE Entry

APP ID *	GOOSE Address (DA) *
<input type="text"/>	<input type="text" value="01:0C:CD:01:"/>
<small>Hex digits only</small>	

**CANCEL** **APPLY**

UI Setting	Description	Valid Range	Default Value
<b>APP ID</b>	Specify the application identifier for the GOOSE message.	Hex values from 0000 to ffff	N/A
<b>GOOSE Address (DA)</b>	Specify the destination MAC address for the GOOSE message.	01-0C-CD-01-00-00 to 01-0C-CD-01-01-ff	N/A

## Deleting a GOOSE Check Monitoring Entry

**Menu Path: Industrial Application > IEC 61850 > GOOSE Check - Settings**

You can delete an entry by using the checkboxes to select the entries you want to delete, then clicking the **Delete (🗑)** icon.

## GOOSE Check - Status

**Menu Path: Industrial Application > IEC 61850 > GOOSE Check - Status**

This page lets you view the current GOOSE check status of the device.

## Monitoring Table Status

### Monitoring Table Status ↻

GOOSE Lock Status: Disabled      Lock Violation Status: Normal i

UI Setting	Description
<b>GOOSE Lock Status</b>	Shows whether GOOSE lock is enabled.
<b>Lock Violation Status</b>	Shows the current GOOSE lock violation status. <ul style="list-style-type: none"> <li><b>Normal:</b> All detected GOOSE packets are shown in the monitoring table.</li> <li><b>Warning:</b> Unexpected GOOSE packets were detected that are not be shown in the monitoring table.</li> </ul>

## GOOSE Message List

↻
🔍 Search

<input type="checkbox"/>	Type	APP ID	GOOSE Address (DA)	GoCB Name	VLAN ID	Ingress Port	Rx Counter	Status
Items per page: 50    0 of 0    < > >>								

UI Setting	Description
<b>Type</b>	Shows the type of the ingress GOOSE message. <ul style="list-style-type: none"> <li><b>Static:</b> The GOOSE message is defined on this device.</li> <li><b>Dynamic:</b> The GOOSE message is learned from GOOSE packets.</li> </ul>
<b>APP ID</b>	Shows the application identifier of the ingress GOOSE message.
<b>GOOSE Address (DA)</b>	Shows the destination MAC address of the ingress GOOSE message.
<b>GoCB Name</b>	Shows the IED name and GOOSE control block name of ingress GOOSE packets.
<b>VLAN ID</b>	Shows the VLAN ID of the ingress GOOSE message.

UI Setting	Description
<b>Ingress Port</b>	Shows the ingress port of the GOOSE message.
<b>Rx Counter</b>	Shows the packet counter of the ingress GOOSE message.
<b>Status</b>	Shows the communication status of the GOOSE message. <ul style="list-style-type: none"> <li>• <b>Healthy:</b> The communication status is normal.</li> <li>• <b>Timeout:</b> The communication status is abnormal. This GOOSE message did not pass through the device at the correct time.</li> <li>• <b>Tampered:</b> There has been possible packet tampering, because there were GOOSE packets with the same DA and APP ID that came from different source ports, or there were GOOSE packets with the same destination address (DA) and APP ID but different source addresses (SA) that came from different source ports.</li> </ul>

## About Modbus TCP

Modbus is a vendor neutral and commonly used communication protocol to monitor and control industrial automation equipment such as PLCs, sensors, and meters. It is a messaging structure used to establish multiple client-server applications to monitor or program devices.

In order to be fully integrated into industrial systems, Moxa's switches support the Modbus TCP/IP protocol for real-time monitoring in a SCADA system.

## Modbus In Depth

Modbus uses a client/server communication structure that is based on transactions built between client and server. The client requests to read or write server data and the server replies with a message to confirm after completing the instruction.

The message format between client/server at a minimum must include a Protocol Data Unit (PDU) and may also include an Application Data Unit (ADU). The PDU includes function code and data. The function code is the instruction code to read or write server data, and the data includes related parameters for the instruction, such as reading the data in certain addresses.

Moxa switches can act as a Modbus server to reply to Modbus clients like a SCADA.

- Supports up to 5 simultaneous connections from clients

- Closes a connection when there are no Modbus TCP requests received through the connection for 60 seconds
- Closes all Modbus TCP connections within 5 seconds when all switch ports are link down
- Supports Function Code 4 with 16-bit (2-word) data access for read-only information

Data Access Type		Function Code	Function Name
<b>Word access (16-bit access)</b>	Physical input registers	4	Read input registers

Information that clients can request:

- System information
- Port information
- Packet information
- Redundancy information

Refer to [Modbus Data Map and Information](#) for detailed data maps and more information.

## Modbus TCP

**Menu Path: Industrial Application > Modbus TCP**

This page lets you enable Modbus TCP functionality for your device.

Modbus TCP \*

Disabled ▼

---

**APPLY**

UI Setting	Description	Valid Range	Default Value
<b>Modbus TCP</b>	Enable or disable Modbus TCP for your device. This allows your device to be detected in a Modbus TCP network.	Enabled / Disabled	Enabled

## About EtherNet/IP

EtherNet/IP is a commercial-off-the-shelf industrial protocol based on IEEE 802.3 combined with the TCP/IP Suite managed by the ODVA association.

EtherNet/IP follows the OSI model and implements Common Industrial Protocol (CIP). CIP is an object-oriented protocol and ODVA defining several communication objects in CIP. Moxa switches support a subset of these objects as a device role in EtherNet/IP ecosystem.

EtherNet/IP is widely adopted as a standard communication protocol among devices in industrial ecosystems. For example, Rockwell Automation uses EtherNet/IP as the standard protocol for their Logix controllers over Ethernet networks. Moxa switches also provide EtherNet/IP features to integrate with the Rockwell system and monitor the status of switches and PLCs, making switches a part of the Rockwell system.

## EtherNet/IP

**Menu Path: Industrial Application > EtherNet/IP**

This page lets you enable EtherNet/IP functionality for your device.



The screenshot shows a configuration window for EtherNet/IP. At the top, it says "EtherNet/IP \*". Below that is a dropdown menu currently set to "Disabled". At the bottom of the window is a green button labeled "APPLY".

UI Setting	Description	Valid Range	Default Value
<b>EtherNet/IP</b>	Enable or disable EtherNet/IP for your device. This allows your device to be detected in an EtherNet/IP network.	Enabled / Disabled	Disabled

## About PROFINET

PROFINET is an open industrial Ethernet communication protocol proposed by PROFIBUS & PROFINET International (PI), an organization dedicated to industrial communication standards. It is fully compatible with Ethernet as defined in the IEEE standard and has

been included in the IEC 61158 and IEC 61784 standards since 2003. PROFINET enables the implementation of applications for production and process automation, safety applications, and a wide range of drive technology.

## Node Roles

PROFINET includes three node roles:

- **IO-Controllers:** IO-Controllers control the automated tasks of IO-Devices and collect relevant information for users.
- **IO-Supervisors:** IP-supervisors are usually PC-based software and allow users to configure parameters and diagnose the status of individual modules. IO-Supervisors do not participate directly in routine operations.
- **IO-Devices:** IO-Devices are controlled and monitored by IO-Controllers, and may include several modules or submodules. A device model describes all field devices in terms of their possible technical and functional features. A device model is specified by the DAP (Device Access Point) and the defined modules for a particular device family. A DAP is the access point for communication with the Ethernet interface and the processing program.
  - This Moxa device is a PROFINET I/O device.

## GSD Files

General Station Description (GSD) files for the field devices to be configured are required for system engineering. A GSD is an XML-based file that describes the properties and functions of the PROFINET I/O field devices. It contains data relevant for engineering as well as for data exchange with the device.

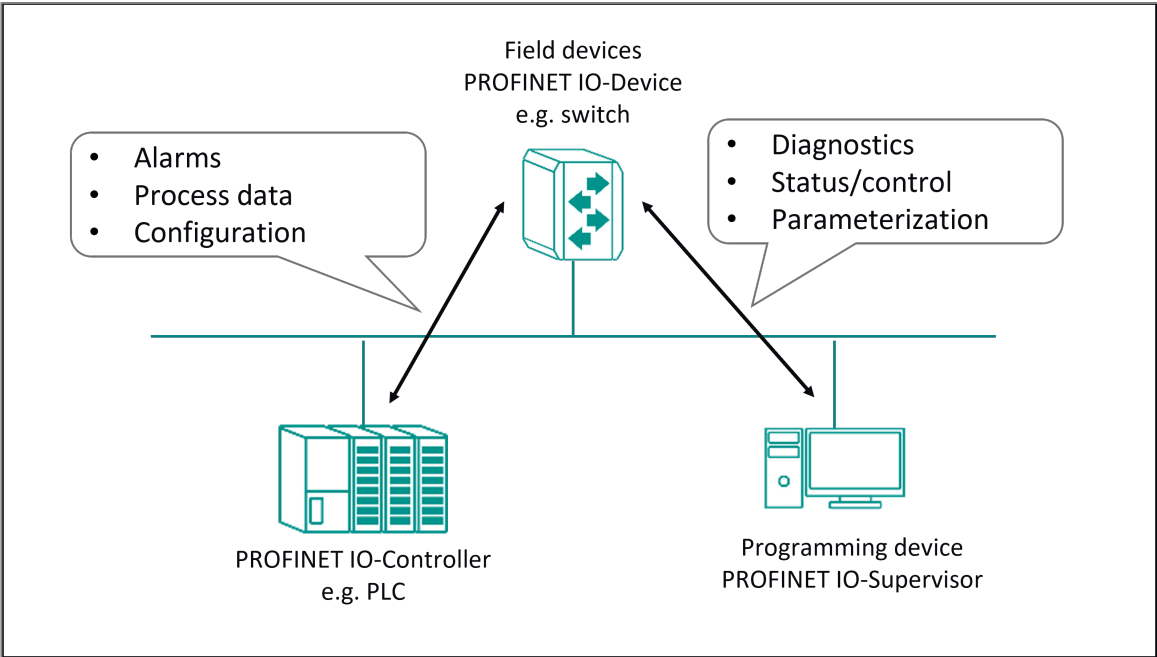
You can download the field device GSD file for this device from the Moxa website.

## PROFINET In Depth

PROFINET IO operates through IO-Supervisors, IO-Controllers, and IO-Devices, and can fulfill various levels of requirements through periodic and aperiodic data transmission.

IO-Devices are standalone units designed to transmit real-time (RT) information to IO-Controllers (PLCs). They do not attempt to communicate directly with other devices.

Instead, they directly provide their real-time (cyclic) data to an IO-Controller and may send some alarm or diagnostic (acyclic) data to an IO-Supervisor.



**PROFINET Attributes and TIA Portal Integration**

**Addressing of I/O Data in PROFINET I/O Based on Slot and Sub-Slots**

The concept of the Moxa PROFINET switch is shown in the table below. In this structure, each switch port represents one sub-slot.

Slot 0					
Sub Slot 0	Sub Slot 0X8000	Sub Slot 0X8001	Sub Slot 0X8002	Sub Slot 0X8003	...
DAP	IO Data	Port 1	Port 2	Port 3	



## Manufacturer Information

Each PROFINET device is addressed based on a MAC address. This address is unique worldwide. The company code (bits 47 to 24) can be obtained from the IEEE Standards Department free of charge. This part is called the OUI (organizationally unique identifier).

MOXA OUI Table:

Bit Value 47..24						Bit Value 23..0					
0	0	0	2	2	9	x	x	x	x	x	x
Company Code (OUI)						Consecutive Number					

## PROFINET Attributes

Combined with the General Station Description (GSD) file, an IO-Controller can quickly configure settings for different devices and seamlessly replace devices. A PROFINET IO General Station Description (GSD) file is a description of an IO-Device provided by the device manufacturer. The contents of the GSD file contain configuration information, parameters, modules, diagnostics and alarms, and vendor and device identification.

### PROFINET Cyclic I/O Data Table

- **Device Status**

Category	Direction	Byte	Bit	Name	Description
<b>Device</b>	Input	0	0	Device status	0 is failed status, 1 is OK.
			1	Power 1	0 is unavailable, 1 is OK
			2	Power 2	0 is unavailable, 1 is OK
<b>Device</b>	Input	1		Reserved for redundancy protocol	

- **Port Status**

Category	Direction	Byte	Bit	Name	Description
<b>Port</b>	Input	0	0	Port 1 Connection	0 is not connected, 1 is connected

Category	Direction	Byte	Bit	Name	Description
			1	Port 2 Connection	0 is not connected, 1 is connected
			2	Port 3 Connection	0 is not connected, 1 is connected
			{ ... }	{ ... }	{ ... }
			7	Port 8 Connection	0 is not connected, 1 is connected
		1	1	Port 9 Connection	0 is not connected, 1 is connected
			2	Port 10 Connection	0 is not connected, 1 is connected
		{ ... }	{ ... }	{ ... }	{ ... }
		7	7	Port 64 Connection	0 is not connected, 1 is connected
<b>Port</b>	Input	8	0	Port channel 1 Connection	0 is not connected, 1 is connected
			1	Port channel 2 Connection	0 is not connected, 1 is connected
		{ ... }	{ ... }	{ ... }	{ ... }
		11	7	Port channel 32 Connection	0 is not connected, 1 is connected

You can monitor these attributes in the TIA Portal.

Monitoring Device I/O Cyclic Data and Port I/O Cyclic Data in the TIA Portal:

The screenshot shows a 'Watch table\_1' window in TIA Portal. The table contains 20 rows of data with columns for Name, Address, Display format, Monitor value, Modify value, Comment, and Tag comment. The 'Monitor value' column shows values like 16#00, TRUE, FALSE, and 16#403D.

	Name	Address	Display format	Monitor value	Modify value	Comment	Tag comment
1	"Cyclic Data - Device Status - All"	%I80	Hex	16#00			
2	"Cyclic Data - Device Status"	%I0.0	Bool	TRUE			
3	"Cyclic Data - Power 1"	%I0.1	Bool	TRUE			
4	"Cyclic Data - Power 2"	%I0.2	Bool	FALSE			
5	"Cyclic Data - Port Status - All"	%I02	Hex	16#403D			
6	"Cyclic Data - Port 1"	%I2.0	Bool	FALSE			
7	"Cyclic Data - Port 2"	%I2.1	Bool	FALSE			
8	"Cyclic Data - Port 3"	%I2.2	Bool	FALSE			
9	"Cyclic Data - Port 4"	%I2.3	Bool	FALSE			
10	"Cyclic Data - Port 5"	%I2.4	Bool	FALSE			
11	"Cyclic Data - Port 6"	%I2.5	Bool	FALSE			
12	"Cyclic Data - Port 7"	%I2.6	Bool	TRUE			
13	"Cyclic Data - Port 8"	%I2.7	Bool	FALSE			
14	"Cyclic Data - Port 9"	%I3.0	Bool	FALSE			
15	"Cyclic Data - Port 10"	%I3.1	Bool	FALSE			
16	"Cyclic Data - Port 11"	%I3.2	Bool	FALSE			
17	"Cyclic Data - Port 12"	%I3.3	Bool	FALSE			
18	"Cyclic Data - Port 13"	%I3.4	Bool	TRUE			
19	"Cyclic Data - Port 14"	%I3.5	Bool	TRUE			
20							

## PROFINET I/O Parameters

Moxa defines comprehensive PROFINET I/O parameters for more flexible settings and monitoring. The attributes are readable or writable. PROFINET I/O parameters use PROFINET acyclic data to achieve communication in the network. You can use the TIA Portal tool or engineering deployment software to edit it.

There are 2 categories of parameters, including Device Status and Device Alarms.

The following tables provide parameter information:

- r/w: Read and Write
- ro: Read Only

### Device Status

Byte	Name	Access	Value	Description
0	PLC Connection Status	ro	0	Unavailable
			1	Connection failure
			2	OK
1	PLC Connection Status	ro	0	Unavailable
			1	Device detect fault
			2	OK
2	Power 1 Status	ro	0	Unavailable

Byte	Name	Access	Value	Description
			1	Power 1 fails
			2	OK
<b>3</b>	Power 2 Status	ro	0	Unavailable
			1	Power 2 fails
			2	OK
<b>4</b>	DI 1 Status	ro	0	Unavailable
			1	Closed
			2	Open
<b>5</b>	DI 2 Status	ro	0	Unavailable
			1	Closed
			2	Open
<b>6</b>	Spanning Tree Config	ro	0	Unavailable
			1	Disable
			2	RSTP
			3	MSTP
<b>7</b>	Turbo Ring v2 Config	ro	0	Unavailable
			1	Disable
			2	Enable
<b>8</b>	Turbo Ring v2 Ring 1 Config	ro	0	Unavailable
			1	Disable
			2	Enable
<b>9</b>	Turbo Ring v2 Ring 1 Status	ro	0	Unavailable
			1	Disable

Byte	Name	Access	Value	Description
			2	Broken
			3	Healthy
<b>10</b>	Turbo Ring v2 Ring 2 Config	ro	0	Unavailable
			1	Disable
			2	Enable
<b>11</b>	Turbo Ring v2 Ring 2 Status	ro	0	Unavailable
			1	Connection failure
			2	OK
<b>12</b>	Turbo Chain Config	ro	0	Unavailable
			1	Disable
			2	Head
			3	Member
			4	Tail
<b>13</b>	Dual Homing Config	ro	0	Unavailabe
			1	Disable
			2	Primary path always first
			3	Maintain current path
			4	Primary path sensing recovery
<b>14</b>	Media Redundancy Protocol Config	ro	0	Unavailable
			1	Disable
			2	Enable
<b>15</b>	Media Redundancy Protocol Manager Status	ro	0	Unavailable
			1	Disable

Byte	Name	Access	Value	Description
			2	Initiation
			3	Awaiting Connection
			4	Primary Ring Port Link Up
			5	Ring Open
			6	Ring Closed
<b>16</b>	Media Redundancy Protocol Client Status	ro	0	Unavailable
			1	Connection failure
			2	OK
			3	Awaiting Connection
			4	Data Exchange Idle
			5	Pass Through
			6	Data Exchange
			7	Pass Through Idle

## Device Alarms

These parameters control PROFINET Alarm functions. A PROFINET alarm is a message which is sent from the switch to a PLC immediately once the event is triggered.

Byte	Name	Access	Value	Description	Default Value
<b>0</b>	Status Alarm	rw	0	Do not send any alarms	0: No alarms
			1	Send alarm if any status change	
<b>1</b>	Power Alarm 1	rw	0	Do not send power failed alarm	0: No alarms
			1	Send alarm if power supply 1 fails	
<b>2</b>	Power Alarm 2	rw	0	Do not send power failed alarm	0: No alarms

Byte	Name	Access	Value	Description	Default Value
			1	Send alarm if power supply 2 fails	
<b>3</b>	RSTP Topology Changed Alarm	rw	0	Do not send RSTP topology changed alarm	0: No alarms
			1	Send alarm if RSTP topology changed	
<b>4</b>	MSTP Topology Changed Alarm	rw	0	Do not send MSTP topology changed alarm	0: No alarms
			1	Send alarm if MSTP topology changed	
<b>5</b>	Turbo Ring V2 Ring Broken	rw	0	Do not send TR2 broken alarm	0: No alarms
			1	Send alarm if TR2 is broken	
<b>6</b>	MRP Ring Broken	rw	0	Do not send MRP broken alarm	0: No alarms
			1	Send alarm if MRP is broken	

## Reset to Factory Mode

The following table is the list of Reset to Factory Modes supported by MOXA:

Reset to Factory Modes	Mode Description	Action taken
<b>Mode 0 - Factory Default Mode</b>	Original Factory Reset	Cleans all configured settings including PROFINET
<b>Mode 1</b>	Reset Application data	Resets I&M data and the alarm configuration of devices and ports
<b>Mode 2</b>	Reset Communication parameter	Resets Device Name to " " and IP to 0.0.0.0
<b>Mode 3</b>	Reset Engineering parameter	Performs Mode 1, 2, and clears all configured settings

# PROFINET

## Menu Path: Industrial Application > PROFINET

This page lets you manage PROFINET functionality on your device.

This page includes these tabs:

- Settings
- Status

## PROFINET - Settings

### Menu Path: Industrial Application > PROFINET - Settings

This page lets you configure PROFINET for your device.

PROFINET \*  
Disabled

Interface Name \*  
vlan1

Device Name i

The maximum characters for a label is 63 0 / 240

APPLY

UI Setting	Description	Valid Range	Default Value
<b>PROFINET</b>	Enable or disable PROFINET for your device. This allows your device to be detected in a PROFINET network.	Enabled / Disabled	Disabled
<b>Interface Name</b>	Select which interface to use for PROFINET.	Drop-down list of interfaces	vlan1




UI Setting	Description	Valid Range	Default Value
<b>Device Name</b>	<p>Specify the labels you want to use to identify this device in PROFINET.</p> <p>Multiple labels can be entered, separated by a period(.). For example, "moxa.rks-g4028" can be entered to specify "moxa" and "rks-g4028" as separate labels.</p> <div style="background-color: #f0f0f0; padding: 10px; border: 1px solid #ccc;"> <p><b>Note</b></p> <p>PROFINET labels are subject to the following naming rules:</p> <ul style="list-style-type: none"> <li>• Labels only support the following characters: a-z, 0-9, and dashes (-)</li> <li>• Labels must be 1 to 63 characters long</li> <li>• Labels cannot be in IP address format</li> <li>• Labels cannot start with "port" followed by 3 or more digits</li> <li>• Labels cannot start or end with a period (.) or a dash (-)</li> </ul> </div>	<p>1 to 63 characters for each label</p> <p>0 to 240 characters total</p>	N/A

## PROFINET - Status

### Menu Path: Industrial Application > PROFINET - Status

This page lets you monitor the status of PROFINET on your device.

Protocol Information 	
Interface Name	Link Status
vlan1	Disconnected
Device Name	---

UI Setting	Description
<b>Interface Name</b>	Shows the interface used for PROFINET.
<b>Device Name</b>	Shows the user-defined labels for the device.
<b>Link Status</b>	Shows the PROFINET link status.

## Chapter 4

---

# Appendix

# CIP EtherNet/IP Objects

Several communication objects are defined in CIP (Common Industrial Protocol).

Moxa switches support the following objects for PLCs and SCADA systems to monitor:

Definition	CIP Object Name	Class ID
<b>ODVA</b>	Identity Object	0x01
	Message Router	0x02
	Assembly	0x04
	Connection Manager Object	0x06
	Base Switch Object	0x51
	Port Object	0xF4
	TCP/IP Interface Object	0xF5
	Ethernet Link Object	0xF6
	LLDP Management Object	0x109
	LLDP Data Table Object	0x10A
<b>MOXA</b>	Moxa Networking Object (Vendor Specific)	0x404

The supported attributes and services of the above objects are introduced in the table below, including Each object should consist of Class ID, Instance ID, Attribute ID, and Service Code. The supported attributes and services of the above objects are introduced in the following chapters, including the access rules, data type, and description for each attribute.

## Identity Object

The Class code of Identity object is **0x01**.

There is **one** instance of this object in our product. It stores the information of the production and the device. The following tables summarize the class attribute, instance attributes, and service code.

## Class Attribute List

Attr ID	Access Rule	Name	Data Type	Description
1	Get	Revision	UINT (16)	Revision of this object
2	Get	Max Instance	UINT (16)	Maximum instance number of an object currently created in this class level of the device
3	Get	Number of Instances	UINT (16)	Number of object instances currently created in this class level of the device.
6	Get	Maximum ID Number Class Attributes	UINT (16)	Maximum class attribute ID number implemented in the device
7	Get	Maximum ID Number Instance Attributes	UINT (16)	Maximum instance attribute ID number implemented in the device

## Instance Attribute List

Attr ID	Access Rule	Name	(Struct.)	Data Type	Description
1	Get	Vendor ID		UINT (16)	<b>0x3DF</b> , the vendor ID of Moxa is 991.
2	Get	Device Type		UINT (16)	<b>0x2C</b> , "Managed Ethernet Switch".
3	Get	Product Code		UINT (16)	Please refer to Product Code Table.
4	Get	Revision		(Struct.)	Revision of the item the Identity Object represents.
			Major	USINT (8)	The structure member, major. The value zero is not valid. If product version is 0, using 1-base.
			Minor	USINT (8)	The structure member, minor. The value zero is not valid. If product version is 0, using 1-base.
5	Get	Status		WORD (16)	Summary status of the device.
6	Get	Serial Number		UDINT (32)	The serial number of each device.
7	Get	Product Name		SHORT_STRING	The product model of the Moxa switch. Maximum length is 32 characters.

Attr ID	Access Rule	Name	(Struct.)	Data Type	Description
15	Get/Set	Assigned Name		STRINGI	Switch device's host name.
17	Get/Set	Geographic Location		STRINGI	The assigned switch location.

The Identity Object Instance supports the following CIP Common services:

## Common Service List

Service Code	Implementation Class	Implementation Instance	Service Name	Description
				0x01 ✓ ✓ Get_Attributes_All Returns the contents of all attributes of the class.
0x0E	✓	✓	Get_Attribute_Single	Used to read an object instance attribute.
0x10		✓	Get_Attribute_Single	Used to write an object instance attribute.
0x05		✓	Reset	Invokes the reset service for the device.
0x18		✓	Get_Member	Returns the content of a selected member of an attribute.

# Message Router Object

The Class code of Message Router Object is **0x02**. The object within a node that distributes messaging requests to the appropriate application objects.

The supported messaging connections are as the following:

- Explicit Messaging
- Unconnected Messaging
- Implicit messaging

When using the UCMM to establish an explicit messaging connection, the target application object is the Message Router object.

## Class Attribute List

Attr ID	Access Rule	Name	Data Type	Description
1	Get	Revision	UINT (2)	Revision of this object

## Instance Attribute List

Attr ID	Access Rule	Name	(Struct.)	Data Type	Description
1	Get	Object_list		(Struct.)	A list of supported objects
			Number	UINT (16)	Number of supported classes in the classes array
			Classes	Array of UINT (16)	List of supported class codes
2	Get	Number Available		UINT (16)	Maximum number of connections supported
3	Get	Number Active		UINT (16)	Number of connections currently used by system components
4	Get	Active Connections		Array of UINT (16)	A list of the connection IDs of the currently active connections

## Common Service List

Service Code	Implementation Class	Implementation Instance	Service Name	Description
0x0E		✓	Get_Attribute_Single	Used to read an object instance attribute.

## Assembly Object

The Moxa switch support **static** assembly object for CIP I/O messaging.

The Class code is **0x04**.

There are three instances of this object as the following.

	Instance Number	Size (32 bit)
<b>Output</b>	1	18
<b>Input</b>	50	16
<b>Configuration</b>	100	10

The **Input** means the data is produced by switch which includes the information and status report to the originator for monitoring. The **Output** means the data is generated by the originator (remote host) and is consumed by switch.

## Class Attribute List

Attr ID	Access Rule	Name	Data Type	Description
1	Get	Revision	UINT (16)	Revision of this object

## Instance Attribute List

Attr ID	Access Rule	Name	Data Type	Description
3	Get/Set	Data	Array of BYTE	The implicit messaging content

Attr ID	Access Rule	Name	Data Type	Description
4	Get	Size	UINT (16)	Number of bytes in Attr. 3

## Common Service List

Service Code	Implementation Class	Implementation Instance	Service Name	Description
0x0E	✓	✓	Get_Attribute_Single	Used to read an object instance attribute.
0x10		✓	Set_Attribute_Single	Used to modify an object instance attribute

For the definition of the I/O messaging, see the following table for details.

## I/O Assembly Data Attribute Formats

Direction	Instance	Byte	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
<b>Input</b>	1	0	Power Source Status (Least Significant Byte)							
		1	Power Source Status (Most Significant Byte)							
		2-5	Global Link Status DWORD 0							
		6-9	Global Link Status DWORD 1							
		10-13	Global Link Status DWORD 2							
		14-17	Global Link Status DWORD 3							
<b>Output</b>	50	0-3	Global Admin State DWORD 0							
		4-7	Global Admin State DWORD 1							
		8-11	Global Admin State DWORD 2							
		12-15	Global Admin State DWORD 3							



# Mapping I/O Assembly Data Attribute

## Components

The following table indicates the I/O assembly Data attribute mapping for the Managed Ethernet Switch device.

Service Code	Class	Instance	Attribute Name	Attribute Number
<b>Power Source Status</b>	Base Switch Object	1	Power Source	4
<b>Global Admin State</b>			Global Port Admin State	7
<b>Global Link Status</b>			Global Port Link Status	8

## Connection Manager Object

The class code of Connection Manager Object is **0x06**. The Connection Manager Object allocates and manages the internal resources associated with both I/O and Explicit Messaging connections. There is one instance of this object. The supported connection trigger type is cyclic and change of state (COS).

The instance attribute list is introduced as the following.

## Class Attribute List

Attr ID	Access Rule	Name	Data Type	Description
<b>1</b>	Get	Revision	UINT (16)	Revision of this object.

## Instance Attribute List

Attr ID	Access Rule	Name	Data Type	Description
1	Get/Set	Open Requests	UINT(16)	<p>Number of Forward_Open service requests received.</p> <p>A device may reject a set request to this attribute, using General Status Code <b>0x09</b> (Invalid Attribute Value), if the attribute value sent is not zero.</p> <p>(Vol1_3.33 3-5.2 Instance Attributes)</p>

## Common Service List

Service Code	Implementation Class	Implementation Instance	Service Name	Description
0x0e	✓	✓	Get_Attribute_Single	Used to read an object instance attribute.
0x10		✓	Set_Attribute_Single	Used to modify an object instance attribute.
0x4E		✓	Forward_Close	Closes a connection.
0x54		✓	Forward_Open	Opens a connection. Maximum data size is 511 bytes.

## QoS Object

The QoS Object provides a means to configure certain QoS-related behaviors in EtherNet/IP devices. The class code of QoS Object is 0x48. The following table defines the default DSCP mappings for EtherNet/IP.

Traffic Type	CIP Priority	DSCP	CIP Traffic Usage (Recommended)
CIP class 0/1	Urgent (3)	55	CIP Motion

Traffic Type	CIP Priority	DSCP	CIP Traffic Usage (Recommended)
	Scheduled (2)	47	Safety I/O I/O
	High (1)	43	I/O
	Low (0)	31	No recommendation at present
<ul style="list-style-type: none"> <li>• CIP UCMM</li> <li>• CIP class 2/3</li> <li>• All other EtherNet/IP Encapsulation messages</li> </ul>	All	27	CIP messaging

## Class Attribute

Attr ID	Access Rule	Name	Data Type	Description
1	Get	Revision	UINT (16)	Revision of this object.

## Instance Attribute

Attr ID	Access Rule	Name	Data Type	Description
4	Get/Set	DSCP Urgent	USINT (8)	CIP transport class 0/1 messages with Urgent priority
5	Get/Set	DSCP Scheduled	USINT (8)	CIP transport class 0/1 messages with Scheduled priority
6	Get/Set	DSCP High	USINT (8)	CIP transport class 0/1 messages with High priority
7	Get/Set	DSCP Low	USINT (8)	CIP transport class 0/1 messages with Low priority
8	Get/Set	DSCP Explicit	USINT (8)	CIP UCMM CIP transport class 2/3 All other EtherNet/IP encapsulation messages

Any change to the value of the above attributes will only take effect after the device is restarted.

## Common Service

Service Code	Implementation Class	Implementation Instance	Service Name	Description
0x0E	✓	✓	Get_Attribute_Single	Used to read an object instance attribute.
0x10		✓	Set_Attribute_Single	Used to modify an object instance attribute.

## Base Switch Object

The class code of Base Switch Object is 0x51. The Base Switch Object provides the CIP application-level interface and basic status information for a Managed Ethernet switch device.

Devices shall implement no more than one instance of the Base Switch Object.

## Class Attribute List

Attr ID	Access Rule	Name	Data Type	Description
1	Get	Revision	UINT (16)	Revision of this object. The current value assigned to this is 1.

## Instance Attribute List

Attr ID	Access Rule	Name	Data Type	Description
1	Get	Device Up Time	UDINT (32)	Time since device was powered up.
2	Get	Total Port Count	UDINT (32)	Number of physical available ports.
3	Get	System Firmware Version	SHORT_STRING	Human readable representation of System Firmware Version. Maximum length is 32 characters.

Attr ID	Access Rule	Name	Data Type	Description
4	Get	Power Source	WORD (16)	<p>Status of switch power source.</p> <p>Bits 0-1: State of the Power Source 1.</p> <p>00 = Not Present (Power source not present in switch)</p> <p>01 = Not Powered (Power source present but not powered)</p> <p>10 = Faulted(internal) (Power source present but faulted)</p> <p>11 = Powered and ok (Power source present, powered, and OK)</p> <p>Bits 2-3: State of the Power Source 2. The values are same as bits 0-1.</p> <p>Bits 4-5: State of the Power Source 3. The values are same as bits 0-1.</p> <p>Bits 6-7: State of the Power Source 4. The values are same as bits 0-1.</p> <p>Bits 8-9: State of the Power Source 5. The values are same as bits 0-1.</p> <p>Bits 10-11: State of the Power Source 6. The values are same as bits 0-1.</p> <p>Bits 12-13: State of the Power Source 7. The values are same as bits 0-1.</p> <p>Bits 14-15: State of the Power Source 8. The values are same as bits 0-1.</p>
5	Get	Port Mask Size	UINT (16)	Number of DWORDs in port array attributes. Minimum = 4, supporting 128 ports.
6	Get	Existing Port	ARRAY OF DWORD (32)	<p>Switch existing port.</p> <p>0 = Port Absent</p> <p>1 = Port Present</p>
7	Get	Global Port Admin State	ARRAY OF DWORD (32)	<p>Port Admin State.</p> <p>0 = Port Disabled</p> <p>1 = Port Enabled</p>
8	Get	Global Port Link Status	ARRAY OF DWORD (32)	<p>Ports Link Status.</p> <p>0 = Link Inactive (Down)</p> <p>1 = Link Active (Up)</p> <p>Bit 0-31: Port 0-31 Link status.</p>

## Common Service List

Service Code	Implementation Class	Implementation Instance	Service Name	Description
0x0E	✓	✓	Get_Attribute_Single	Used to read an object instance attribute.

## Port Object

The port object represents the underlying interface of CIP which is EtherNet/IP.

The class code is **0xf4**. There is one instance of this object.

The instance attribute "**Port Type**" identifies the CIP adaptation.

## Class Attribute List

Attr ID	Access Rule	Name	(Struct.)	Data Type	Description
1	Get	Revision		UINT (16)	Revision of this object
2	Get	Max Instance		UINT (16)	Maximum instance number of an object currently created in this class level of the device
3	Get	Number of Instances		UINT (16)	Number of object instances currently created at this class level of the device.
8	Get	Entry Port		UINT (16)	Returns the instance of the Port Object that describes the port through which this request entered the device.
9	Get	Port Instance Info	Port Type	UINT (16)	Enumerates the type of port.
			Port Number	UINT (16)	CIP port number associated with this port

## Instance Attribute List

Attr ID	Access Rule	Name	(Struct.)	Data Type	Description
1	Get	Port Type		UINT (16)	Enumerates the type of port. 4 = EtherNet/IP.
2	Get	Port Number		UINT (16)	CIP port number associated with this port.  (Values 0-1 are reserved and cannot be used)
3	Get	Link Object	Path Length	UINT (16)	Number of 16 bit words in the following path.
			Link Path	Padded EPATH	Logical path segments that identify the object for this port.
4	Get	Port Name		SHORT_STRING	Vendor assigned name of the communications interface.  The value is always "EIP Port".
5	Get	Port Type Name		SHORT_STRING	String which names the port type.  If Port Type value is 4 (EtherNet/IP), its associated Port Type Name is "EtherNet/IP". The value is always "EtherNet/IP".
7	Get	Node Address		Padded EPATH	This is a single Port Segment containing the Port Number of this port and the Link Address of this device on this port.
9	Get	Port Key		Packed EPATH	The electronic key of the chassis this port is attached to. This attribute shall be limited to format 4 of the Logical Electronic Key segment.  The Vendor ID, Device Type, Product Code, Major Revision and Minor Revision fields shall not be 0.  The Compatibility field shall be 0 (indicating match).
10	Get	Port Routing Capabilities		DWORD (32)	Bit string that defines the routing capabilities of this port.

## Common Service List

Service Code	Implementation Class	Implementation Instance	Service Name	Description
0x0E	✓	✓	Get_Attribute_Single	Used to read an object instance attribute.

## TCP/IP Interface Object

The Class code of TCP/IP Interface object is **0xf5**. The TCP/IP Interface Object provides the mechanism to configure a device's TCP/IP network interface. Examples of configurable items include the device's IP Address, Network Mask, and Gateway Address. There is **one** instance of this object.

The following tables summarize the attributes of this object.

### Class Attribute List

Attr ID	Access Rule	Name	Data Type	Description
1	Get	Revision	UINT (16)	Revision of this object.
2	Get	Max Instance	UINT (16)	Maximum instance number of an object currently created in this class level of the device
3	Get	Number of Instances	UINT (16)	Number of object instances currently created at this class level of the device
6	Get	Maximum ID Number Class Attributes	UINT (16)	Maximum class attribute ID number implemented in the device.
7	Get	Maximum ID Number Instance Attributes	UINT (16)	Maximum instance attribute ID number implemented in the device.



## Instance Attribute List

Attr ID	Access Rule	Name	(Struct.)	Data Type	Description
1	Get	Status		DWORD (32)	Interface status 0 = The Interface Configuration attribute has not been configured. 1 = The Interface Configuration attribute contains valid configurations obtained from BOOTP, DHCP or non-volatile storage.
2	Get	Configuration Capability		DWORD (32)	Indicates the device's support for optional network configuration capability. 0 = Device is not capable. 1 = Device is capable. Bit map of capability flags: Bit 0: BOOTP Client Bit 1: DNS Client Bit 2: DHCP Client Bit 3: DHCP-DNS Update Bit 4: Configuration Settable
3	Get/Set	Configuration Control		DWORD (32)	Interface control flags Bit map of control flags: Bit 0 to 3: Startup Configuration 0 = The device shall use the interface configuration values previously stored (for example, in non-volatile memory or via hardware switches). 1 = The device shall obtain its interface configuration values via BOOTP. 2 = The device shall obtain its interface configuration values via DHCP upon start-up. 3 to15 = Reserved.
4	Get	Physical Link Object	Path Size	UINT (16)	Size of Path
			Path	Padded EPATH	Logical segments identifying the physical link object
5	Get/Set	Interface	IP Address	UDINT (32)	The device's IP address

Attr ID	Access Rule	Name	(Struct.)	Data Type	Description
		Configuration	Network Mask	UDINT (32)	The device's network mask
			Gateway Address	UDINT (32)	Default gateway address
			Name Server	UDINT (32)	Primary name server
			Name Server2	UDINT (32)	Secondary name server
			Domain Name	STRING	Default domain name. Maximum length is 48 characters. A length of 0 shall indicate no Domain Name is configured. Set Domain Name is not supported in Moxa switch.
<b>6</b>	Get/Set	Host Name		STRING	Host name. ASCII characters. Maximum length is 64 characters.
<b>13</b>	Get/Set	Encapsulation Inactivity Timeout		UNIT (16)	Number of seconds of inactivity before TCP connection is closed. Default = 120 0 = Disable timeout 1-3600 = timeout in seconds

The TCP/IP Object Instance supports the following CIP Common services:

## Common Service List

Service Code	Implementation Class	Implementation Instance	Service Name	Description
<b>0x01</b>	✓	✓	Get_Attributes_All	Returns the contents of all attributes of the class
<b>0x0E</b>	✓	✓	Get_Attribute_Single	Used to read an object instance attribute
<b>0x10</b>		✓	Set_Attribute_Single	Used to modify an object instance attribute

## Ethernet Link Object

The Class code of Ethernet Link object is **0xf6** (Defined in CIP Vol2, 5-4). For each switch port, there is an instance of this class. The following table shows the mapping of instance number and the switch port number.

Instance Number	Mapping to
<b>0</b>	Ethernet Link class
<b>1</b>	1st switch port
<b>2</b>	2nd switch port
<b>3</b>	3rd switch port
...	...

The following tables summarize the attributes of the Ethernet Link object.

There are some vendor specific attributes in the table (Starting from attribute Id 100).

### Class Attribute List

Attr ID	Access Rule	Name	Data Type	Description
<b>1</b>	Get	Revision	UINT (16)	Revision of this object
<b>2</b>	Get	Max Instance	UINT (16)	Maximum instance number of an object currently created in this class level of the device
<b>3</b>	Get	Number of Instances	UINT (16)	Number of object instances currently created in this class level of the device
<b>6</b>	Get	Maximum ID Number Class Attributes	UINT (16)	Maximum class attribute ID number implemented in the device.
<b>7</b>	Get	Maximum ID Number Instance Attributes	UINT (16)	Maximum instance attribute ID number implemented in the device.
<b>100</b>	Get	Moxa-specific Revision	UINT (16)	Revision of Moxa specific attributes and services for Linux platform switch. The current value assigned is 1.

## Instance Attribute List

Attr ID	Access Rule	Name	(Struct.)	Data Type	Description
1	Get	Interface Speed		UDINT (32)	Interface speed currently in use. The scale of the attribute is in Mbps.  (Speed in Mbps, e.g., 0, 10, 100, 1000, etc.)
2	Get	Interface Flags		DWORD (32)	Refer to the Interface Flags table.
3	Get	Physical Address		ARRAY of 6 USINT (8)	Interface's MAC layer address.
4	Get	Interface Counters	In Octets	UDINT (32)	Octets received on the interface.
			In Ucast Packets	UDINT (32)	Unicast packets received on the interface.
			In NUcast Packet	UDINT (32)	Non-unicast packets received on the interface.
			In Discards	UDINT (32)	Inbound packets received on the interface but are discarded.
			In Errors	UDINT (32)	Inbound packets that contain Errors (does not include In Discards).
			In Unknown Protos	UDINT (32)	Inbound packets with unknown protocol.
			Out Octets	UDINT (32)	Octets sent on the interface.
			Out Ucast Packets	UDINT (32)	Unicast packets sent on the interface.

Attr ID	Access Rule	Name	(Struct.)	Data Type	Description
			Out NUcast Packets	UDINT (32)	Non-unicast packets sent on the interface.
			Out Discards	UDINT (32)	Discarded outbound packets.
			Out Errors	UDINT (32)	Outbound packets that contain errors.
5	Get	Media Counters	Alignment Errors	UDINT (32)	Received frames that are not an integral number of octets in length.
			FCS Errors	UDINT (32)	Received frames that do not pass the FCS check.
			Single Collisions	UDINT (32)	Successfully transmitted frames which experienced exactly one collision.
			Multiple Collisions	UDINT (32)	Successfully transmitted frames which experienced more than one collision.
			SQE Test Errors	UDINT (32)	Number of times the SQE test error message is generated.
			Deferred Transmissions	UDINT (32)	Frames for which the first transmission attempt is delayed because the medium is busy.

Attr ID	Access Rule	Name	(Struct.)	Data Type	Description
			Late Collisions	UDINT (32)	Number of times a collision is detected later than 512 bit times into the transmission of a packet.
			Excessive Collisions	UDINT (32)	Frames for which transmission fails due to excessive collisions.
			MAC Transmit Errors	UDINT (32)	Frames for which transmission fails due to an internal MAC sublayer transmit error.
			Carrier Sense Errors	UDINT (32)	Times that the carrier sense condition was lost or never asserted when attempting to transmit a frame.
			Frame Too Long	UDINT (32)	Received frames that exceed the maximum permitted frame size.
			MAC Receive Errors	UDINT (32)	Frames for which reception on an interface fails due to an internal MAC sublayer receive error.
<b>6</b>	Get/Set	Interface Control		(Struct.)	Configuration for physical Interface.

Attr ID	Access Rule	Name	(Struct.)	Data Type	Description
			Control Bits	WORD (16)	Bit 0: Auto-Negotiate Value 0: Force Value 1: Auto-Nego Bit 1: Forced Duplex Mode Value 0: half duplex Value 1: full duplex Bit 2 to 15: Reserved, all zero
			Forced Interface Speed	UINT (16)	Speed at which the interface shall be forced to operate. Speed in Mbps (10, 100, 1000, etc.)
<b>10</b>	Get	Interface Label		SHORT_STRING	Port description. Maximum length is 64 characters.
<b>11</b>	Get	Interface Capability		(Struct.)	Indication of capabilities of the interface

Capability Bits	DWORD (32)	<p>Interface capabilities, other than speed/duplex.</p> <p>Bit 0: Manual Setting Requires Reset</p> <p>Value 0: The device automatically applies changes made to the Interface Control attribute (#6). Doesn't require a reset in order for changes to take effect..</p> <p>Value 1: The device doesn't automatically apply changes made to the Interface Control attribute (#6). Require a reset in order for changes to take effect.</p> <p>Bit 1: Auto-Negotiate</p> <p>Value 0: Not support AN</p> <p>Value 1: Support AN</p> <p>Bit 2: Auto-MDIX</p> <p>Value 0: Not support auto MDIX</p> <p>Value 1: Support auto MDIX</p> <p>Bit 3: Manual Speed/Duplex</p> <p>Value 0: Not support manual setting of speed/duplex.</p> <p>Value 1: Supports manual setting of speed/duplex via the Interface Control attribute (#6)</p> <p>Bit 4 to 31: Reserved, all zero</p>
-----------------	------------	---



Attr ID	Access Rule	Name	(Struct.)	Data Type	Description
		Speed/Duplex Options		(Struct.)	Indicates speed/duplex pairs supported in the Interface Control attribute.
12	Get	HC Interface Counters	HCInOctets	ULINT (64)	The total number of octets received on the interface.  This counter is a 64-bit version of In Octets.
			HCInUcastPkts	ULINT (64)	Unicast packets received on the interface.  This counter is a 64-bit version of In Ucast Packets.
			HCInMulticastPkts	ULINT (64)	Multicast packets received on the interface.
			HCInBroadcastPkts	ULINT (64)	Broadcast packets received on the interface.
			HCOctets	ULINT (64)	Octets sent on the interface.  This counter is a 64-bit version of Out Octets.
			HCOUcastPkts	ULINT (64)	Unicast packets sent on the interface.  This counter is a 64-bit version of Out Ucast Packets.
			HCOMulticastPkts	ULINT (64)	Multicast packets sent on the interface.
			HCOBroadcastPkts	ULINT (64)	Broadcast packets sent on the interface.

Attr ID	Access Rule	Name	(Struct.)	Data Type	Description
13	Get	HC Media Counters	HCStatsAlignmentErrors	ULINT (64)	<p>Frames received that are not an integral number of octets in length and do not pass the FCS check.</p> <p>This counter is a 64-bit version of Alignment Errors.</p>
			HCStatsFCSErrors	ULINT (64)	<p>Frames received that are an integral number of octets in length but do not pass the FCS check. This counter is a 64-bit version of FCS Errors.</p>
			HCStatsInternalMacTransmitErrors	ULINT (64)	<p>Frames for which transmission fails due to an internal MAC sublayer transmit error.</p> <p>This counter is a 64-bit version of MAC Transmit Errors.</p>
			HCStatsFrameTooLongs	ULINT (64)	<p>Frames received that exceed the maximum permitted frame size.</p> <p>This counter is a 64-bit version of Frame Too Long Errors.</p>
			HCStatsInternalMacReceiveErrors	ULINT (64)	<p>Frames for which reception on an interface fails due to an internal MAC sublayer receive error.</p> <p>This counter is a 64-bit version of MAC Receive Errors.</p>

Attr ID	Access Rule	Name	(Struct.)	Data Type	Description
			HCStatsSymbolErrors	ULINT (64)	Number of times there was an invalid data symbol on the media when a valid carrier was present.
100	Get	Port State		USINT (8)	Switch port state. Value 1 = Disable Value 2 = Blocking Value 3 = Listening Value 4 = Learning Value 5 = Forwarding Value 6 = Broken
101	Get	Media Type		STRING	Port media type.
102	Get/Set	Traffic Storm Control		USINT (8)	Traffic storm control enable. 0 = Disabled 1 = Enabled Bit 0: Broadcast storm control Bit 1: Multicast storm control Bit 2: DLF storm control
103	Get/Set	Port On event		USINT (8)	Registered port for port on event notification. 0 = Unregistered. 1 = Registered.
104	Get/Set	Port Off event		USINT (8)	Registered port for port off event notification. 0 = Unregistered. 1 = Registered.

Attr ID	Access Rule	Name (Struct.)	Data Type	Description
105	Get/Set	Port shut down by Port Security event	USINT (8)	Registered port for port shut down by Port Security event notification. 0 = Unregistered. 1 = Registered.
106	Get/Set	Port shut down by Rate Limit event	USINT (8)	Registered port for port shut down by Rate Limit event notification. 0 = Unregistered. 1 = Registered.
107	Get/Set	Port recovered by Rate Limit event	USINT (8)	Registered port for port recovered by Rate Limit event notification. 0 = Unregistered. 1 = Registered.
108	Get/Set	Fiber Check Warning	USINT (8)	Registered port for fiber check warning event notification. 0 = Unregistered. 1 = Registered.

## Interface Flags

Bit(s)	Called	Definition
0	Link Status	0 indicates an inactive link; 1 indicates an active link.
1	Half/Full Duplex	0 indicates half duplex; 1 indicates full duplex.

Bit(s)	Called	Definition
2-4	Negotiation Status	<p>Indicates the status of link auto-negotiation</p> <p>0 = Auto-negotiation in progress.</p> <p>1 = Auto-negotiation and speed detection failed. Using default values for speed and duplex. Default values are product-dependent; recommended defaults are 10Mbps and half duplex.</p> <p>2 = Auto negotiation failed but detected speed. Duplex was defaulted. Default value is product-dependent; recommended default is half duplex.</p> <p>3 = Successfully negotiated speed and duplex.</p> <p>4 = Auto-negotiation not attempted. Forced speed and duplex.</p>
5	Manual Setting Requires Reset	0 indicates the interface can activate changes to link parameters (auto-negotiate, duplex mode, interface speed) automatically. 1 indicates the device requires a Reset service be issued to its Identity Object in order for the changes to take effect.
6	Local Hardware Fault	0 indicates the interface detects no local hardware fault; 1 indicates a local hardware fault is detected. The meaning of this is product-specific. For example, an AUI/MII interface might detect no transceiver attached, or a radio modem might detect no antenna attached. In contrast to the soft, possibly self-correcting nature of the Link Status being inactive, this is assumed a hard-fault requiring user intervention.
7~31	Reserved.	Shall be set to zero

The Ethernet Link Object Instance supports the following CIP common services:

## Common Service List

Service Code	Implementation Class	Implementation Instance	Service Name	Description
0x0E	✓	✓	Get_Attribute_Single	Used to read an object instance attribute
0x10		✓	Set_Attribute_Single	Used to modify an object instance attribute

# LLDP Management Object

The LLDP Management Object contains administrative information for the LLDP protocol. Only one instance of the LLDP Management Object shall be implemented. The class code of LLDP Management Object is 0x109.

## Class Attribute List

Attr ID	Access Rule	Name	Data Type	Description
1	Get	Revision	UINT (16)	Revision of this object. The current value assigned to this value is 1.

## Instance Attribute List

Attr ID	Access Rule	Name	(Struct.)	Data Type	Description	
1	Get/Set	LLDP Enable		(Struct.)		
				LLDP Enable Array Length	USINT (16)	Number of bits defined in the LLDP Enable Array member of this structure.
				LLDP Enable Array	Array of BYTE (8)	Bit 0 : Global Enable 0 = LLDP Tx & Rx Disabled 1 = LLDP Tx & Rx Enabled Bit 1-N : Port Tx Enable 0 = LLDP Tx Disabled 1 = LLDP Tx Enabled Bit >N : Reserved Shall be zero and ignored.
2	Get/Set	msgTxInterval		USINT (16)	Message Transmission Interval for LLDP frames. 0 = Reserved 1 - 3600 = Transmit interval (sec.) 3601 - 65535 = Reserved Recommended default value is 30. Note : <b>MOXA real supported transmit interval range is 5-32768.</b>	

Attr ID	Access Rule	Name	(Struct.)	Data Type	Description
3	Get/Set	msgTxHold		USINT (8)	Message Transmission Multiplier for LLDP Frames 0 = Reserved 1 - 100 = Transmission Multiplier 101 - 255 = Reserved Recommended default value is 4. Note : <b>MOXA real supported transmit hold time multiplier range is 2-10.</b>
4	Get	LLDP Datastore		WORD (16)	An indication of the retrieval methods for the LLDP database supported by the device. Bit: 0 = LLDP Data Table Object 1 = SNMP 2 = NETCONF YANG 3 = RESTCONF YANG 4 - 15 = Reserved At least one of bits 0 & 1 are required.
5	Get	Last Change		UDINT (32)	The value of sysUpTime taken the last time any entry in the local LLDP database (ignoring TTL) changed.

## Common Service List

Service Code	Implementation Class	Implementation Instance	Service Name	Description
0x0E	✓	✓	Get_Attribute_Single	Used to read an object instance attribute
0x10		✓	Set_Attribute_Single	Used to modify an object instance attribute

## LLDP Data Table Object

The LLDP Data Table object displays a record of all adjacent LLDP implementing devices that are currently active according to the receive state machine of the LLDP protocol. An instance of the LLDP Data Table object shall be implemented per adjacent device detected. Instances shall be created and removed as neighboring devices change. The

same instance number should be maintained for each neighboring device until the next power cycle of the device implementing this object.

The class code of the LLDP Data Table Object is 0x10A.

## Common Attribute List

Attribute ID	Access Rule	Name	Data Type	Description
1	Get	Revision	UINT (16)	Revision of this object. The current value is 1.
2	Get	Max Instance	UINT (16)	Maximum instance number of an object currently created in this class level of the device.
3	Get	Number of Instances	UINT (16)	Number of object instances currently created in this class level of the device.
6	Get	Maximum ID Number Class Attributes	UINT (16)	Maximum class attribute ID number implemented in the device.
7	Get	Maximum ID Number Instance Attributes	UINT (16)	Maximum instance attribute ID number implemented in the device.

## Instance Attribute

Attribute ID	Access Rule	Name	(Struct.)	Data Type	Description
1	Get	Ethernet Link Instance Number		UINT (16)	The physical Ethernet port the LLDP frame populating this instance was received on.  0 = Unknown  1-65535 = Ethernet Link Object (0xF6) Instance Number



Attribute ID	Access Rule	Name	(Struct.)	Data Type	Description
2	Get	MAC Address		ETH_MAC_ADDR	<p>The MAC address will be set by the first occurrence of a MAC ID that exists in the following list:</p> <ol style="list-style-type: none"> <li>1. The CIP MAC Address (TLV Type = 127, Subtype = 2)</li> <li>2. The Chassis ID (TLV Type = 1) only if subtype = 2</li> <li>3. The Port ID (TLV Type = 2) only if subtype = 3</li> <li>4. All zero</li> </ol>
3	Get	Interface Label		SHORT_STRING	<p>The Interface Label will be a maximum of 64 characters. It is set by the first occurrence of an interface label that exists in the following list:</p> <ol style="list-style-type: none"> <li>1. The CIP Interface Label (TLV Type = 127, Subtype = 1)</li> <li>2. The Chassis ID (TLV Type = 1) only if subtype = 6</li> <li>3. The Port ID (TLV Type = 2) only if subtype = 5</li> <li>4. A null string</li> </ol>
4	Get	Time to Live		UINT (16)	<p>The number of seconds the neighboring information is to be considered valid.</p> <p>0 = Reserved 1-65535 = Time To Live (in seconds)</p>
5	Get	System Capabilities TLV		(Struct.)	<p>A structure that contains bitmaps of both the supported and enabled capabilities of the neighboring device.</p>

Attribute ID	Access Rule	Name	(Struct.)	Data Type	Description
			System Capabilities	WORD (16)	<p>The capabilities which the neighboring device supports based on currently loaded firmware.</p> <p>Bit 0 : Other            Bit 1 : Repeater            Bit 2 : Bridge            Bit 3 : Access Point            Bit 4 : Router            Bit 5 : Telephone            Bit 6 : DOCSIS Cable Device            Bit 7 : End Station            Bit 8 : C-VLAN component            Bit 9 : S-VLAN component            Bit 10 : Two-port MAC Relay Component            Bit 11-15 : Reserved by IEEE</p> <p><b>Note :</b>  <b>EtherNet/IP Bridged multiport neighboring devices are expected to assert high bits 0 &amp; 2.</b></p>

Attribute ID	Access Rule	Name	(Struct.)	Data Type	Description
			Enabled Capabilities	WORD (16)	<p>The capabilities currently enabled on the neighboring device.</p> <p>Bit 0 : Other            Bit 1 : Repeater            Bit 2 : Bridge            Bit 3 : Access Point            Bit 4 : Router            Bit 5 : Telephone            Bit 6 : DOCSIS Cable Device            Bit 7 : End Station            Bit 8 : C-VLAN component            Bit 9 : S-VLAN component            Bit 10 : Two-port MAC Relay Component            Bit 11-15 : Reserved by IEEE</p> <p><b>Note :</b></p> <p><b>EtherNet/IP Bridged multiport neighboring devices are expected to assert high bits 0 &amp; 2.</b></p>
6	Get	IPv4 Management Address		(Struct.)	The IPv4 management addresses of the neighboring device.
			Management Address Count	USINT	0-255 = Number of received Management Address TLV's from this neighbor.
			Management Address	ARRAY of UDINT (32)	<p>The IP address shall be set to a valid Class A, B, or C address.</p> <p>And shall not be set to all zeros or the loopback address (127.0.0.1).</p>
7	Get	CIP Identification		(Struct.)	<p>The CIP Identification TLV of the neighboring device, if present.</p> <p>Set by the CIP Identification TLV (TLV Type = 127, Subtype = 09), if present. Otherwise 0</p>
			Vendor ID	UINT (16)	Vendor ID

Attribute ID	Access Rule	Name	(Struct.)	Data Type	Description
			Device Type	UINT (16)	Device Type
			Product Code	UINT (16)	Product Code
			Major Revision	BYTE (8)	Major Revision
			Minor Revision	USINT (8)	Minor Revision
			CIP Serial Number	UDINT (32)	Serial Number – Shall not be zero 0.
<b>8</b>	Get	Additional Ethernet Capabilities		(Struct.)	A TLV for Ethernet Preemption Support from the neighboring device.  Set by the Additional Ethernet Capabilities TLV (TLV type = 127, Subtype 7), if present. Otherwise, 0.
			Preemption Support	BOOL (8)	Allows a link partner to know if preemption is supported on the link.  0 = Not Supported 1 = Supported
			Preemption Status	BOOL (8)	Allows a link partner to know if preemption is enabled on the link.  0 = Not Enabled 1 = Enabled
			Preemption Active	BOOL (8)	Allows a link partner to know if link preemption has passed embedded verification.  0 = Not Active 1 = Active

Attribute ID	Access Rule	Name	(Struct.)	Data Type	Description
			Additional Fragment Size	USINT (8)	The number of octets that must be transmitted of a frame before preemption occur. 0 = 64 octets 1 = 128 octets 2 = 192 octets 3 = 256 octets 4-255 = Reserved
9	Get	Last Change		UDINT (32)	The value of sysUpTime taken the last time any attribute in this instance changed.

## Common Service

Service Code	Implementation Class	Implementation Instance	Service Name	Description
0x01	✓		Get_Attribute_All	Returns the contents of all attributes of the class.
0x0E	✓	✓	Get_Attribute_Single	Used to read an object instance attribute.
0x11	✓		Find_Next_Object_Instance	Causes the specified Class to search for and return a list of instances ID's of existing instances of the LLDP Data Table Object.

## Moxa Networking Object (Vendor Specific)

The Moxa Networking object includes system information and status.

It can also be used to do the device diagnostic & configuration through explicit messaging.

The class code is **0x404**.

### Class Attribute List

Attr ID	Access Rule	Name	Data Type	Description
1	Get	Revision	UINT (16)	Revision of this objec

### Instance Attribute List

Attr ID	Access Rule	Name	Data Type	Description
1	Get	CPU Usage	USINT (8)	Percentage of CPU usage (0 to100)

Attr ID	Access Rule	Name	Data Type	Description
2	Get	L2 Redundancy	USINT (8)	<p>Bit mask of device roles.</p> <p>Bit 0: RSTP 0 = RSTP Disabled 1 = RSTP Enabled</p> <p>Bit 1: MSTP 0 = MSTP Disabled 1 = MSTP Enabled</p> <p>Bit 2: Turbo Chain 0 = Turbo Chain Disabled 1 = Turbo Chain Enabled</p> <p>Bit 3: Turbo Ring v2 0 = Turbo Ring v2 Disabled 1 = Turbo Ring v2 Enabled</p> <p>Bit 4: Dual-Homing 0 = Dual-Homing Disabled 1 = Dual-Homing Enabled</p> <p>Bit 5: MRP 0 = MRP Disabled 1 = MRP Enabled</p>
3	Get	Relay Alarm Status	USINT (8)	<p>Relay alarm event-triggered status.</p> <p>When Relay alarm is triggered, value will change from 0x0 to 0x1.</p> <p>Bit 0: Relay (MGMT-Relay) alarm status 0 = Alarm doesn't trigger. 1 = Alarm triggered.</p> <p>Bit 1: PWR1-Relay alarm status 0 = Alarm doesn't trigger. 1 = Alarm triggered.</p> <p>Bit 2: PWR2-Relay alarm status 0 = Alarm doesn't trigger. 1 = Alarm triggered.</p>

Attr ID	Access Rule	Name	Data Type	Description
4	Get/Set	Cold Start	USINT (8)	<p>System cold start event notification.</p> <p>(Bit 1 should call MGMT-Relay if device support more than 1 relay. Bit 2-3 depends on device supported relay number.)</p> <p>Bit 0: Event notification enable.</p> <p>0 = Disabled 1 = Enabled</p> <p>Bit 1: Relay (MGMT-Relay) alarm enable.</p> <p>0 = Disabled 1 = Enabled</p> <p>Bit 2: PWR1-Relay alarm enable.</p> <p>0 = Disabled 1 = Enabled</p> <p>Bit 3: PWR2-Relay alarm enable.</p> <p>0 = Disabled 1 = Enabled</p>
5	Get/Set	Warm Start	USINT (8)	<p>System warm start event notification.</p> <p>(Bit 1 should call MGMT-Relay if device support more than 1 relay. Bit 2-3 depends on device supported relay number.)</p> <p>Bit 0: Event notification enable.</p> <p>0 = Disabled 1 = Enabled</p> <p>Bit 1: Relay (MGMT-Relay) alarm enable.</p> <p>0 = Disabled 1 = Enabled</p> <p>Bit 2: PWR1-Relay alarm enable.</p> <p>0 = Disabled 1 = Enabled</p> <p>Bit 3: PWR2-Relay alarm enable.</p> <p>0 = Disabled 1 = Enabled</p>



Attr ID	Access Rule	Name	Data Type	Description
6	Get/Set	Redundant port health check fail	USINT (8)	<p>Redundant port health check fail.</p> <p>(Bit 1 should call MGMT-Relay if device support more than 1 relay. Bit 2-3 depends on device supported relay number.)</p> <p>Bit 0: Event notification enable.</p> <p>0 = Disabled 1 = Enabled</p> <p>Bit 1: Relay (MGMT-Relay) alarm enable.</p> <p>0 = Disabled 1 = Enabled</p> <p>Bit 2: PWR1-Relay alarm enable.</p> <p>0 = Disabled 1 = Enabled</p> <p>Bit 3: PWR2-Relay alarm enable.</p> <p>0 = Disabled 1 = Enabled</p>
7	Get/Set	PD over current	USINT (8)	<p>Current of port has exceeded the safety limit.</p> <p>(Bit 1 should call MGMT-Relay if device support more than 1 relay. Bit 2-3 depends on device supported relay number.)</p> <p>Bit 0: Event notification enable.</p> <p>0 = Disabled 1 = Enabled</p> <p>Bit 1: Relay (MGMT-Relay) alarm enable.</p> <p>0 = Disabled 1 = Enabled</p> <p>Bit 2: PWR1-Relay alarm enable.</p> <p>0 = Disabled 1 = Enabled</p> <p>Bit 3: PWR2-Relay alarm enable.</p> <p>0 = Disabled 1 = Enabled</p>

Attr ID	Access Rule	Name	Data Type	Description
8	Get/Set	PD no response	USINT (8)	<p>The device connected to this port is not responding to the PD failure check.</p> <p>(Bit 1 should call MGMT-Relay if device support more than 1 relay. Bit 2-3 depends on device supported relay number.)</p> <p>Bit 0: Event notification enable. 0 = Disabled 1 = Enabled</p> <p>Bit 1: Relay (MGMT-Relay) alarm enable. 0 = Disabled 1 = Enabled</p> <p>Bit 2: PWR1-Relay alarm enable. 0 = Disabled 1 = Enabled</p> <p>Bit 3: PWR2-Relay alarm enable. 0 = Disabled 1 = Enabled</p>
9	Get/Set	Power On	USINT (8)	<p>Power supply on event notification.</p> <p>(Bit 1 should call MGMT-Relay if device support more than 1 relay. Bit 2-3 depends on device supported relay number.)</p> <p>Bit 0: Event notification enable. 0 = Disabled 1 = Enabled</p> <p>Bit 1: Relay (MGMT-Relay) alarm enable. 0 = Disabled 1 = Enabled</p> <p>Bit 2: PWR1-Relay alarm enable. 0 = Disabled 1 = Enabled</p> <p>Bit 3: PWR2-Relay alarm enable. 0 = Disabled 1 = Enabled</p>

Attr ID	Access Rule	Name	Data Type	Description
10	Get/Set	Power Off	USINT (8)	<p>Power supply off event notification.</p> <p>(Bit 1 should call MGMT-Relay if device support more than 1 relay. Bit 2-3 depends on device supported relay number.)</p> <p>Bit 0: Event notification enable.</p> <p>0 = Disabled 1 = Enabled</p> <p>Bit 1: Relay (MGMT-Relay) alarm enable.</p> <p>0 = Disabled 1 = Enabled</p> <p>Bit 2: PWR1-Relay alarm enable.</p> <p>0 = Disabled 1 = Enabled</p> <p>Bit 3: PWR2-Relay alarm enable.</p> <p>0 = Disabled 1 = Enabled</p>
11	Get/Set	DI on	USINT (8)	<p>Digital input on event notification.</p> <p>(Bit 1 should call MGMT-Relay if device support more than 1 relay. Bit 2-3 depends on device supported relay number.)</p> <p>Bit 0: Event notification enable.</p> <p>0 = Disabled 1 = Enabled</p> <p>Bit 1: Relay (MGMT-Relay) alarm enable.</p> <p>0 = Disabled 1 = Enabled</p> <p>Bit 2: PWR1-Relay alarm enable.</p> <p>0 = Disabled 1 = Enabled</p> <p>Bit 3: PWR2-Relay alarm enable.</p> <p>0 = Disabled 1 = Enabled</p>

Attr ID	Access Rule	Name	Data Type	Description
12	Get/Set	DI off	USINT (8)	<p>Digital input off event notification.</p> <p>(Bit 1 should call MGMT-Relay if device support more than 1 relay. Bit 2-3 depends on device supported relay number.)</p> <p>Bit 0: Event notification enable.</p> <p>0 = Disabled 1 = Enabled</p> <p>Bit 1: Relay (MGMT-Relay) alarm enable.</p> <p>0 = Disabled 1 = Enabled</p> <p>Bit 2: PWR1-Relay alarm enable.</p> <p>0 = Disabled 1 = Enabled</p> <p>Bit 3: PWR2-Relay alarm enable.</p> <p>0 = Disabled 1 = Enabled</p>
13	Get/Set	Port On	USINT (8)	<p>Port link up event notification.</p> <p>(Bit 1 should call MGMT-Relay if device support more than 1 relay. Bit 2-3 depends on device supported relay number.)</p> <p>Bit 0: Event notification enable.</p> <p>0 = Disabled 1 = Enabled</p> <p>Bit 1: Relay (MGMT-Relay) alarm enable.</p> <p>0 = Disabled 1 = Enabled</p> <p>Bit 2: PWR1-Relay alarm enable.</p> <p>0 = Disabled 1 = Enabled</p> <p>Bit 3: PWR2-Relay alarm enable.</p> <p>0 = Disabled 1 = Enabled</p>

Attr ID	Access Rule	Name	Data Type	Description
14	Get/Set	Port Off	USINT (8)	<p>Port link down event notification.</p> <p>(Bit 1 should call MGMT-Relay if device support more than 1 relay. Bit 2-3 depends on device supported relay number.)</p> <p>Bit 0: Event notification enable.</p> <p>0 = Disabled 1 = Enabled</p> <p>Bit 1: Relay (MGMT-Relay) alarm enable.</p> <p>0 = Disabled 1 = Enabled</p> <p>Bit 2: PWR1-Relay alarm enable.</p> <p>0 = Disabled 1 = Enabled</p> <p>Bit 3: PWR2-Relay alarm enable.</p> <p>0 = Disabled 1 = Enabled</p>
15	Get/Set	Port shutdown by Port Security	USINT (8)	<p>Port shutdown by Port Security event notification.</p> <p>(Bit 1 should call MGMT-Relay if device support more than 1 relay. Bit 2-3 depends on device supported relay number.)</p> <p>Bit 0: Event notification enable.</p> <p>0 = Disabled 1 = Enabled</p> <p>Bit 1: Relay (MGMT-Relay) alarm enable.</p> <p>0 = Disabled 1 = Enabled</p> <p>Bit 2: PWR1-Relay alarm enable.</p> <p>0 = Disabled 1 = Enabled</p> <p>Bit 3: PWR2-Relay alarm enable.</p> <p>0 = Disabled 1 = Enabled</p>

Attr ID	Access Rule	Name	Data Type	Description
16	Get/Set	Port shutdown by Rate Limit	USINT (8)	<p>Port shutdown by Rate Limit event notification. (Bit 1 should call MGMT-Relay if device support more than 1 relay. Bit 2-3 depends on device supported relay number.)</p> <p>Bit 0: Event notification enable. 0 = Disabled 1 = Enabled</p> <p>Bit 1: Relay (MGMT-Relay) alarm enable. 0 = Disabled 1 = Enabled</p> <p>Bit 2: PWR1-Relay alarm enable. 0 = Disabled 1 = Enabled</p> <p>Bit 3: PWR2-Relay alarm enable. 0 = Disabled 1 = Enabled</p>
17	Get/Set	Port recovered by Rate Limit	USINT (8)	<p>Port recovered by Rate Limit event notification. (Bit 1 should call MGMT-Relay if device support more than 1 relay. Bit 2-3 depends on device supported relay number.)</p> <p>Bit 0: Event notification enable. 0 = Disabled 1 = Enabled</p> <p>Bit 1: Relay (MGMT-Relay) alarm enable. 0 = Disabled 1 = Enabled</p> <p>Bit 2: PWR1-Relay alarm enable. 0 = Disabled 1 = Enabled</p> <p>Bit 3: PWR2-Relay alarm enable. 0 = Disabled 1 = Enabled</p>

Attr ID	Access Rule	Name	Data Type	Description
18	Get/Set	Fiber Check Warning	USINT (8)	<p>Fiber check warning event notification.</p> <p>(Bit 1 should call MGMT-Relay if device support more than 1 relay. Bit 2-3 depends on device supported relay number.)</p> <p>Bit 0: Event notification enable.</p> <p>0 = Disabled 1 = Enabled</p> <p>Bit 1: Relay (MGMT-Relay) alarm enable.</p> <p>0 = Disabled 1 = Enabled</p> <p>Bit 2: PWR1-Relay alarm enable.</p> <p>0 = Disabled 1 = Enabled</p> <p>Bit 3: PWR2-Relay alarm enable.</p> <p>0 = Disabled 1 = Enabled</p>
19	Set	Relay Alarm Cut-off	USINT (8)	<p>Cut off the relay alarm.</p> <p>(Bit 0 should call MGMT-Relay if device support more than 1 relay. Bit 1-2 depends on device supported relay number.)</p> <p>Bit 0: Relay (MGMT-Relay)</p> <p>0 = Don't cut-off relay 1 = Cut-off relay</p> <p>Bit 1: PWR1-Relay</p> <p>0 = Don't cut-off relay 1 = Cut-off relay</p> <p>Bit 2: PWR2-Relay</p> <p>0 = Don't cut-off relay 1 = Cut-off relay</p>
20	Set	Reset MIB Count	USINT (8)	<p>Reset port MIB counters. (Ethernet Link object's attributes 4-5 and 12-13.)</p> <p>Any value indicates to reset port MIB counter.</p>
21	Set	Reset Device	USINT (8)	<p>Reboot and reset to default</p> <p>0 = Reserved. 1 = Reboot the device 2 = Reset to default</p>

## Common Service List

Service Code	Implementation Class	Implementation Instance	Service Name	Description
<b>0x0E</b>	✓	✓	Get_Attribute_Single	Used to read an object instance attribute.
<b>0x10</b>	✓		Set_Attribute_Single	Used to modify an object instance attribute



# Configuration Types

This table describes the different types of configurations that your device uses.

Configuration Type	Description
<b>Startup Config</b>	The configuration that is loaded when the device boots up. These settings persist even when the device is powered off.
<b>Running Config</b>	<p>The configuration that is currently in use by the device.</p> <ul style="list-style-type: none"><li>• <b>If auto-save is enabled</b>, all changes will be saved to the startup config, and will be retained when the device powers off.</li><li>• <b>If auto-save is disabled</b>, any unsaved changes will be lost when the device powers off.</li></ul> <p>Refer to <a href="#">Disable/Enable Auto Save</a> for more information.</p>
<b>Factory Default Config</b>	The pre-defined factory default configuration of your device. This configuration cannot be changed.

# Event Log Descriptions

This table describes the different events that can be recorded in the event log files.

Event Name	Severity	Event Description
<b>802.1X Auth Failed</b>	Warning	802.1x authentication failed on port {{index}}/{{number}} with {{buffer}}
<b>ABC-02 is inserted or unplugged</b>	Notice	ABC-02 is {{inserted/unplugged}}.
<b>ABC-03 is inserted or unplugged</b>	Notice	ABC-03 is {{inserted/unplugged}}.
<b>Account log out</b>	Notice	[Account:{{user_name}}] logged out.
<b>Account removed</b>	Notice	[Account:{{user_name}}] has been removed by admin.
<b>Account settings changed</b>	Notice	Account settings of [Account:{{user_name}}] has been updated. Account settings of [Account:{{user_name}}] has been deleted. Account settings of [Account:{{user_name}}] has been created.
<b>Announce message with different interval</b>	Warning	An Announce message with a different interval has been received from port {{index}}/{{number}}
<b>Announce timeout</b>	Warning	PTP port {{index}}/{{number}} Announce receipt timer has timed out.
<b>Check if hardware revision is valid</b>	Notice	The hardware revision of Power Module {{index}} is not allowed.
<b>Check if it is a known power module</b>	Warning	To avoid potential overheating, Moxa does not recommend using a {{index}} power supply with this device.
<b>Cold start</b>	Critical	System has performed a cold start.
<b>Configuration changed</b>	Notice	Configuration {{modules}} changed by {{username}}.
<b>Configuration exported</b>	Notice	Configurations exported {{successful /failed}} by {{username}} via {{method}}.
<b>Configuration imported</b>	Notice	Configuration import {{successful /failed}} by {{username}} via {{method}}.
<b>Coupling changed</b>	Warning	Turbo Ring v2 coupling path status has changed.

Event Name	Severity	Event Description
<b>DHCP client ingress discards packets due to the DHCP Snooping rule</b>	Warning	VLAN <vlan-id> dropped DHCP client ingress packets due to a violation of the DHCP Snooping rule. Total packets discarded: <number>
<b>DHCP server discards packets due to the DHCP Snooping rule</b>	Warning	VLAN <vlan-id> dropped DHCP server packets due to a violation of the DHCP Snooping rule. Total packets discarded: <number>
<b>DI off</b>	Notice	Digital Input {{index}} has been turned off.
<b>DI on</b>	Notice	Digital Input {{index}} has been turned on.
<b>Dual homing path changed</b>	Warning	Dual Homing path has switched.
<b>Event log export</b>	Notice	Event Log export {{successful /failed}} by {{username}} via {{method}}.
<b>Failed to overwrite the dhcpsnp static entry</b>	Warning	Static entry: VLAN: {{Vlan Id}}, MAC: {{mac addr}} already exists.
<b>Fiber Check warning</b>	Warning	Port {{index}}/{{number}} 's temperature has exceeded the threshold. Port{{index}}/{{number}} Tx power is over the threshold. Port{{index}}/{{number}} Tx power is under the threshold. Port{{index}}/{{number}} Rx power is over the threshold. Port{{index}}/{{number}} Rx power is under the threshold.
<b>Firmware upgrade failed</b>	Warning	Firmware failed to upgrade.
<b>Firmware upgrade successful</b>	Notice	Firmware successfully upgraded.
<b>Grand Master changed</b>	Warning	The PTP grandmaster has changed from {{mac addr}} to {{mac addr}}
<b>Hardware revision is not allowed</b>	Error	The hardware revision of Line Module %d is not allowed.
<b>Interface link down</b>	Notice	Interface{{number}} down.
<b>Interface link up</b>	Notice	Interface {{number}} up.

Event Name	Severity	Event Description
<b>Issue event log to syslog server</b>	Emergency	The system has lost power.
<b>LLDP table changed</b>	Info	LLDP remote table has changed.
<b>Log capacity threshold</b>	Warning	Number of event log entries {{logEntryNum}} has reached the threshold.
<b>Log Turbo Chain Port Restart</b>	Notice	Port-Channel {{channel id}} has restarted by Turbo Chain. Port {{index}}/{{number}} has restarted by Turbo Chain.
<b>Login failed</b>	Warning	[Account {{user_name}}] log in failed via {{interface}}.
<b>Login lockout</b>	Warning	[Account {{user_name}}] locked due to {{failed_times}} failed login attempts.
<b>Login successful</b>	Notice	[Account {{user_name}}] successfully logged in via {{interface}}.
<b>Low input voltage</b>	Warning	The input voltage of the power supply has dropped below 46 VDC. Please adjust the voltage to between 46 and 57 VDC to fit the PoE voltage requirement.
<b>Master changed</b>	Warning	Ring {{Index}} master has changed.
<b>Master mismatch</b>	Warning	Ring {{Index}} master setting does not match.
<b>Module change</b>	Notice	M{{index}} module has changed.
<b>Module Initialized Fail</b>	Error	M{{index}} Module initialized has failed.
<b>Module inserted</b>	Notice	M{{Index}} Module inserted.
<b>Module removed</b>	Notice	M{{index}} Module removed.
<b>MSTP new port role</b>	Warning	MSTP (MST{{Index}}) port {{number}} role changed from {{role}} to {{role}}.
<b>MSTP root changed</b>	Warning	MSTP (MST{{Index}}) new root has been elected in topology.
<b>MSTP topology changed</b>	Warning	Topology (MST{{Index}}) has been changed by MSTP.
<b>OSPF DR router adjacency changed</b>	Notice	Interface {{ip addr}}{{ip addr}}{{ip addr}}{{ip addr}} DR neighbor {{ip addr}}{{ip addr}}{{ip addr}}{{ip addr}} adjacency changed.

Event Name	Severity	Event Description
<b>OSPF interface DR changed</b>	Notice	Interface {{ip addr}}-{{ip addr}}-{{ip addr}}-{{ip addr}} DR Change{{ip addr}}-{{ip addr}}-{{ip addr}}-{{ip addr}} to {{ip addr}}-{{ip addr}}-{{ip addr}}-{{ip addr}}.
<b>OSPF interface ISM became DR</b>	Notice	Interface {{ip addr}}-{{ip addr}}-{{ip addr}}-{{ip addr}} become DR.
<b>Packet dropped by Port Security</b>	Warning	Port {{index}}/{{number}} dropped packets due to violation of Port Security rule.
<b>Password changed</b>	Notice	Password of [Account: {{user_name}}] has been changed.
<b>PD no response</b>	Error	Port {{number}} device is not responding to the PD failure check. Please check the device status.
<b>PD over-current</b>	Error	Current of port {{number}} has exceeded the safety limit. Please check the device status.
<b>PD power off</b>	Notice	Port {{number}} PD power off.
<b>PD power on</b>	Notice	Port {{number}} PD power on.
<b>Port Link Down</b>	Notice	Port {{index}}/{{number}} link down. Port-channel {{Channel id}} link down.
<b>Port Link Up</b>	Notice	Port {{index}}/{{number}} link up. Port-channel {{Channel id}} link up.
<b>Port recovery by Rate Limit</b>	Warning	Port {{index}}/{{number}} has recovered by rate limit.
<b>Port shutdown by Loop</b>	Critical	Port {{index}}/{{number}} looping and shutdown.
<b>Port shutdown by Port Security</b>	Warning	Port {{index}}/{{number}} has shut down due to a violation of the Port Security rule.
<b>Port shutdown by Rate Limit</b>	Warning	Port {{index}}/{{number}} has excessive traffic and shutdown.
<b>Port state change</b>	Info	PTP port {{index}}/{{number}} has changed from {{state}} to {{state}}.
<b>Power budget exceeded</b>	Warning	The consumed power {{power_value}} of all the PDs have exceeded the maximum input power {{input_power_value}}.

Event Name	Severity	Event Description
<b>Power detection failure</b>	Warning	Port {{number}} device is {{Not present/Legacy PD/802.3 af/802.3 at/802.3 bt/NIC/Unknown}}. Please {{No suggestion/enable PoE power output/disable PoE power output/select PoE output mode to High power/select PoE output mode to Force/enable legacy PD detection/raise external power supply voltage greater than 46 VDC}}.
<b>Power module inserted</b>	Notice	Power Module {{index}} has been inserted.
<b>Power module removed</b>	Notice	Power Module {{index}} has been removed.
<b>Power Off-&gt;On</b>	Notice	Power {{index}} has turned off.
<b>Power On-&gt;Off</b>	Notice	Power {{index}} has turned on.
<b>PTP message with the wrong domain number</b>	Warning	The PTP message with the wrong domain number was received from port {{index}}/{{number}}.
<b>Redundant port health check failed</b>	Error	Redundant port {{index}}/{{number}} health check fail.
<b>Relay Override message</b>	Notice	{{relay_name}} relay alarm has been cut off.
<b>Relay Triggered message</b>	Notice	{{MGMT/PWR1/PWR2}} alarm is on due to {{Event Name}}.
<b>Resource log export</b>	Notice	Resource Log export {{successful /failed}} by {{username}} via {{method}}.
<b>RMON failing alarm</b>	Warning	{{user defined}}.
<b>RMON raising alarm</b>	Warning	{{user defined}}.
<b>RSTP invalid BPDU</b>	Warning	RSTP Port-Channel {{channel id}} received an invalid BPDU (type: {{type}}, value: {{value}}). RSTP port {{index}}/{{number}} received an invalid BPDU (type: {{type}}, value: {{value}}).
<b>RSTP migration</b>	Warning	Port-Channel {{channel id}} changed to {{rstp/stp}}. Port {{index}}/{{number}} changed to {{rstp/stp}}.

Event Name	Severity	Event Description
<b>RSTP new port role</b>	Warning	RSTP Port-Channel {{channel id}} role changed from {{role}} to {{role}}. RSTP port {{index}}/{{number}} role changed from {{role}} to {{role}}.
<b>RSTP root changed</b>	Warning	RSTP new root has been elected in topology.
<b>RSTP topology changed</b>	Warning	Topology has been changed by RSTP.
<b>Send message failed</b>	Warning	PTP port {{index}}/{{number}} failed to transmit {{Type}}.
<b>SSH Key generated</b>	Notice	SSH key has been regenerated.
<b>SSL certification changed</b>	Notice	SSL certificate has been changed. SSL certificate has been regenerated.
<b>Sync status changed</b>	Warning	The PTP sync status has changed from {{PreSyncStatus}} to {{CurSyncStatus}}.
<b>Topology changed (MRP)</b>	Warning	Topology change has been detected, MRP {{strMRMState}}.
<b>Topology changed (MSTP)</b>	Warning	Topology (MST{{Index}}) has been changed by MSTP.
<b>Topology changed (RSTP)</b>	Warning	Topology has been changed by RSTP.
<b>Topology changed (Turbo Chain)</b>	Warning	Topology has been changed by Turbo Chain.
<b>Topology changed (Turbo Ring)</b>	Warning	Topology change has been detected on Ring {{RingIndex}} of Turbo Ring v2.
<b>Trust host moved from one port to another port (Port Security)</b>	Warning	A trust host, MAC is {{mac address}} with VLAN {{Vlan Id}}, moved from port {{index}}/{{number}} to port {{index}}/{{number}}.
<b>Unknown module</b>	Warning	Module {{index}} Unknown Module Initialized Failed.
<b>Warm start</b>	Notice	System has performed a warm start.

# Modbus Data Map and Information

The data map addresses of Moxa switches shown in the following tables start from MODBUS address 30001 for Function Code 4. For example, the address offset 0x0000 (hex) equals MODBUS address 30001, and the address offset 0x0010 (hex) equals MODBUS address 30017. Note that all the information read from Moxa switches are in hex mode. To interpret the information, refer to the ASCII table for the translation (For example, 0x4D = 'M', 0x6F = 'o').

## System Information

Address Offset	Data type	Interpretation	Description
<b>0x0000</b>	1 word	HEX	Vendor ID = 0x1393
<b>0x0001</b>	1 word		Unit ID (Ethernet = 1)
<b>0x0002</b>	2 word	HEX	Product Code (Please refer to Product Code Table)
<b>0x0010</b>	20 words	ASCII	Vendor Name Ex: Vendor Name = "Moxa" Word 0 Hi byte = 'M' Word 0 Lo byte = 'o' Word 1 Hi byte = 'x' Word 1 Lo byte = 'a' Word 2 Hi byte = '\0' Word 2 Lo byte = '\0'



Address Offset	Data type	Interpretation	Description
<b>0x0030</b>	20 words	ASCII	Product Model EX: Product Model = "MDS-G4028" Word 0 Hi byte = 'M' Word 0 Lo byte = 'D' Word 1 Hi byte = 'S' Word 1 Lo byte = '-' Word 2 Hi byte = 'G' Word 2 Lo byte = '4' Word 3 Hi byte = '0' Word 3 Lo byte = '2' Word 3 Hi byte = '8' Word 4 Lo byte = '\0'
<b>0x004B</b>	6 words	ASCII	Product Serial Number
<b>0x0051</b>	2 words	HEX	Firmware Version Word 0 Hi byte = major (A) Word 0 Lo byte = minor (B) Word 1 Hi byte = release (C) Word 1 Lo byte = build (D)
<b>0x0053</b>	2 words	HEX	Firmware Build Date For example: Word 0 = 0 x 0609 Word 1 = 0 x 0705 Firmware was built on 2007-05-06 at 09 o'clock
<b>0x0055</b>	3 words	HEX	Ethernet MAC Address Ex: MAC = 00-01-02-03-04-05 Word 0 Hi byte = 0 x 00 Word 0 Lo byte = 0 x 01 Word 1 Hi byte = 0 x 02 Word 1 Lo byte = 0 x 03 Word 2 Hi byte = 0 x 0 Word 2 Lo byte = 0 x 05
<b>0x0058</b>	1 word	HEX	Power 1 0x0000: Off 0x0001: ON

Address Offset	Data type	Interpretation	Description
<b>0x0059</b>	1 word	HEX	Power 2 0x0000: Off 0x0001: On
<b>0x005A</b>	1 word	HEX	Fault LED Status 0x0000: No 0x0001: Yes
<b>0x0080</b>	1 word	HEX	DI1 0x0000:Off 0x0001:On 0xFFFE: DI1 is Not Supported
<b>0x0081</b>	1 word	HEX	DI2 0x0000:Off 0x0001:On 0xFFFE: DI2 is Not Supported
<b>0x0082</b>	1 word	HEX	DO1 0x0000:Off 0x0001:On 0xFFFE: DO1 is Not Supported
<b>0x0083</b>	1 word	HEX	DO2 0x0000:Off 0x0001:On 0xFFFE: DO2 is Not Supported
<b>0x0084</b>	1 word	HEX	DO3 0x0000:Off 0x0001:On 0xFFFE: DO3 is Not Supported
<b>0x0085 (Power Module 1)</b> <b>0x0086 (Power Module 2)</b>	1 word	HEX	Power Module Present 0x0000: Not Present 0x0001: Present 0xFFFE: Power Module is Not Supported

Address Offset	Data type	Interpretation	Description
<b>0x0087 (Power Module 1)</b> <b>0x0097 (Power Module 2)</b>	16 words	ASCII	Power Module Name EX: "PWR-HV-P48" Word 0 Hi byte = 'P' Word 0 Lo byte = 'W' Word 1 Hi byte = 'R' Word 1 Lo byte = '-' Word 2 Hi byte = 'H' Word 2 Lo byte = 'V' Word 3 Hi byte = '-' Word 3 Lo byte = 'P' Word 4 Hi byte = '4' Word 4 Lo byte = '8' Word 5 Hi byte = '\n' Word 5 Lo byte = '\n'
<b>0x00A7 (Power Module 1)</b> <b>0x00AD (Power Module 2)</b>	6 words	ASCII	Power Module Serial Number
<b>0x00B3 (Power Module 1)</b> <b>0x00B5 (Power Module 2)</b>	2 words	HEX	Power Module Product Revision Word 0 Hi byte = major (A) Word 0 Lo byte = subversion (B) Word 1 Hi byte = minor (C) Word 1 Lo byte = 0
<b>0x00B7 (External Module 1)</b> <b>0x00B8 (External Module 2)</b> ...	1 word	HEX	External Module Present 0x0000: Not Present 0x0001: Present 0xFFFE: External Module is Not Supported

Address Offset	Data type	Interpretation	Description
<b>0x00C7 (External Module 1)</b>	16 words	ASCII	External Module Name
<b>0x00D7 (External Module 2)</b>			EX: "LM-7000H-4GTX"
...			Word 0 Hi byte = 'L'
			Word 0 Lo byte = 'M'
			Word 1 Hi byte = '-'
			Word 1 Lo byte = '7'
			Word 2 Hi byte = '0'
			Word 2 Lo byte = '0'
			Word 3 Hi byte = '0'
			Word 3 Lo byte = 'H'
			Word 4 Hi byte = '-'
			Word 4 Lo byte = '4'
			Word 5 Hi byte = 'G'
	Word 5 Lo byte = 'T'		
	Word 6 Hi byte = 'X'		
	Word 6 Lo byte = '\n'		
<b>0x01C7 (External Module 1)</b>	6 words	ASCII	External Module Serial Number
<b>0x01CD (External Module 2)</b>			
...			
<b>0x0227 (External Module 1)</b>	2 words	HEX	External Module Product Revision
<b>0x0229 (External Module 2)</b>			Word 0 Hi byte = major (A)
...			Word 0 Lo byte = subversion (B)
			Word 1 Hi byte = minor (C)
			Word 1 Lo byte = 0

# Port Information

Address Offset	Data type	Interpretation	Description
<b>0x1000 (Port 1)</b>	1 word	HEX	Port Status
<b>0x1001 (Port 2)</b>			0x0000: Link down
...			0x0001: Link up
<b>Maximum Port (n)</b>			0x0002: Disable
<b>0x1000 + n (Channel Group 1)</b>			0xFFFF: No port
<b>0x1000 + n + 1 (Channel Group 2)</b>			
...			
<b>0x1100 (Port 1)</b>	1 word	HEX	Port Speed (Y: Channel group active port count)
<b>0x1101 (Port 2)</b>			0x0000: 10M-Half
...			0xY001: 10M-Full
<b>Maximum Port (n)</b>			0x0002: 100M-Half
<b>0x1100 + n (Channel Group 1)</b>			0xY003: 100M-Full
<b>0x1100 + n + 1 (Channel Group 2)</b>			0xY004: 1G-Full
...			0xY005: 2500M-Full
			0xY006: 10G-Full
			0xY007: 40G-Full
			0xY008: 50G-Full
			0xY009: 25G-Full
			0xY00A: 100G-Full
	0xFFFE: Inactive Link		
	0xFFFF: No port		
<b>0x1200 (Port 1)</b>	1 word	HEX	Port Flow Ctrl
<b>0x1201 (Port 2)</b>			0x0000:Off
...			0x0001:On
<b>Maximum Port (n)</b>			0xFFFE: Inactive Link
	0xFFFF:No port		

Address Offset	Data type	Interpretation	Description
<b>0x1300 (Port 1)</b>	1 word	HEX	Port MDI/MDIX
<b>0x1301 (Port 2)</b>			0x0000: MDI
...			0x0001: MDIX
<b>Maximum Port (n)</b>			0xFFFF: Fiber Port
			0xFFFFE: Inactive Link
	0xFFFFF: No port		
<b>0x1400 (Port 1)</b>	32 words	ASCII	Port Media Type
<b>0x1420 (Port 2)</b>			Ex: Port 1 Media Type = "100TX,RJ45."
...			Word 0 Hi byte = '1'
<b>Maximum Port (n)</b>			Word 0 Lo byte = '0'
			Word 1 Hi byte = '0'
			Word 1 Lo byte = 'T'
			...
			Word 4 Hi byte = '4'
			Word 4 Lo byte = '5'
			Word 5 Hi byte = '\'
	Word 5 Lo byte = '\0'		

## Packet Information

Address Offset	Data type	Interpretation	Description
<b>0x2000 (Port 1)</b>	2 words	HEX	Port Tx Packets
<b>0x2002 (Port 2)</b>			Ex: port 1 Tx Packet Amount = 44332211
...			Received MODBUS response: 0x02A474B3
<b>Maximum Port (n)</b>			Word 0 = 0x02A4
<b>0x2000 + (n * 2) (Channel Group 1)</b>			Word 1 = 0x74B3
<b>0x2000 + ((n + 1) * 2) (Channel Group 2)</b>			
...			

Address Offset	Data type	Interpretation	Description
<b>0x2100 (Port 1)</b>	2 words	HEX	Port Rx Packets
<b>0x2102 (Port 2)</b>			Ex: port 1 Tx Packet Amount = 44332211
...			
<b>Maximum Port (n)</b>			Received MODBUS response: 0x02A474B3
<b>0x2100 + (n * 2) (Channel Group 1)</b>			Word 0 = 0x02A4
<b>0x2100 + ((n + 1) * 2) (Channel Group 2)</b>			Word 1 = 0x74B3
...			
<b>0x2200 (Port 1)</b>	2 words	HEX	Port Tx Error Packets
<b>0x2202 (Port 2)</b>			Ex: port 1 Tx Packet Amount = 44332211
...			
<b>Maximum Port (n)</b>			Received MODBUS response: 0x02A474B3
<b>0x2200 + (n * 2) (Channel Group 1)</b>			Word 0 = 0x02A4
<b>0x2200 + ((n + 1) * 2) (Channel Group 2)</b>			Word 1 = 0x74B3
...			
<b>0x2300 (Port 1)</b>	2 words	HEX	Port Rx Error Packets
<b>0x2302 (Port 2)</b>			Ex: port 1 Tx Packet Amount = 44332211
...			
<b>Maximum Port (n)</b>			Received MODBUS response: 0x02A474B3
<b>0x2300 + (n * 2) (Channel Group 1)</b>			Word 0 = 0x02A4
<b>0x2300 + ((n + 1) * 2) (Channel Group 2)</b>			Word 1 = 0x74B3
...			

# Redundancy Information

Address Offset	Data type	Interpretation	Description
<b>0x3000</b>	1 word	HEX	Redundancy Protocol 0x0000: None 0x0001: RSTP 0x0002: Turbo Ring V2 0x0003: Turbo Chain 0x0004: Dual Homing 0x0005: RSTP & Dual Homing 0x0006: Turbo Ring V2 & Dual Homing 0x0007: Turbo Chain & Dual Homing
<b>0x3100</b>	1 word	HEX	RSTP Root 0x0000: Not Root 0x0001: Root 0xFFFFE: RSTP is Not Supported 0xFFFFF: RSTP is Not Enabled
<b>0x3200 (Port 1)</b> <b>0x2301 (Port 2)</b> ... <b>Maximum Port (n)</b> <b>0x3200 + n (Channel Group 1)</b> <b>0x3200 + n + 1 (Channel Group 2)</b> ...	1 word	HEX	RSTP Port Status 0x0000: Port Disabled 0x0001: Not RSTP Port 0x0002: Link Down 0x0003: Blocked 0x0004: Learning 0x0005: Forwarding 0xFFFFD: No Port 0xFFFFE: RSTP is Not Supported 0xFFFFF: RSTP is Not Enabled
<b>0x3500</b>	1 word	HEX	Turbo Ring V2 Coupling Mode 0x0000: None 0x0001: Coupling Backup 0x0002: Coupling Primary 0xFFFFE: Turbo Ring V2 is Not Supported 0xFFFFF: Turbo Ring V2 is Not Enabled



Address Offset	Data type	Interpretation	Description
<b>0x3501</b>	1 word	HEX	Turbo Ring V2 Coupling Port Primary Status 0x0000: Not Coupling Port 0x0001: Link Down 0x0002: Blocked 0x0003: Learning 0x0004: Forwarding 0xFFFFD: Turbo Ring V2 Coupling is Not Enabled 0xFFFFE: Turbo Ring V2 is Not Supported 0xFFFFF: Turbo Ring V2 is Not Enabled
<b>0x3502</b>	1 word	HEX	Turbo Ring V2 Coupling Port Backup Status 0x0000: Not Coupling Port 0x0001: Link Down 0x0002: Blocked 0x0003: Learning 0x0004: Forwarding 0xFFFFD: Turbo Ring V2 Coupling is Not Enabled 0xFFFFE: Turbo Ring V2 is Not Supported 0xFFFFF: Turbo Ring V2 is Not Enabled
<b>0x3600</b>	1 word	HEX	Turbo Ring V2 Ring 1 Status 0x0000: Healthy 0x0001: Break 0xFFFFD: Turbo Ring V2 Ring 1 is Not Enabled 0xFFFFE: Turbo Ring V2 is Not Supported 0xFFFFF: Turbo Ring V2 is Not Enabled
<b>0x3601</b>	1 word	HEX	Turbo Ring V2 Ring 1 Master/Slave 0x0000: Slave 0x0001: Master 0xFFFFD: Turbo Ring V2 Ring 1 is Not Enabled 0xFFFFE: Turbo Ring V2 is Not Supported 0xFFFFF: Turbo Ring V2 is Not Enabled

Address Offset	Data type	Interpretation	Description
<b>0x3602</b>	1 word	HEX	<p>Turbo Ring V2 Ring 1's 1st Port Status</p> <p>0x0000: Link Down</p> <p>0x0001: Blocked</p> <p>0x0002: Learning</p> <p>0x0003: Forwarding</p> <p>0xFFFFD: Turbo Ring V2 Ring 1 is Not Enabled</p> <p>0xFFFFE: Turbo Ring V2 is Not Supported</p> <p>0xFFFFF: Turbo Ring V2 is Not Enabled</p>
<b>0x3603</b>	1 word	HEX	<p>Turbo Ring V2 Ring 1's 2nd Port Status</p> <p>0x0000: Link Down</p> <p>0x0001: Blocked</p> <p>0x0002: Learning</p> <p>0x0003: Forwarding</p> <p>0xFFFFD: Turbo Ring V2 Ring 1 is Not Enabled</p> <p>0xFFFFE: Turbo Ring V2 is Not Supported</p> <p>0xFFFFF: Turbo Ring V2 is Not Enabled</p>
<b>0x3680</b>	1 word	HEX	<p>Turbo Ring V2 Ring 2 Status</p> <p>0x0000: Healthy</p> <p>0x0001: Break</p> <p>0xFFFFD: Turbo Ring V2 Ring 2 is Not Enabled</p> <p>0xFFFFE: Turbo Ring V2 is Not Supported</p> <p>0xFFFFF: Turbo Ring V2 is Not Enabled</p>
<b>0x3681</b>	1 word	HEX	<p>Turbo Ring V2 Ring 2 Master/Slave</p> <p>0x0000: Slave</p> <p>0x0001: Master</p> <p>0xFFFFD: Turbo Ring V2 Ring 2 is Not Enabled</p> <p>0xFFFFE: Turbo Ring V2 is Not Supported</p> <p>0xFFFFF: Turbo Ring V2 is Not Enabled</p>

Address Offset	Data type	Interpretation	Description
<b>0x3682</b>	1 word	HEX	Turbo Ring V2 Ring 2's 1st Port Status 0x0000: Link Down 0x0001: Blocked 0x0002: Learning 0x0003: Forwarding 0xFFFFD: Turbo Ring V2 Ring 2 is Not Enabled 0xFFFFE: Turbo Ring V2 is Not Supported 0xFFFFF: Turbo Ring V2 is Not Enabled
<b>0x3683</b>	1 word	HEX	Turbo Ring V2 Ring 2's 2nd Port Status 0x0000: Link Down 0x0001: Blocked 0x0002: Learning 0x0003: Forwarding 0xFFFFD: Turbo Ring V2 Ring 2 is Not Enabled 0xFFFFE: Turbo Ring V2 is Not Supported 0xFFFFF: Turbo Ring V2 is Not Enabled
<b>0x3700</b>	1 word	HEX	Turbo Chain Switch Role 0x0000: Head 0x0001: Member 0x0002: Tail 0xFFFFE: Turbo Chain is Not Supported 0xFFFFF: Turbo Chain is Not Enabled
<b>0x3701</b>	1 word	HEX	Turbo Chain 1st Port Status 0x0000: Link Down 0x0001: Blocked 0x0002: Listening 0x0003: Forwarding 0xFFFFE: Turbo Chain is Not Supported 0xFFFFF: Turbo Chain is Not Enabled

Address Offset	Data type	Interpretation	Description
<b>0x3702</b>	1 word	HEX	Turbo Chain 2nd Port Status 0x0000: Link Down 0x0001: Blocked 0x0002: Listening 0x0003: Forwarding 0xFFFE: Turbo Chain is Not Supported 0xFFFF: Turbo Chain is Not Enabled
<b>0x3800</b>	1 word	HEX	Dual Homing Primary Link Status 0x0000: Link Down 0x0001: Link Up 0xFFFE: Dual Homing is Not Supported 0xFFFF: Dual Homing is Not Enabled
<b>0x3801</b>	1 word	HEX	Dual Homing Primary Port State 0x0000: Link Down 0x0001: Blocking 0x0002: Forwarding 0xFFFE: Dual Homing is Not Supported 0xFFFF: Dual Homing is Not Enabled
<b>0x3802</b>	1 word	HEX	Dual Homing Secondary Link Status 0x0000: Link Down 0x0001: Link Up 0xFFFE: Dual Homing is Not Supported 0xFFFF: Dual Homing is Not Enabled
<b>0x3803</b>	1 word	HEX	Dual Homing Secondary Port Status 0x0000: Link Down 0x0001: Blocking 0x0002: Forwarding 0xFFFE: Dual Homing is Not Supported 0xFFFF: Dual Homing is Not Enabled
<b>0x3804</b>	1 word	HEX	Dual Homing Path Switching Mode 0x0000: Primary path always first 0x0001: Maintain current path 0xFFFE: Dual Homing is Not Supported 0xFFFF: Dual Homing is Not Enabled

# Product Codes Used in Industrial Protocols

The following table contains Moxa product codes used in industrial protocols.

Product name	Product code (16 bits)	Product code (32 bits)
<b>EDS-4008</b>	0x1100	0x11021000
<b>EDS-4008-2GT-2GS</b>	0x1104	0x11021004
<b>EDS-4008-2MSC</b>	0x1101	0x11021001
<b>EDS-4008-2MST</b>	0x1102	0x11021002
<b>EDS-4008-2SSC</b>	0x1103	0x11021003
<b>EDS-4008-4P-2GT-GS</b>	0x1105	0x11024005
<b>EDS-4009-3MSC</b>	0x1107	0X11022007
<b>EDS-4009-3MST</b>	0x1108	0X11022008
<b>EDS-4009-3SSC</b>	0x1109	0X11022009
<b>EDS-4012-4GC</b>	0x110B	0X1102300b
<b>EDS-4012-4GC-HV-T</b>	0x110D	0X1102300d
<b>EDS-4012-4GS</b>	0x110A	0X1102300a
<b>EDS-4012-4GS-HV-T</b>	0x110C	0X1102300c
<b>EDS-4012-8P-4GS</b>	0x110E	0x1102340e
<b>EDS-4014-4GS-2QGS-HV-T</b>	0x1112	0x11024012
<b>EDS-G4008</b>	0x1106	0x11021806
<b>EDS-G4012-4GC</b>	0x110F	0x1102380f
<b>EDS-G4012-8P-4GS</b>	0x1110	0x11023c10
<b>EDS-G4014-4GS-2QGS</b>	0x1111	0x11024011

Product name	Product code (16 bits)	Product code (32 bits)
<b>EDS-G4014-4QGS-2XGS</b>	0x1114	0x11024814
<b>EDS-G4014-6QGS</b>	0x1113	0x11024813
<b>MDS-G4012</b>	0x1081	0x11010001
<b>MDS-G4012-4XGS-T</b>	0x1281	0x11050001
<b>MDS-G4012-L3</b>	0x2081	0x12010001
<b>MDS-G4012-L3-4XGS-T</b>	0x2281	0x12050001
<b>MDS-G4020</b>	0x1082	0x11010002
<b>MDS-G4020-4XGS-T</b>	0x1282	0x11050002
<b>MDS-G4020-L3</b>	0x2082	0x12010002
<b>MDS-G4020-L3-4XGS-T</b>	0x2282	0x12050002
<b>MDS-G4028</b>	0x1083	0x11010003
<b>MDS-G4028-4XGS-FM</b>	0x2284	0x11050004
<b>MDS-G4028-4XGS-T</b>	0x1283	0x11050003
<b>MDS-G4028-L3</b>	0x2083	0x12010003
<b>MDS-G4028-L3-4XGS-T</b>	0x2283	0x12050003
<b>RKS-G4028-4GS-2HV-T</b>	0x1304	0x11060004
<b>RKS-G4028-4GS-2LV-T</b>	0x1308	0x11060008
<b>RKS-G4028-4GS-HV-T</b>	0x1303	0x11060003
<b>RKS-G4028-4GS-LV-T</b>	0x1307	0x11060007
<b>RKS-G4028-4GT-2HV-T</b>	0x1302	0x11060002
<b>RKS-G4028-4GT-2LV-T</b>	0x1306	0x11060006
<b>RKS-G4028-4GT-HV-T</b>	0x1301	0x11060001
<b>RKS-G4028-4GT-LV-T</b>	0x1305	0x11060005

Product name	Product code (16 bits)	Product code (32 bits)
<b>RKS-G4028-4MGSFP-8GPoE</b>	0x1185	0x11030005
<b>RKS-G4028-4MGSFP-8GPoE-PTP</b>	0x118B	0x1103000B
<b>RKS-G4028-4MGSFP-8GSFP</b>	0x1186	0x11030006
<b>RKS-G4028-4MGSFP-8GSFP-PTP</b>	0x118C	0x1103000C
<b>RKS-G4028-4MGSFP-8GTX</b>	0x1184	0x11030004
<b>RKS-G4028-4MGSFP-8GTX-PTP</b>	0x118A	0x1103000A
<b>RKS-G4028-4MGTX-8GPoE</b>	0x1191	0x11030011
<b>RKS-G4028-4MGTX-8GPoE-PTP</b>	0x1197	0x11030017
<b>RKS-G4028-4MGTX-8GSFP</b>	0x1192	0x11030012
<b>RKS-G4028-4MGTX-8GSFP-PTP</b>	0x1198	0x11030018
<b>RKS-G4028-4MGTX-8GTX</b>	0x1190	0x11030010
<b>RKS-G4028-4MGTX-8GTX-PTP</b>	0x1196	0x11030016
<b>RKS-G4028-4XGSFP-8GPoE</b>	0x1182	0x11030002
<b>RKS-G4028-4XGSFP-8GPoE-PTP</b>	0x1188	0x11030008
<b>RKS-G4028-4XGSFP-8GSFP</b>	0x1183	0x11030003
<b>RKS-G4028-4XGSFP-8GSFP-PTP</b>	0x1189	0x11030009
<b>RKS-G4028-4XGSFP-8GTX</b>	0x1181	0x11030001
<b>RKS-G4028-4XGSFP-8GTX-PTP</b>	0x1187	0x11030007
<b>RKS-G4028-4XGTX-8GPoE</b>	0x118E	0x1103000E
<b>RKS-G4028-4XGTX-8GPoE-PTP</b>	0x1194	0x11030014
<b>RKS-G4028-4XGTX-8GSFP</b>	0x118F	0x1103000F
<b>RKS-G4028-4XGTX-8GSFP-PTP</b>	0x1195	0x11030015
<b>RKS-G4028-4XGTX-8GTX</b>	0x118D	0x1103000D

Product name	Product code (16 bits)	Product code (32 bits)
<b>RKS-G4028-4XGTX-8GTX-PTP</b>	0x1193	0x11030013
<b>RKS-G4028-L3-4GS-2HV-T</b>	0x2304	0x12060004
<b>RKS-G4028-L3-4GS-2LV-T</b>	0x2308	0x12060008
<b>RKS-G4028-L3-4GS-HV-T</b>	0x2303	0x12060003
<b>RKS-G4028-L3-4GS-LV-T</b>	0x2307	0x12060007
<b>RKS-G4028-L3-4GT-2HV-T</b>	0x2302	0x12060002
<b>RKS-G4028-L3-4GT-2LV-T</b>	0x2306	0x12060006
<b>RKS-G4028-L3-4GT-HV-T</b>	0x2301	0x12060001
<b>RKS-G4028-L3-4GT-LV-T</b>	0x2305	0x12060005
<b>RKS-G4028-L3-PoE-4GS-2HV-T</b>	0x230A	0x1206000A
<b>RKS-G4028-L3-PoE-4GS-2LV-T</b>	0x230C	0x1206000C
<b>RKS-G4028-L3-PoE-4GS-HV-T</b>	0x2309	0x12060009
<b>RKS-G4028-L3-PoE-4GS-LV-T</b>	0x230B	0x1206000B
<b>RKS-G4028-PoE-4GS-2HV-T</b>	0x130A	0x1106000A
<b>RKS-G4028-PoE-4GS-2LV-T</b>	0x130C	0x1106000C
<b>RKS-G4028-PoE-4GS-HV-T</b>	0x1309	0x11060009
<b>RKS-G4028-PoE-4GS-LV-T</b>	0x130B	0x1106000B



# Security Guidelines

This appendix explains security practices for installing, operating, maintaining, and decommissioning this device. We strongly recommend you follow these guidelines to enhance network and equipment security.

## Physical Installation

1. This device must be installed in an access controlled area, where only the necessary personnel have physical access to the device.
2. This device must not be directly connected to the Internet, which means switches must be installed within a security perimeter, which can be implemented by a firewall at the border since this device is not classified as zone/boundary equipment
3. Please follow the instructions in the Quick Installation Guide, which is included in the package, to ensure you install this device correctly in your environment.
4. This device has anti-tamper labels on the enclosures. This allows an administrator to tell whether the device has been tampered with.
5. Ports that are not in use should be deactivated. Please refer to Port Interface for more information.

## Account Management

Follow these best practices when setting up an account.

1. Each account should be assigned the correct privileges: Only allow the minimum number of people necessary to have admin privileges so they can perform device configuration or modifications, while other users should only have read access privileges. This device supports both local accounts and remote centralized mechanisms for authentication, including RADIUS and TACACS+.
2. Change the default password, and strengthen the account password complexity by:
  - a. Enabling the Password Policy function.

- b. Increasing the minimum password length to at least eight characters.
  - c. Defining a password policy to ensure that passwords contain at least an uppercase and lowercase letter, a digit, and a special character.
  - d. Setting user passwords to expire after a certain period of time.
3. Enforce regulations that ensure that only a trusted host can access this device. Please refer to [Trusted Access](#) for more information.

## Vulnerable Network Ports

1. For network security concerns, we strongly recommend that you change the port numbers—such as TCP port numbers for HTTP, HTTPS, Telnet, and SSH—for the protocols that are in use. Ports that are not in use but are still reachable create a security risk and should be disabled. Refer to [Management Interface](#) for more information.
2. In order to avoid eavesdroppers from snooping confidential information, users should adopt encryption-based communication protocols, such as HTTPS instead of HTTP, SSH instead of Telnet, SFTP instead of TFTP, SNMPv3 instead of SNMPv1/v2c, etc. In addition, the maximum number of sessions should be kept to an absolute minimum. Refer to [Management Interface](#) for more information.
3. Users should regenerate SSL certificate and SSH key for this device before commissioning HTTPS or SSH applications. Refer to [SSH & SSL](#) for more information.

## Operation

1. In order to ensure that communications are properly protected, use a strong cryptographic algorithm for key exchange or encryption protocols for HTTPS/SSH applications. This device follows the NIST SP800-52 and SP800-131 standards, and supports TLS v1.2 and v1.3 with the following cipher suites:
  - a. **TLS v1.2**

Cipher suite name	Key exchange	Authentication	Encryption	Hash function
<b>TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256</b>	ECDHE	RSA	CHACHA20-POLY1305	SHA256
<b>TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256</b>	ECDHE	ECDSA	AES128	SHA256
<b>TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256</b>	ECDHE	RSA	AES128	SHA256
<b>TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384</b>	ECDHE	RSA	AES256	SHA384
<b>TLS_DHE_RSA_WITH_AES_128_GCM_SHA256</b>	Ephemeral DH	RSA	AES128	SHA256
<b>TLS_DHE_RSA_WITH_AES_256_GCM_SHA384</b>	Ephemeral DH	RSA	AES256	SHA384
<b>TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256</b>	Ephemeral DH	RSA	CHACHA20-POLY1305	SHA256
<b>TLS_ECDHE-RSA_WITH_AES256-SHA384</b>	ECDHE	RSA	AES256	SHA384
<b>TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256</b>	ECDHE	RSA	AES128	SHA256
<b>TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256</b>	ECDHE	ECDSA	CHACHA20-POLY1305	SHA256
<b>TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384</b>	ECDHE	RSA	AES256	SHA384
<b>TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384</b>	ECDHE	ECDSA	AES256	SHA384
<b>TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256</b>	ECDHE	ECDSA	AES128	SHA256

**b. TLS V1.3**

Cipher suite name	Key exchange	Encryption	Mode	Hash function
<b>TLS_AES_256_GCM_SHA384</b>	any	AES256	GCM	SHA384
<b>TLS_CHACHA20_POLY1305_SHA256</b>	any	CHACHA20-POLY1305	N/A	SHA256
<b>TLS_AES_128_GCM_SHA256</b>	any	AES128	GCM	SHA256

2. Below is a list of the recommended secure browsers that support TLS v1.2 or higher:

Browser	Version
<b>Microsoft Edge</b>	All
<b>Microsoft Internet Explorer</b>	v11 or above
<b>Mozilla Firefox</b>	v27 or above
<b>Google Chrome</b>	v38 or above
<b>Apple Safari</b>	v7 or above

Reference: <https://support.globalsign.com/ssl/general-ssl/tls-protocol-compatibility#Browsers>

3. This device supports event logs and syslog for SIEM integration:
- Event log:** Due to limited storage capacity, the event log can only accommodate a maximum of 10,000 entries. Administrators can set a warning for a pre-defined threshold. We recommend that users regularly back up system event logs. Please refer to [Event Logs](#) for more information.
  - Syslog:** this device supports syslog, and advanced secure TLS-based syslog for centralized SIEM integration. Please refer to [Syslog](#) for more information.
4. This device can provide information for control system inventory:
- SNMPv1, v2c, v3:** We recommend administrators use SNMPv3 with authentication and encryption to manage the network. Please refer to the MIB file for more information.
  - Telnet/SSH:** We recommend that administrators use SSH with authentication and encryption to retrieve device properties.
  - HTTP/HTTPS:** We recommend that administrators use HTTPS with a certificate that has been granted by a Certificate Authority to configure this device.

d. **MMS:** We recommend administrators enable MMS security mode to enhance protection.

5. **Denial of Service protection:** To avoid disruption of normal operation of the switch, administrators should configure the QoS function. This device supports ingress rate limit and egress shaper. Administrators can decide how to deal with excess data flow and configure the device accordingly. This process will regulate the resulted data rate per port. Please refer to **QoS** for more information.
6. **Time synchronization with authentication:** Time synchronization is crucial for process control. To prevent malicious attacks whereby the settings are changed without permission, authentication must be in place between the NTP server and client. This device supports NTP with a pre-shared key. Please refer to **NTP** for more information.
7. **Periodically regenerate the SSH and SSL certificates:** Even though this device supports RSA 2048-bit and SHA-256 to ensure sufficient complexity, we strongly recommend that users frequently renew their SSH key and SSL certificate in case the key is compromised. Please refer to **SSH & SSL** for more information.
8. Below is the list of the protocol port numbers used for all external interfaces.

a. **Protocol:TCP**

Service Type	Port Number	Default state	Port can be modified
<b>SSH</b>	22	Enabled	Y
<b>Telnet</b>	23	Disabled	Y
<b>E-Mail Server (SMTP)</b>	25	Disabled	Y
<b>TACACS+</b>	49	Disabled	Y
<b>HTTP</b>	80	Enabled	Y
<b>MMS</b>	102	Disabled	N
<b>HTTPS</b>	443	Enabled	Y
<b>Moxa Service</b>	443	Enabled	N
<b>Modbus</b>	502	Disabled	N

Service Type	Port Number	Default state	Port can be modified
<b>Ethernet/IP</b>	44818	Disabled	N

**b. Protocol: UDP**

Service Type	Port Number	Default state	Port can be modified
<b>DHCP Server</b>	67	Disabled	N
<b>NTP</b>	123	Disabled	N
<b>SNMP</b>	161	Disabled	Y
<b>PTP (IP based)</b>	319/320	Disabled	N
<b>Syslog</b>	514	Disabled	Y
<b>RADIUS</b>	1812	Disabled	Y
<b>Ethernet/IP</b>	2222	Disabled	N
<b>PROFINET</b>	34964/49152	Disabled	N
<b>Moxa Service</b>	40404	Enabled	N

## Maintenance

1. Perform firmware upgrades frequently to enhance features, deploy security patches, or fix bugs.
2. Frequently back up the system configurations. In order to properly protect the system configuration files from being tampered with, this device supports password encryption and signature authentication for backup files.
3. Examine event logs frequently to detect any anomalies.
4. To report vulnerabilities of Moxa products, please submit your findings on the following web page: <https://www.moxa.com/en/support/product-support/security-advisory/report-a-vulnerability>

## **Decommissioning**

To avoid disclosing sensitive information such as account passwords and certificates, please reset the system settings to factory default before decommissioning this device or sending it back to Moxa RMA service.

# Severity Level List

This is a list of severity levels and descriptions, which are based on CVSS vulnerability classifications.

Severity	Description
<b>Emergency</b>	System is unusable
<b>Alert</b>	Action must be taken immediately
<b>Critical</b>	Critical conditions
<b>Error</b>	Error conditions
<b>Warning</b>	Warning conditions
<b>Notice</b>	Normal but significant condition
<b>Infomational</b>	Informational messages
<b>Debug</b>	Debug-level messages



# SNMP MIB Files

This appendix contains the SNMP MIB file for the managed switch.

You can download the MIB file via the product site. Please note the MIB file varies by model.

## Structure of the Moxa MIB group package

Moxa support standard MIB and properties MIB. Below are all of folder and related MIB files. Please note that the applicable MIB files may vary across different models.

<Package File Lists>

EX. MOXA\_MIB\_XXX-XXXX\_v1.0\_YYYY\_MMDD\_HHMM.zip //XXX-XXXX means model name

```
├─ Private // MOXA properties MIB
|
|   └─ General // General group
|       ├── mx1588.mib
|       ├── mxDeviceIo.mib
|       ├── mxDhcpRelay.mib
|       ├── mxDhcpSvr.mib
|       ├── mxEip.mib
|       ├── mxEmailC.mib
|       ├── mxEventLog.mib
|       ├── mxGene.mib
|       ├── mxGeneral.mib
|       ├── mxIec6185093Profile.mib
|       ├── mxIeeeC37238Profile.mib
|       ├── mxLocator.mib
|       ├── mxManagementIp.mib
|       ├── mxMms.mib
|       ├── mxModbusTcp.mib
|       ├── mxPoe.mib
|       ├── mxPorte.mib
|       └── mxProfinet.mib
```





- | └─ IF-MIB.mib
- | └─ INET-ADDRESS-MIB.mib
- | └─ LLDP-EXT-DOT1-MIB.mib
- | └─ LLDP-EXT-DOT3-MIB.mib
- | └─ LLDP-EXT-ODVA-MIB.mib
- | └─ LLDP-MIB.mib
- | └─ P-BRIDGE-MIB.mib
- | └─ Q-BRIDGE-MIB.mib
- | └─ RFC1213-MIB.mib
- | └─ RFC1271-MIB.mib
- | └─ RMON2-MIB.mib
- | └─ RMON-MIB.mib
- | └─ SNMP-FRAMEWORK-MIB.mib
- | └─ SNMPv2-CONF.mib
- | └─ SNMPv2-MIB.mib
- | └─ SNMPv2-SMI.mib
- | └─ SNMPv2-TC.mib
- | └─ OSPF-MIB.mib
- | └─ PTPBASE-MIB.mib
- | └─ TOKEN-RING-RMON-MIB.mib
- | └─ IEEE8021-AS-MIB.mib
- | └─ IEEE8021-BRIDGE-MIB.mib
- | └─ IEEE8021-Q-BRIDGE-MIB.mib
- | └─ IEEE8021-ST-MIB.mib
- | └─ README.txt // this file

## Standard MIB Installation Order

If your tool need to import MIB one-by-one, please refer to the Standard MIBs Installation Order.

- 1.RFC1213-MIB.mib
- 2.SNMP-FRAMEWORK-MIB.mib
- 3.SNMPv2-SMI.mib
- 4.SNMPv2-TC.mib
- 5.SNMPv2-CONF.mib



```

|-org(3)
  |-dod(6)-internet(1)
    |   |-mgmt(2)-mib-2(1)           : SNMPv2-MIB.mib
    |   |   |-system(1)             : RFC1213-MIB.mib
    |   |   |-interface(2)         : RFC1213-MIB.mib
    |   |   |-at(3)                 : RFC1213-MIB.mib
    |   |   |-snmp(11)              : RFC1213-MIB.mib
    |   |   |-ospf(14)              : OSPF-MIB.mib
    |   |   |-rmon(16)              : RMON-MIB.mib
    |   |   |-dot1dBridge(17)       : BRIDGE-MIB.mib, P-BRIDGE-MIB.mib,
Q-BRIDGE-MIB.mib
    |   |   |-ifMIB(31)             : IF-MIB.mib
    |   |   |-etherMIB(35)          : EtherLike-MIB.mib
    |   |   |-private(4)-moxa(8691)
    |   |   |   |-product(600)       : mxGeneralInfo.mib, mxProductInfo.mib,
    |   |   |   |-general(602)      : mxGeneral.mib, mxDeviceIo.mib,
mxDhcpRelay.mib, mxDhcpSvr.mib, mxEmailC.mib,
    |   |   |   |                   : mxEventLog.mib, mxGene.mib,
mxLocator.mib, mxManagementIp.mib, mxPoe.mib,
    |   |   |   |                   : mxPorte.mib, mxRelayC.mib, mxSnmp.mib,
mxSwe.mib, mxSysLoginPolicySvr.mib,
    |   |   |   |                   : mxSyslogSvr.mib,
mxSysPasswordPolicySvr.mib, mxSystemInfo.mib,
    |   |   |   |                   : mxSysTrustAccessSvr.mib, mxSysUtilSvr.mib,
mxTimeSetting.mib,
    |   |   |   |                   : mxTimeZone.mib, mxTrapC.mib,
mxUiServiceMgmt.mib, mxRte.mib, mxMms.mib,
    |   |   |   |                   : mxPtp.mib, mx1588.mib,
mxIec6185093Profile.mib, mxIeeeC37238Profile.mib mxModbusTcp.mib,
    |   |   |   |                   : mxEip.mib, mxProfinet.mib, mxTrackinge.mib
    |   |   |   |-switching(603)    : mxSwitching.mib
    |   |   |   |   |- portInterface : mxPort.mib, mxLa.mib
    |   |   |   |   |- basicLayer2  : mxLhc.mib, mxQos, mxVlan.mib
    |   |   |   |   |- layer2Redundancy : mxRstp.mib, mxTrv2.mib,
mxTurboChain.mib, mxDualHoming.mib
    |   |   |   |   |- layer2Security : mxStcl.mib, mxRlps.mib, mxPssp.mib,

```

mxPsms.mib, mxDot1x.mib, mxRadius.mib, mxLp.mib, mxDhcpSnp.mib, mxIpSg.mib,  
mxMab.mib, mxDai.mib, mxMacsec.mib

| | | |- layer2Diagnostic : mxLldp.mib, mxTcst.mib,  
mxPortMirror.mib, mxRmon.mib, mxFiberCheck.mib, mxTracking.mib

| | | |- layer3Diagnostic

| | | |- layer2Multicast : mxIcmpSnp.mib

| | | |- layer3Multicast

| | |-routing(605)

| | | |- I3Genral : mxIpIf.mib, mxArp.mib

| | | |- unicastRouting : mxUnicastRoutingTable.mib,

mxStaticRoute.mib, mxOspf.mib

| | | |- multicastRouting : mxMulticastRouting.mib,

mxPimSm.mib

| | | |- I3Redundant : mxVrrp.mib

| | |-poe(608) : mxPoe.mib

| |-snmpV2(6)-snmpModules(3)

| |-snmpFrameworkMIB(10) : SNMP-FRAMEWORK.mib

|

|-ieee(111)-standards-association-numbers-series-standards(2)-lan-man-  
stds(802)-ieee802dot1(1)-ieee802dot1mibs(1)-ieee8021SpanningTreeMib(3)  
: IEEE8021-SPANNING-TREE-MIB.mib

# User Role Privileges

This page shows the privilege levels granted to the different authority levels: Admin, Supervisor, and User on Moxa’s Managed Ethernet Series switches. Refer to [System > Account Management > User Accounts](#) for more information on user accounts.

Privileges are indicated as follows:

- **R/W:** Read and write access granted for the relevant settings.
- **R:** Read-only access granted for the relevant settings.
- **Execute:** Execute-only access granted for the relevant settings.
- **-:** No access granted for the relevant settings.

 **Note**

Available settings and options will vary depending on the product model.

## Options Menu

Settings	Admin	Supervisor	User
<b>Change Language</b>	R/W	R/W	R/W
<b>Change Mode: Standard/Advanced Mode</b>	R/W	R/W	R/W
<b>Disable Auto Save</b>	R/W	R/W	-
<b>Locator</b>	R/W	R/W	R
<b>Reboot</b>	R/W	R/W	-
<b>Reset to Default Settings</b>	R/W	-	-
<b>Log Out</b>	R/W	R/W	R/W



# System

Settings	Admin	Supervisor	User
<b>Device Summary</b>	R	R	R
<b>System Management</b>			
<b>Information Settings</b>	R/W	R/W	R
<b>Firmware Upgrade</b>	R/W	-	-
<b>Config Backup and Restore</b>	R/W	-	-
<b>Account Management</b>			
<b>User Accounts</b>	R/W	-	-
<b>Online Accounts</b>	R/W	-	-
<b>Password Policy</b>	R/W	-	-
<b>Management Interface</b>			
<b>User Interface</b>	R/W	-	-
<b>Hardware Interfaces</b>	R/W	R/W	R
<b>SNMP</b>	R/W	R	-
<b>Time</b>			
<b>System Time</b>	R/W	R/W	R
<b>NTP Server</b>	R/W	R/W	R
<b>Time Synchronization</b>	R/W	R/W	R

## Port

Settings	Admin	Supervisor	User
<b>Port Interface</b>			
<b>Port Settings</b>	R/W	R/W	R
<b>Linkup Delay</b>	R/W	R/W	R
<b>Link Aggregation</b>	R/W	R/W	R
<b>PoE</b>	R/W	R/W	R

## Layer 2 Switching

Settings	Admin	Supervisor	User
<b>VLAN</b>	R/W	R/W	R
<b>GARP</b>	R/W	R/W	R
<b>MAC</b>			
<b>Static Unicast</b>	R/W	R/W	R
<b>MAC Address Table</b>	R/W	R/W	R
<b>QoS</b>			
<b>Classification</b>	R/W	R/W	R
<b>Ingress Rate Limit</b>	R/W	R/W	R
<b>Scheduler</b>	R/W	R/W	R
<b>Egress Shaper</b>	R/W	R/W	R
<b>Multicast</b>			
<b>IGMP Snooping</b>	R/W	R/W	R

Settings	Admin	Supervisor	User
<b>GMRP</b>	R/W	R/W	R
<b>Static Multicast</b>	R/W	R/W	R

## Network Interface

Settings	Admin	Supervisor	User
<b>Network Interface</b>	R/W	R/W	R

## Redundancy

Settings	Admin	Supervisor	User
<b>Layer 2 Redundancy</b>			
<b>Spanning Tree</b>	R/W	R/W	R
<b>Turbo Ring v2</b>	R/W	R/W	R
<b>Turbo Chain</b>	R/W	R/W	R
<b>MRP</b>	R/W	R/W	R
<b>Multiple Dual Homing</b>	R/W	R/W	R
<b>Multiple Network Coupling</b>	R/W	R/W	R
<b>Layer 3 Redundancy</b>			
<b>VRRP</b>	R/W	R/W	R
<b>Tracking</b>	R/W	R/W	R

## Network Service

Settings	Admin	Supervisor	User
<b>DHCP Server</b>	R/W	R/W	R
<b>DHCP Relay Agent</b>	R/W	R/W	R
<b>DNS Server</b>	R/W	R/W	R

## Routing

Settings	Admin	Supervisor	User
<b>Unicast Route</b>			
<b>Static Routing</b>	R/W	R/W	R
<b>OSPF Settings</b>	R/W	R/W	R
<b>OSPF Status</b>	R	R	R
<b>Routing Table</b>	R	R	R
<b>Multicast Route</b>			
<b>PIM-DM</b>	R/W	R/W	R
<b>PIM-SM Settings</b>	R/W	R/W	R
<b>PIM-SM Status</b>	R	R	R
<b>Multicast Local Route</b>	R/W	R/W	R
<b>Multicast Routing Table</b>	R	R	R

# Security

Settings	Admin	Supervisor	User
<b>Device Security</b>			
<b>Login Policy</b>	R/W	R	R
<b>Trusted Access</b>	R/W	R	R
<b>SSH &amp; SSL</b>	R/W	R/W	-
<b>Network Security</b>			
<b>IEEE 802.1X</b>	R/W	R/W	R
<b>MAC Authentication Bypass</b>	R/W	R/W	R
<b>MAC Security</b>	R/W	R/W	R
<b>Port Security</b>	R/W	R/W	R
<b>Traffic Storm Control</b>	R/W	R/W	R
<b>Access Control List</b>	R/W	R/W	R
<b>Network Loop Protection</b>	R/W	R/W	R
<b>Binding Database</b>	R/W	R/W	R
<b>DHCP Snooping</b>	R/W	R/W	R
<b>IP Source Guard</b>	R/W	R/W	R
<b>Dynamic ARP Inspection</b>	R/W	R/W	R
<b>Authentication</b>			
<b>Login Authentication</b>	R/W	-	-
<b>RADIUS</b>	R/W	-	-
<b>TACACS+</b>	R/W	-	-

# Diagnostics

Settings	Admin	Supervisor	User
<b>System Status</b>			
Resource Utilization	R	R	R
Fiber Check	R/W	R/W	R
Module Information	R	R	R
<b>Network Status</b>			
Network Statistics	R	R	R
LLDP	R/W	R/W	R
ARP Table	R	R	R
<b>Tools</b>			
Port Mirroring	R/W	R/W	R
Ping	R/W	R/W	R/W
<b>Event Logs and Notifications</b>			
Event Logs	R/W	R/W	R
Event Notifications	R/W	R/W	R
Syslog General	R/W	R/W	R
Syslog Authentication	R/W	-	-
SNMP Trap/Inform	R/W	-	-
Email Settings	R/W	R/W	R
Relay Alarm	R/W	R/W	R

# Industrial Application

Settings	Admin	Supervisor	User
<b>IEC 61850</b>			
<b>MMS</b>	R/W	R/W	R
<b>GOOSE Check</b>	R/W	R/W	R
<b>Modbus TCP</b>	R/W	R/W	R
<b>EtherNet/IP</b>	R/W	R/W	R
<b>PROFINET</b>	R/W	R/W	R



**Moxa Inc.**

Copyright © 2024 Moxa, Inc. All rights reserved. Reproduction without permission is prohibited. Trademarks and logos are copyrights of their respective owners.

[www.moxa.com/products](http://www.moxa.com/products)