MX-NOS V6

User Manual

Version 1.1

September 2026



Table of Contents

Overview 21

Introduction 22

About MX-NOS 23

What's in This Document 24

Supported Series and Firmware Versions 25

Product Series Feature Comparison Table 26

Options Menu 26

System 27

Port 28

Layer 2 Switching 28

IP Configuration 29

Network Interface 29

Redundancy 30

Network Service 30

Routing 31

Security 32

Diagnostics 33

Industrial Application 34

Quick Start 35

Using a Web Browser to Configure the Industrial Ethernet Switch 36

Using a RS-232 Console to Configure the Device 38

Using Telnet to Configure the Device 41

UI Reference 43

UI Reference Overview 44

The MX-NOS User Interface 45

Options Menu 47

Options Menu - User Privileges 47

Locator 48

Reboot 48

Reset to Default Settings 48

Auto-save to Startup 49

Change Mode 50

Change Language 50

Log Out 50

Device Summary 51

System Information 51

Panel Status 52

Panel View 54

Event Summary (Last 3 days) 54

CPU Usage History (%) 55

System 56

System - User Privileges 56

System Management 57

Information Settings 57

Firmware Upgrade 59

Creating a Configuration Backup 63

Account Management 79

User Accounts 79

Online Accounts 85

Password Policy 86

Management Interface 88

User Interface 88

Hardware Interfaces *91*

Configuring Simple Network Management Protocol *92*

Time 101

About System Time *101*

About NTP Server *107*

About Time Synchronization *109*

Port 125

Port - User Privileges 125

Port Interface 125

About Port Settings *126*

About Linkup Delay *131*

About Link Aggregation 133

Static Trunk *134*

LACP *134*

Link Aggregation Algorithms *134*

Link Aggregation Settings *135*

About PoE 142

PoE Settings *142*

Layer 2 Switching 159

Layer 2 Switching - User Privileges 159

About VLAN 160

Assigning VLANs to Ports *160*

Creating VLANs *161*

VLANs in Depth *162*

VLAN Settings *164*

GARP 170

GARP Settings *170*

MAC 172
About Static Unicast 173
About MAC Address Tables 175
About QoS 178
QoS In Depth 178
QoS 179
Multicast 209
Multicast In Depth 210
Multicast 212
Network Interface 227
Network Interface - User Privileges 227
Network Interface - Settings 227
Loopback Interface Table 228
VLAN Interface Table 229
Network Interface - Status 233
Loopback Interface List 233
VLAN Interface List 234
Redundancy 235
Redundancy - User Privileges 235
Layer 2 Redundancy 236
About Layer 2 Redundancy Protocols 236
About Scenarios for Turbo Ring 238
About Spanning Tree 239
About Turbo Ring v2 269
About Turbo Chain 286
About MRP (Media Redundancy Protocol) 292
About Multiple Dual Homing 300

About Multiple Network Coupling *308*
About IEC 62439-3 319
About RedBoxes *320*
PRP in Depth *320*
HSR in Depth *322*
About PRP-HSR Single Coupling *324*
About PRP-HSR Multiple Coupling *325*
Considerations for PRP/HSR Network Planning *327*
About Supervision Frames *328*
Enabling PRP/HSR *328*
Configuring Supervision Frames *329*
IEC 62439-3 ..... *330*
Layer 3 Redundancy 334
About VRRP *334*
About Tracking 344
Layer 3 Tracking: VRRP *345*
Layer 3 Tracking: Static Route *345*
Layer 2 Tracking: Port Tracking *345*
Scenario: Configuring Interface Tracking for VRRP *346*
Scenario: Configuring Logical Tracking for Turbo Chain *351*
Scenario: Configuring Tracking for Static Route *355*
Tracking *356*
Network Service 371
Network Service - User Privileges 371
Configuring DHCP Server Functions 371
Introduction to DHCP *372*
Overview of DHCP Server Configuration *372*

Configuring Dynamic IP Address Assignment (DHCP Server Pool) *373*

Reserving IP Addresses for Specific Devices (MAC-based IP Assignment) .. *374*

Configuring Port-based IP Assignment *377*

DHCP Server *379*

Configuring DHCP Relay Agent 386

About DHCP Relay Agents *386*

Configuring DHCP Relay Agent (RKS-G4000 Series) *387*

Configuring Option 82 ..... *388*

DHCP Relay Agent *388*

About DNS 393

DNS Settings *393*

Routing 395

Routing - User Privileges 395

About Unicast Routes 396

Unicast Route *397*

Multicast Route 428

About PIM-DM *428*

About PIM-SM *432*

About Multicast Local Routes *453*

Multicast Routing Table *463*

About Bidirectional Forwarding Detection (BFD) 464

BFD In Depth *465*

Enabling Bidirectional Forwarding Detection *466*

BFD *467*

Security 472

Security - User Privileges 472

Device Security 473

About Login Policy *473*
About Trusted Access *475*
About SSH & SSL *478*
Network Security 482
About IEEE 802.1X *483*
About MAC Authentication Bypass *497*
About MAC Security *504*
Port Security *510*
About Traffic Storm Control *521*
About Access Control Lists *523*
About Network Loop Protection *539*
About Binding Databases *542*
About DHCP Snooping *547*
About IP Source Guard *551*
About Dynamic ARP Inspection *553*
Authentication 556
About Login Authentication *556*
RADIUS *558*
TACACS+ *560*
Diagnostics 563
Diagnostics - User Privileges 563
System Status 564
About Resource Utilization *564*
About Fiber Check *568*
Module Information *574*
Network Status 575
About Network Statistics *575*

About LLDP *581*

About ARP Tables *591*

Tools 592

About Port and VLAN Mirroring *592*

About Ping *627*

Event Logs and Notifications 627

About Event Logs *628*

About Event Notifications *635*

About Syslog *639*

About SNMP Trap/Inform *647*

About Email Settings *653*

Relay Alarm *655*

Industrial Application 657

Industrial Application - User Privileges 657

IEC 61850 658

MMS *658*

About GOOSE Check *666*

About Modbus TCP 673

Modbus In Depth *674*

Modbus TCP *675*

About EtherNet/IP 675

EtherNet/IP *676*

About PROFINET 676

Node Roles *676*

GSD Files *677*

PROFINET In Depth *677*

PROFINET *685*

Security Hardening Guide 688

Security Hardening Guide Overview 689

Security Best Practices 690

Product Security 690

Physical Installation Guidelines 690

Account Management Guidelines 691

Protecting Vulnerable Network Ports 692

Maintaining Communication Integrity 693

Communication Integrity Features 694

Device Access Control Best Practices 695

About Device Integrity and Authenticity 696

Securing USB Interfaces on Network Devices 697

Device Resource Management and Monitoring 698

About Device Resource Monitoring 698

About Event Logs for Monitoring 699

About Port Mirroring for Monitoring 699

Recommended Settings for Services and Features 699

Common Protocols and Ports 700

Security-Related Functions 701

Considerations for GOOSE Check 702

Protocols/Services with Weak Authentication/Encryption 703

Services 703

Redundant Protocols 704

Industrial Protocols 704

L3 protocols 704

Common Threats and Countermeasures 704

Recommended Operational Roles and Duties 705

Administrator 705

Supervisor *706*

Auditor *706*

Recommended Patching and Backup Practices 707

Configuration Backup *707*

Recommendations for Vulnerability Management 707

Recommendations for Decommissioning 708

Security Standards and Concepts 709

Introduction to Defense in Depth 709

About AAA - Authentication, Authorization, and Accounting 709

Authentication *709*

Authorization *710*

Accounting *710*

About Authentication Types 710

Local Authentication *710*

Remote Authentication *710*

Example: Creating a Local User *711*

Example: Configuring Account Controls for Local Users *712*

Example: Configuring a Remote RADIUS Server *714*

ISA/IEC 62443 Standards and Architecture 716

Security Reference Standards *716*

ISA/IEC 62443 Standards and Architecture *717*

Establishing Foundational Requirements *719*

Applying FR 1: User Identification and Authentication *720*

Product Lifecycle and Security *722*

Appendix 724

Advanced Mode Settings 725

CEF Message Format for Event Logs 727

Version 727

Device Vendor 727
Device Product 727
Device Version 727
CEF Event ID 727
Bytes 0-1: OS Identification 728
Bytes 2-3: Revision 728
Bytes 4-5: Classification System (Feature ID) 728
Bytes 6-7: Sequence Number 729
Event Name 729
Severity 729
Extension (Key + Value) 730
CIP EtherNet/IP Objects 732
Identity Object 732
Class Attribute List 733
Instance Attribute List 733
Common Service List 734
Message Router Object 734
Assembly Object 735
Mapping I/O Assembly Data Attribute Components 737
Connection Manager Object 737
QoS Object 738
Base Switch Object 740
Port Object 742
TCP/IP Interface Object 744
Ethernet Link Object 747
LLDP Management Object 757
LLDP Data Table Object 759

Moxa Networking Object (Vendor Specific) *765*

CIP Tags **776**

Tags for Identity Objects 776

Tags for TCPIP Objects 776

Tags for Ethernet Link Objects 777

Tags for Moxa Networking Objects 781

Tags for Moxa Base Switch Objects 783

Pre-configured Tags in the Moxa AOI 784

Identity Object (0x01) *784*

Base Switch Object (0x51) *785*

TCP/IP Interface Object (0xF5) *785*

Ethernet Link Object (0xF6) *786*

Moxa Networking Object (0x404) *787*

I/O Message Object *788*

Configuration Types **789**

Event Log Descriptions **790**

1. System 790

1.1 Cold start *790*

1.2 Warm start *791*

1.3 Configuration change by user *791*

1.4 Login success *791*

1.5 Login failure *792*

1.6 Login lockout *792*

1.7 Account settings change *793*

1.8 Configuration import *793*

1.9 Configuration export *794*

1.10 Password change *794*

1.11 Power Off→On *795*

1.12 Power On→Off *795*

1.13 Sync status change *795*

1.14 Grandmaster clock change *796*

1.15 Port state change *796*

1.16 PTP message with the wrong domain number *797*

1.17 Announce message with different interval *797*

1.18 Announce timeout *798*

1.19 Send message failed *798*

1.20 ABC-02 insertion/removal *799*

1.21 ABC-03 insertion/removal *799*

1.22 Module insertion *799*

1.23 Module removal *800*

1.24 Power module insertion *800*

1.25 Power module removal *801*

1.26 Power module overheating risk *801*

1.27 Unsupported power module hardware version *802*

1.28 Unknown module *802*

1.29 Hardware revision is not allowed *803*

1.30 Firmware upgrade success *803*

1.31 Firmware upgrade failure *803*

1.32 Account log out *804*

1.33 Account removal *804*

1.34 Module change *805*

1.35 DIP setting failure *805*

1.36 Issue event log to syslog server *806*

1.38 Self-healing system reboot (main function) *806*

1.39 Self-healing system reboot (framework) *807*

2. Port 807

2.1 Port link up *807*

2.2 Port link down *808*

2.3 PD power on *808*

2.4 PD power off *809*

2.5 Low input voltage *809*

2.6 PD overcurrent *809*

2.7 PD no response *810*

2.8 Power budget overrun *810*

2.9 Power detection failure *811*

2.10 Port link up (port channel) *811*

2.11 Port link down (port channel) *812*

2.12 Interface up *812*

2.13 Interface down *813*

2.14 Non-PD or PD short circuit *813*

3. Layer 2 Switching 814

3.1 Port shutdown (Rate Limit) *814*

3.2 Port recovery (Rate Limit) *814*

5. Redundancy 815

5.1 Topology Changed(MRP, Turbo Ring, Turbo Chain, Dual Homing) *815*

5.2 Topology Changed(MRP, Turbo Ring, Turbo Chain, Dual Homing) *815*

5.3 Dual homing path change *816*

5.4 Redundant port health check failure *816*

5.5 Multiple Network Coupling path change *816*

5.6 Topology change (MSTP) *817*

5.7 MSTP root change *817*

5.8 MSTP new port role *818*

5.9 Topology change (RSTP) *818*

5.10 RSTP invalid BPDU *819*

5.11 RSTP migration *819*

5.12 RSTP root change *820*

5.13 RSTP new port role *820*

5.14 Topology Changed(MRP, Turbo Ring, Turbo Chain, Dual Homing) *821*

5.15 Port (channel) restart (Turbo Chain) *821*

5.16 Topology Changed(MRP, Turbo Ring, Turbo Chain, Dual Homing) *822*

5.17 Master mismatch *822*

5.18 Master change *822*

5.19 Coupling change *823*

5.20 VRRP Master change *823*

5.21 A PHR Supervision frame time difference event occurred on ports A, B *824*

5.22 MRP multi managers *824*

5.23 Tracking state change *825*

5.24 Tracking action on port *825*

5.25 Tracking action on static route *826*

5.26 Tracking action on VRRP ID *826*

5.28 Topology change (MRP Interconnection) *826*

5.29 SWIFT status change (RSTP) *827*

5.30 MRP Ring-Open *827*

5.31 Port shutdown (Turbo Chain) *828*

5.32 Port recovery (Turbo Chain) *828*

5.33 Port shutdown (Turbo Ring) *829*

5.34 Port recovery (Turbo Ring) *829*

5.35 PRP LAN cross-connection detected *830*

7. Security 830
7.1 SSH key regeneration 830
7.2 SSL certification change 831
7.3 DHCP client ingress packet drop 831
7.4 DHCP server packet drop 831
7.5 DHCPSNP static entry overwrite failure 832
7.6 Port shutdown (Network Loop Protection) 832
7.7 MACsec MKA expiration 833
7.8 802.1X Auth Fail 833
7.9 Port shutdown (Port Security) 834
7.10 Packet dropped by Port Security 834
7.11 Trust host moved from one port to another port (Port Security) 835
7.12 Integrity check failure 835
7.13 Integrity is missing 835
7.14 VLAN Assignment check port mode 836
7.15 VLAN Assignment check vlan 836
7.16 Event Logs Cleared 837
7.17 Configuration integrity check failure 837
8. Diagnostics 838
8.1 Event log export 838
8.2 Resource log export 838
8.3 Log capacity threshold warning 839
8.4 LLDP table change 839
8.5 Module initialization failure 840
8.6 RMON raising alarm 840
8.7 RMON falling alarm 840
8.8 Fiber Check warning 841

8.9 Relay trigger *841*
8.10 Relay cut-off *842*
8.11 DI on *842*
8.12 DI off *843*
8.13 Moxa tech support login *843*
8.14 Moxa tech support logout *844*
8.15 Moxa tech support function activation *844*
8.16 Moxa tech support function deactivation *844*
9. Industrial 845
9.1 DCP IP change *845*
9.2 DCP default route change *845*
9.3 GOOSE Check entry counter timeout *846*
9.4 GOOSE Check entry counter timeout clear *846*
9.5 GOOSE Check tampered ingress port *847*
9.6 GOOSE Check tampered source MAC address *847*
9.7 GOOSE Check Lock violation *848*
9.8 GOOSE Check entry reset *848*
9.9 GOOSE Check entry delete *849*
9.10 Port shutdown (GOOSE Check) *849*
11. Routing 850
11.1 OSPF DR change *850*
11.2 OSPF DR adjacency change *850*
11.3 OSPF become DR *851*
11.4 PIM-SM DR change *851*
11.5 PIM-SM RP addition (BSM) *851*
11.6 PIM-SM RP deletion (BSM) *852*
11.7 BFD session up *852*

11.8 BFD session down *853*

11.9 BFD attempt limit overrun *853*

11.10 BFD time renegotiation *854*

Fiber Check Threshold Values for Auto Mode **855**

Modbus Data Map and Information **858**

System Information 858

Port Information 863

Packet Information 864

Redundancy Information 866

Product Codes Used in Industrial Protocols **871**

Security Guidelines **875**

Physical Installation 875

Account Management 875

Vulnerable Network Ports 876

Operation 876

Maintenance 880

Decommissioning 881

Severity Level List 881

SNMP MIB Files **882**

Structure of the Moxa MIB group package 882

Standard MIB Installation Order 885

MIB Tree 886

User Role Privileges **889**

Options Menu 889

System 890

Port 891

Layer 2 Switching 891

IP Configuration 892
Network Interface 892
Redundancy 892
Network Service 893
Routing 893
Security 894
Diagnostics 895
Industrial Application 896

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
MDS-G4000-L2 Series	v6.0
MDS-G4000-L2-4XGS Series	v6.0
MDS-G4000-L3 Series	v6.0
MDS-G4000-L3-4XGS Series	v6.0
RKS-G4000-L2 Series	v6.0
RKS-G4000-L3 Series	v6.0

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.

- **YES:** Supported
- **PARTIAL:** Partially supported
- **–**: Unsupported

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

Options Menu

Settings	MDS-G4000-L2 Series	MDS-G4000-L2-4XGS Series	MDS-G4000-L3 Series	MDS-G4000-L3-4XGS Series	RKS-G4000-L2 Series	RKS-G4000-L3 Series
Locator	YES	YES	YES	YES	YES	YES
Reboot	YES	YES	YES	YES	YES	YES
Reset to Default Settings	YES	YES	YES	YES	YES	YES
Auto-save to Startup	YES	YES	YES	YES	YES	YES
Advanced Mode	YES	YES	YES	YES	YES	YES
Change Language	YES	YES	YES	YES	YES	YES
Log Out	YES	YES	YES	YES	YES	YES

System

Settings	MDS-G4000-L2 Series	MDS-G4000-L2-4XGS Series	MDS-G4000-L3 Series	MDS-G4000-L3-4XGS Series	RKS-G4000-L2 Series	RKS-G4000-L3 Series
System Management	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**
Information Settings	YES	YES	YES	YES	YES	YES
Firmware Upgrade	YES	YES	YES	YES	YES	YES
Config Backup and Restore	YES	YES	YES	YES	YES	YES
Account Management	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**
User Accounts	YES	YES	YES	YES	YES	YES
Online Accounts	YES	YES	YES	YES	YES	YES
Password Policy	YES	YES	YES	YES	YES	YES
Management Interface	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**
User Interface	YES	YES	YES	YES	YES	YES
Hardware Interfaces	YES	YES	YES	YES	YES	YES
SNMP	YES	YES	YES	YES	YES	YES
RMON1 (Only in CLI)	YES	YES	YES	YES	YES	YES
Time	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**
System Time	YES	YES	YES	YES	YES	YES
NTP Server	YES	YES	YES	YES	YES	YES
Time Synchronization	YES	YES	YES	YES	YES	YES

Port

Settings	MDS-G4000-L2 Series	MDS-G4000-L2-4XGS Series	MDS-G4000-L3 Series	MDS-G4000-L3-4XGS Series	RKS-G4000-L2 Series	RKS-G4000-L3 Series
Port Interface	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**
Port Settings	YES	YES	YES	YES	YES	YES
Linkup Delay	YES	YES	YES	YES	YES	YES
Link Aggregation	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**
PoE (for PoE models)	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**

Layer 2 Switching

Settings	MDS-G4000-L2 Series	MDS-G4000-L2-4XGS Series	MDS-G4000-L3 Series	MDS-G4000-L3-4XGS Series	RKS-G4000-L2 Series	RKS-G4000-L3 Series
VLAN	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**
GARP	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**
MAC	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**
Static Unicast	YES	YES	YES	YES	YES	YES
MAC Address Table	YES	YES	YES	YES	YES	YES
QoS	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**
Classification	YES	YES	YES	YES	YES	YES
Ingress Rate Limit	YES	YES	YES	YES	YES	YES

Settings	MDS-G4000-L2 Series	MDS-G4000-L2-4XGS Series	MDS-G4000-L3 Series	MDS-G4000-L3-4XGS Series	RKS-G4000-L2 Series	RKS-G4000-L3 Series
Scheduler	YES	YES	YES	YES	YES	YES
Egress Shaper	YES	YES	YES	YES	YES	YES
Multicast	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**
IGMP Snooping	YES	YES	YES	YES	YES	YES
GMRP	YES	YES	YES	YES	YES	YES
Static Multicast	YES	YES	YES	YES	YES	YES

IP Configuration

Settings	MDS-G4000-L2 Series	MDS-G4000-L2-4XGS Series	MDS-G4000-L3 Series	MDS-G4000-L3-4XGS Series	RKS-G4000-L2 Series	RKS-G4000-L3 Series
IP Configuration	**YES**	**YES**	**-**	**-**	**YES**	**-**

Network Interface

Settings	MDS-G4000-L2 Series	MDS-G4000-L2-4XGS Series	MDS-G4000-L3 Series	MDS-G4000-L3-4XGS Series	RKS-G4000-L2 Series	RKS-G4000-L3 Series
Network Interface	**-**	**-**	**YES**	**YES**	**-**	**YES**

Redundancy

Settings	MDS-G4000-L2 Series	MDS-G4000-L2-4XGS Series	MDS-G4000-L3 Series	MDS-G4000-L3-4XGS Series	RKS-G4000-L2 Series	RKS-G4000-L3 Series
Layer 2 Redundancy	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**
Spanning Tree	YES	YES	YES	YES	YES	YES
Turbo Ring v2	YES	YES	YES	YES	YES	YES
Turbo Chain	YES	YES	YES	YES	YES	YES
MRP	YES	YES	YES	YES	YES	YES
Multiple Dual Homing	YES	YES	YES	YES	YES	YES
Multiple Network Coupling	YES	YES	YES	YES	YES	YES
IEC 62439-3	**YES**	**YES**	-	-	-	-
PRP/HSR	YES	YES	-	-	-	-
Supervision Frame	YES	YES	-	-	-	-
Layer 3 Redundancy	-	-	**YES**	**YES**	-	**YES**
VRRP	-	-	**YES**	**YES**	-	**YES**
Tracking	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**

Network Service

Settings	MDS-G4000-L2 Series	MDS-G4000-L2-4XGS Series	MDS-G4000-L3 Series	MDS-G4000-L3-4XGS Series	RKS-G4000-L2 Series	RKS-G4000-L3 Series
DHCP Server	**YES**	**YES**	**-**	**-**	**YES**	**-**

Settings	MDS-G4000-L2 Series	MDS-G4000-L2-4XGS Series	MDS-G4000-L3 Series	MDS-G4000-L3-4XGS Series	RKS-G4000-L2 Series	RKS-G4000-L3 Series
DHCP Relay Agent	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**
DNS Settings	**-**	**-**	**YES**	**YES**	**-**	**YES**

Routing

Settings	MDS-G4000-L2 Series	MDS-G4000-L2-4XGS Series	MDS-G4000-L3 Series	MDS-G4000-L3-4XGS Series	RKS-G4000-L2 Series	RKS-G4000-L3 Series
Unicast Route	**-**	**-**	**YES**	**YES**	**-**	**YES**
Static Routing	-	-	YES	YES	-	YES
RIP	-	-	YES	YES	-	YES
OSPF	-	-	YES	YES	-	YES
Routing Table	-	-	YES	YES	-	YES
Multicast Route	**-**	**-**	**YES**	**YES**	**-**	**YES**
PIM-DM	-	-	YES	YES	-	YES
PIM-SM	-	-	YES	YES	-	YES
Multicast Local Route	-	-	YES	YES	-	YES
Multicast Routing Table	-	-	YES	YES	-	YES
BFD	**-**	**-**	**YES**	**YES**	**-**	**YES**

Security

Settings	MDS-G4000-L2 Series	MDS-G4000-L2-4XGS Series	MDS-G4000-L3 Series	MDS-G4000-L3-4XGS Series	RKS-G4000-L2 Series	RKS-G4000-L3 Series
Device Security	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**
Login Policy	YES	YES	YES	YES	YES	YES
Trusted Access	YES	YES	YES	YES	YES	YES
SSH & SSL	YES	YES	YES	YES	YES	YES
Network Security	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**
IEEE 802.1X	YES	YES	YES	YES	YES	YES
MAC Authentication Bypass	YES	YES	YES	YES	YES	YES
MACsec	YES	YES	YES	YES	YES	YES
Port Security	YES	YES	YES	YES	YES	YES
Traffic Storm Control	YES	YES	YES	YES	YES	YES
Access Control List	YES	YES	YES	YES	YES	YES
Network Loop Protection	YES	YES	YES	YES	YES	YES
Binding Database	YES	YES	YES	YES	YES	YES
DHCP Snooping	YES	YES	YES	YES	YES	YES
IP Source Guard	YES	YES	YES	YES	YES	YES
Dynamic ARP Inspection	YES	YES	YES	YES	YES	YES
Authentication	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**

Settings	MDS-G4000-L2 Series	MDS-G4000-L2-4XGS Series	MDS-G4000-L3 Series	MDS-G4000-L3-4XGS Series	RKS-G4000-L2 Series	RKS-G4000-L3 Series
Login Authentication	YES	YES	YES	YES	YES	YES
RADIUS	YES	YES	YES	YES	YES	YES
TACACS+	YES	YES	YES	YES	YES	YES

Diagnostics

Settings	MDS-G4000-L2 Series	MDS-G4000-L2-4XGS Series	MDS-G4000-L3 Series	MDS-G4000-L3-4XGS Series	RKS-G4000-L2 Series	RKS-G4000-L3 Series
System Status	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**
Resource Utilization	YES	YES	YES	YES	PARTIAL	PARTIAL
Fiber Check	YES	YES	YES	YES	YES	YES
Module Information	YES	YES	YES	YES	YES	YES
Network Status	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**
Network Statistics	YES	YES	YES	YES	YES	YES
LLDP	YES	YES	YES	YES	YES	YES
ARP Table	YES	YES	YES	YES	YES	YES
Tools	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**
Port and VLAN Mirroring	YES	YES	YES	YES	YES	YES
Ping	YES	YES	YES	YES	YES	YES
Event Logs and Notifications	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**

Settings	MDS-G4000-L2 Series	MDS-G4000-L2-4XGS Series	MDS-G4000-L3 Series	MDS-G4000-L3-4XGS Series	RKS-G4000-L2 Series	RKS-G4000-L3 Series
Event Logs	YES	YES	YES	YES	YES	YES
Event Notifications	YES	YES	YES	YES	YES	YES
Syslog	YES	YES	YES	YES	YES	YES
SNMP Trap / Inform	YES	YES	YES	YES	YES	YES
Email Settings	YES	YES	YES	YES	YES	YES
Relay Alarm	YES	YES	YES	YES	YES	YES

Note

Power utilization monitoring is only supported for MDS devices.

Industrial Application

Settings	MDS-G4000-L2 Series	MDS-G4000-L3 Series	MDS-G4000-L2-4XGS Series	MDS-G4000-L3-4XGS Series	RKS-G4000-L2 Series	RKS-G4000-L3 Series
IEC 61850	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**
MMS	YES	YES	YES	YES	YES	YES
GOOSE Check	YES	YES	YES	YES	YES	YES
Modbus TCP	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**
EtherNet / IP	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**
PROFINET	**YES**	**YES**	**YES**	**YES**	**YES**	**YES**

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

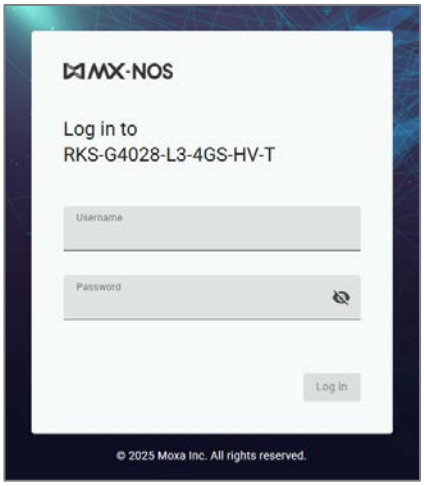
Perform the following steps to access the device's web interface:

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 (**192.168.127.253** 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

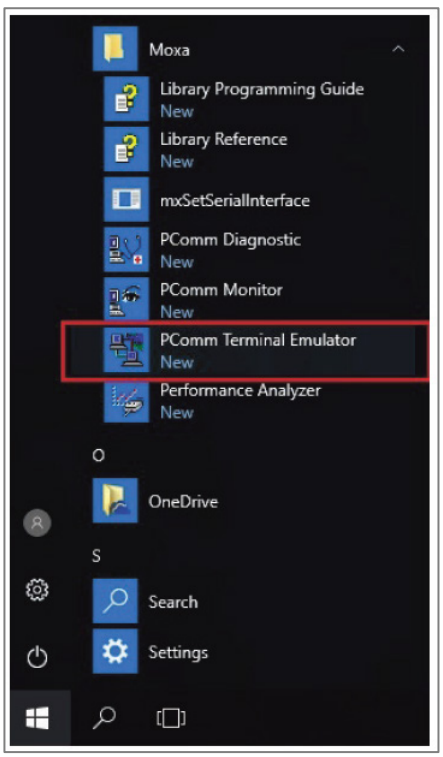
You can connect to your device's serial console port to configure settings.

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

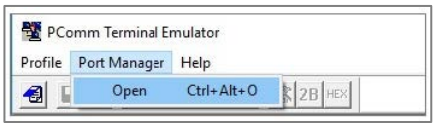
1. Prepare an RS-232 serial cable with an RJ45 interface.
2. Connect the RJ45 interface end to the console port on the device, and the other end to your computer.
3. We recommend you use PComm Terminal Emulator for serial communication. The software can be downloaded free of charge from Moxa's website.

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

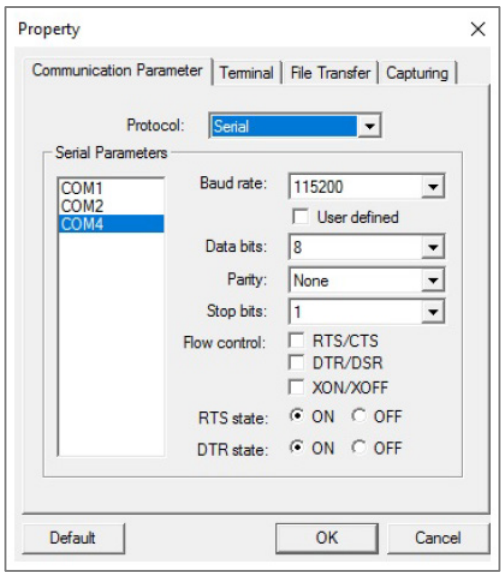
1. From the Windows desktop, click **Start > Moxa > PComm Terminal Emulator**.



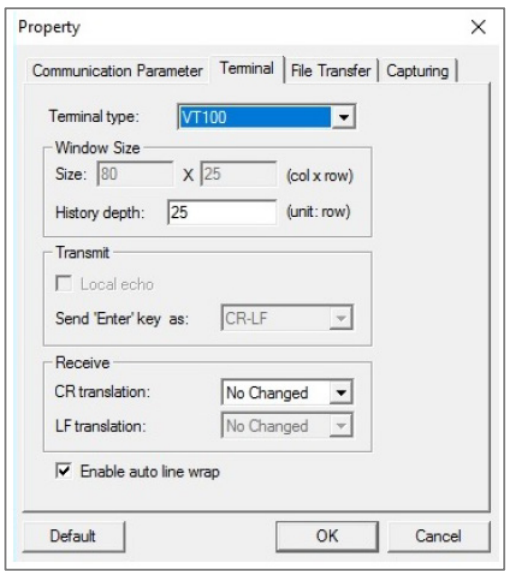
2. Select **Open** under the **Port Manager** menu to open a new connection.



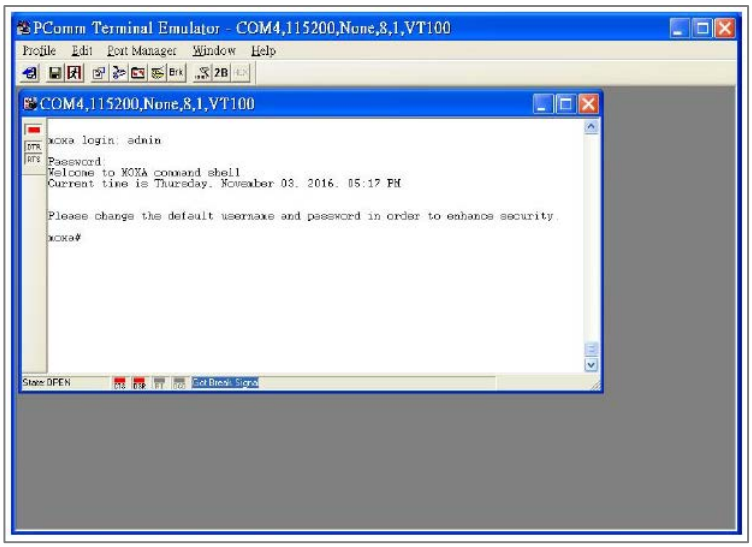
3. The **Property** window should open. In the **Communication Parameter** tab for **Ports**, select the COM port that is being used for the console connection. Set the other fields as follows: **115200** for **Baud Rate**, **8** for **Data Bits**, **None** for **Parity**, and **1** for **Stop Bits**.



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



5. 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).



6. 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.

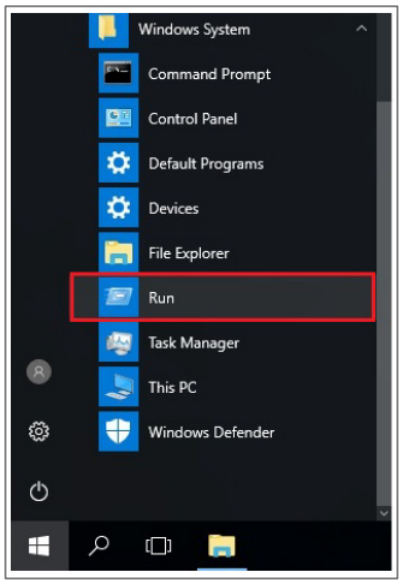
Using Telnet to Configure the Device

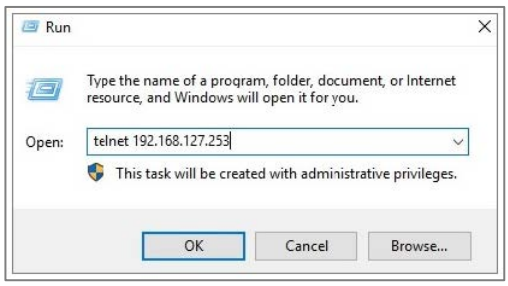
You can use Telnet to connect to the device and configure it. This requires the host and the target device to configure to be on the same logical subnet, so you may need to adjust your PC host's IP address and subnet mask. By default, the device IP address is **192.168.127.253** and the default subnet 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.

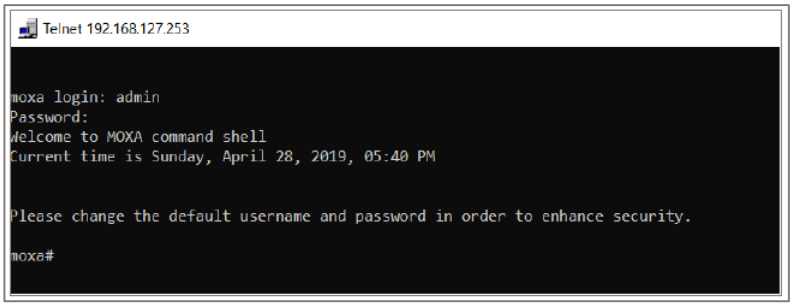
After making sure that the device is connected to the same LAN and logical subnet as your PC, perform these steps to connect to your device:

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

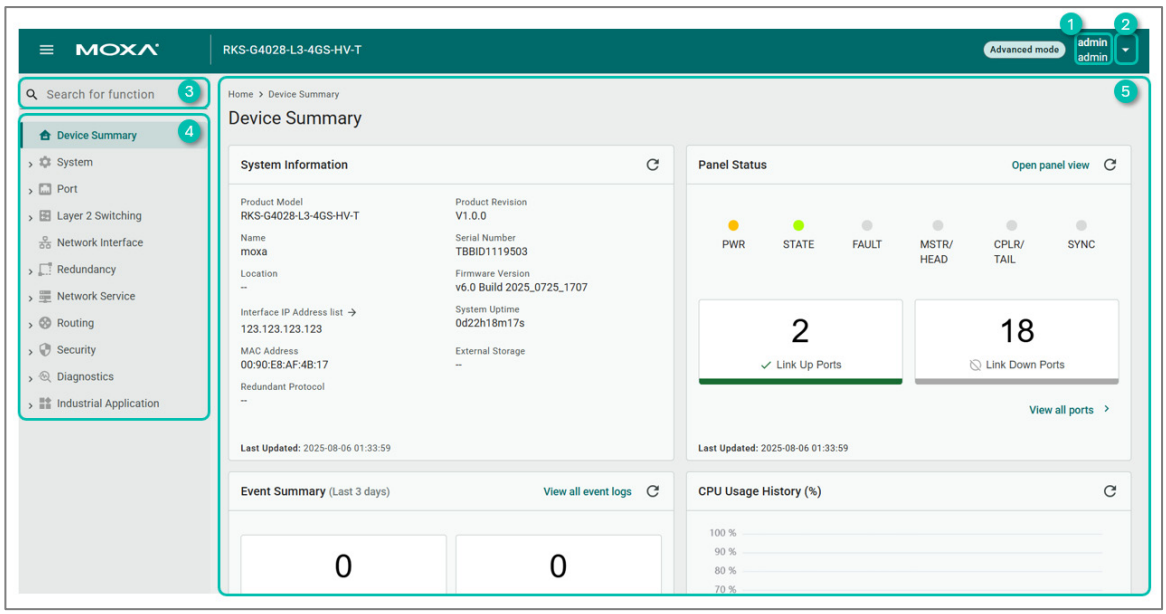
The rest of this section follows the order of the menu areas in the user interface:

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:

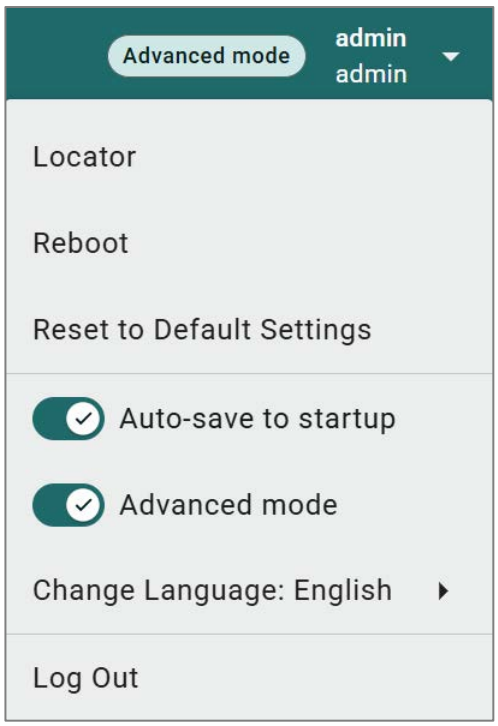


1. **Login Name:** Indicates the current user's account privilege at the top and their account name at the bottom.
2. **Options Menu:** Allows the user to perform various operations, including the locator function, resetting the device to its default configuration, and modifying the configuration mode, etc.
    - **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 User Accounts for more information on user accounts.

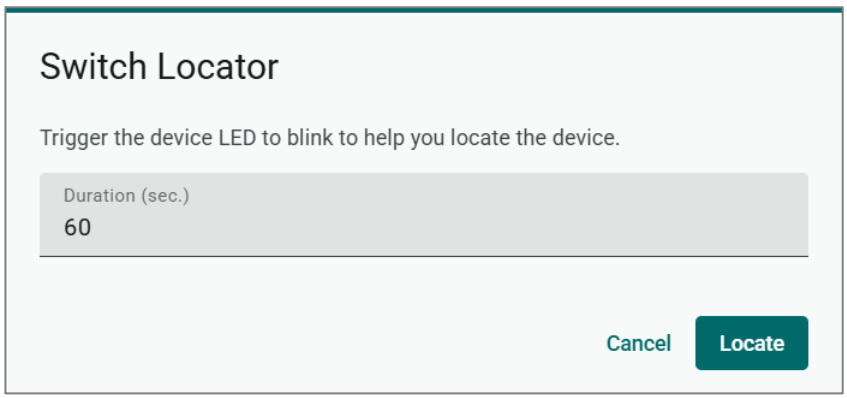
Settings	Admin	Supervisor	User
Locator	R/W	R/W	R
Reboot	R/W	R/W	-
Reset to Default Settings	R/W	-	-
Auto-save to Startup	R/W	R/W	-
Advanced Mode	R/W	R/W	R/W

Settings	Admin	Supervisor	User
Change Language	R/W	R/W	R/W
Log Out	R/W	R/W	R/W

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**.

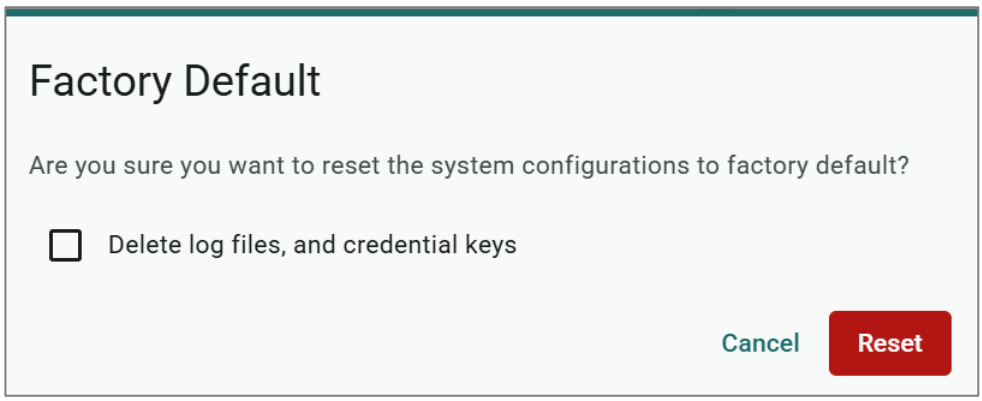
Reset to Default Settings

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.



Auto-save to Startup

Auto-save to Startup 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 to Startup is enabled by default.

To enable or disable auto-saving to the startup configuration, click the **Options ( )** icon in the upper-right corner of the page, and toggle **Auto-save to startup**.

When auto-saving is disabled, you can save configuration changes to the startup configuration by clicking the **Save ( )** icon.

Note

When auto-saving 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.

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 switch on/off the **Advanced mode** button.

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**.

Log Out

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

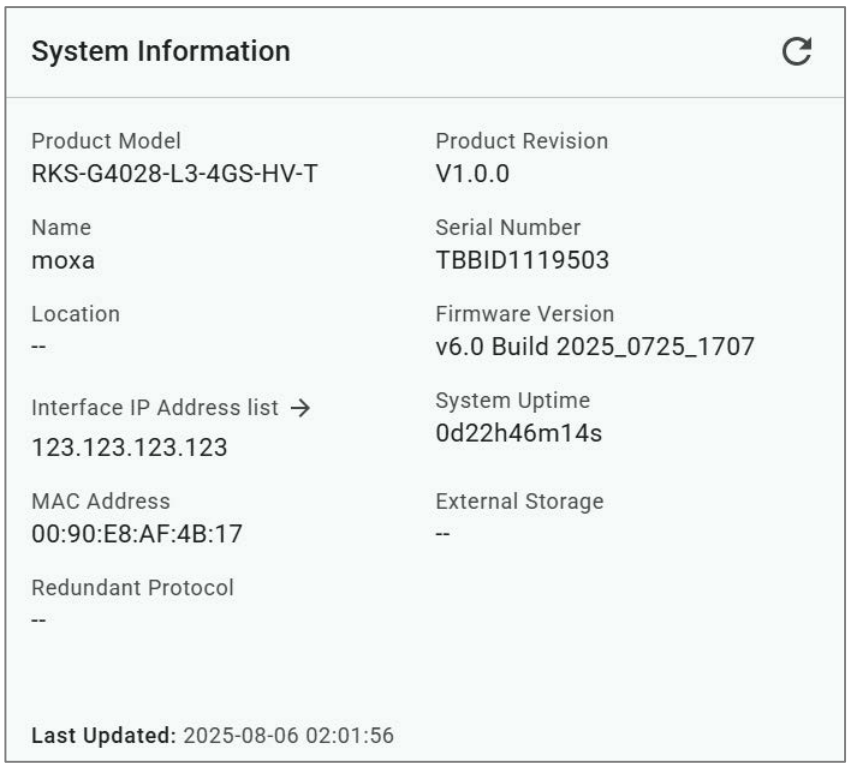
Device Summary

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.

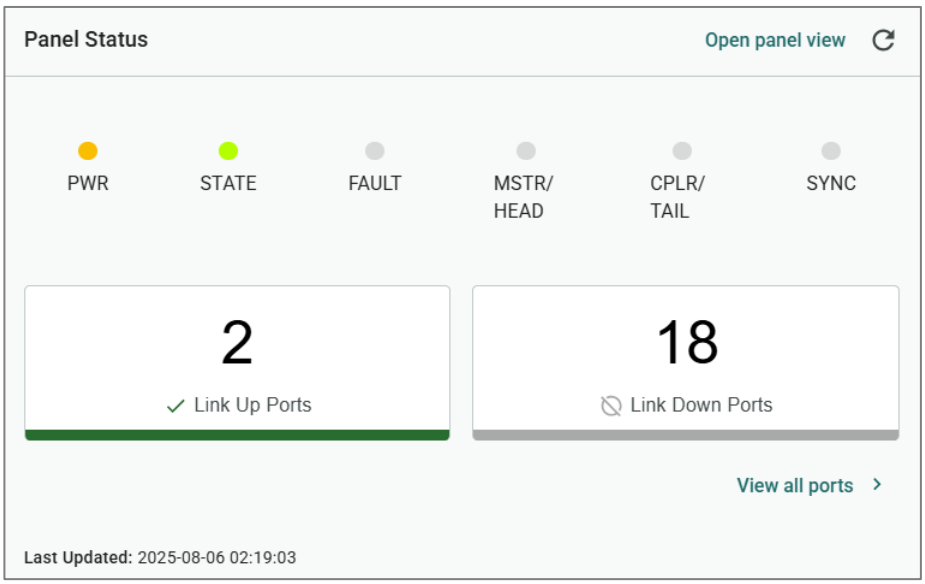


UI Setting	Description
Product Model	Shows the product model of the device.
Name	Shows the name of the device. Refer to System > System Management > Information Settings for more information.

UI Setting	Description
Location	Shows the location of the device. Refer to System > System Management > Information Settings for more information.
Interface IP Address list	Shows the Interface IP Address list of the device. Click the arrow icon to navigate to the **Network Interface** page. Refer to Network Interface for more information.
MAC Address	Shows the MAC address of your device.
Redundant Protocol	Shows the current redundancy protocol for this switch.
Product Revision	Shows the product revision of the device.
Serial Number	Shows the serial number of your device.
Firmware Version	Shows the firmware version of your device.
System Uptime	Shows the amount of time your device has been continuously running for.
External Storage	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 **View all ports** to view more detailed information, or click **Close** to return to the compact view.



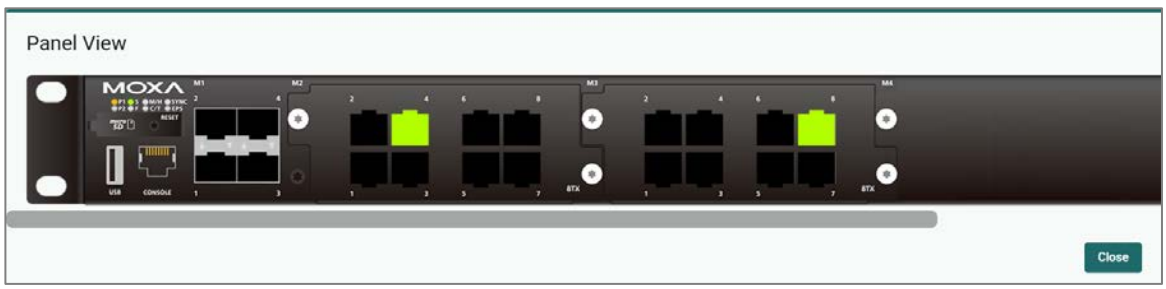
Panel View

By clicking **Open panel view** 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.

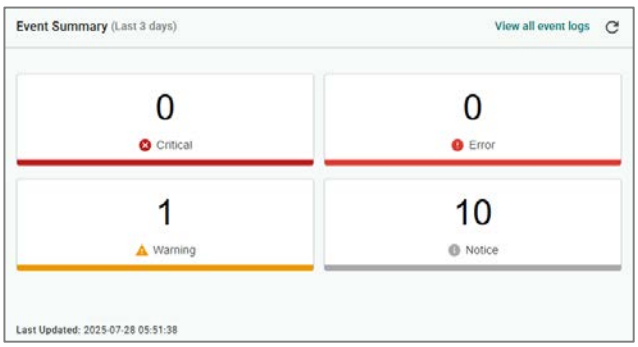
Click **Close** to close the **Panel View** and show the **Panel Status** again.

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



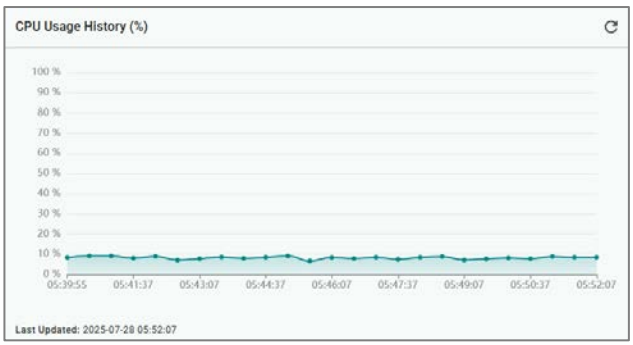
Event Summary (Last 3 days)

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 User Accounts for more information on user accounts.

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

Settings	Admin	Supervisor	User
User Interface	R/W	-	-
Hardware Interfaces	R/W	R/W	R
SNMP	R/W	-	-
RMON1 (Only in CLI)	R/W	R/W	R
Time			
System Time	R/W	R/W	R
NTP Server	R/W	R/W	R
Time Synchronization	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:

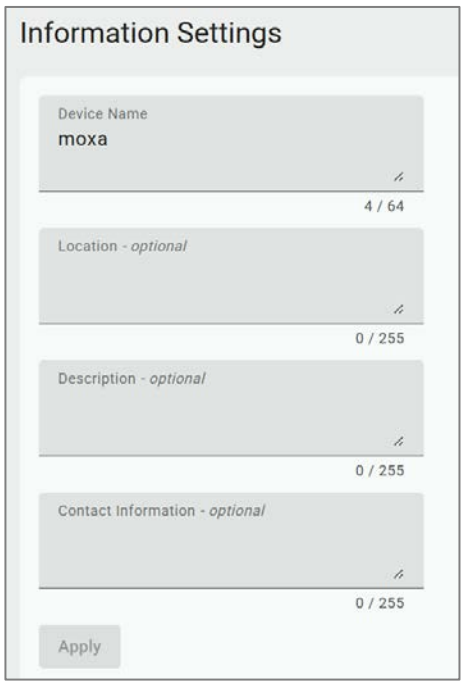
- Information Settings
- Firmware Upgrade
- Config Backup and Restore

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.



UI Setting	Description	Valid Range	Default Value
Device Name	Specify a name for the device. This helps you differentiate between the roles or applications of different devices.	1 to 64 characters • characters: a-z, A-Z, 0-9 • special characters: .- • The device name cannot start with– (dash) and cannot end with–(dash).	moxa
Location	Specify a location for the device. This helps you differentiate between different locations or sites for different devices.	0 to 255 characters • characters: a-z, A-Z, 0-9 • special characters: ~ ! @ # $ % ^ & * ( ) { } [ ] < > _ + - = \ : ; , . /	N/A
Description	Specify a description for the device. This helps you keep a more detailed description of the device.	0 to 255 characters	N/A
Contact Information	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

This section lets you upgrade the firmware through the following methods:

- Local
- TFTP
- SFTP
- USB
- microSD

> **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.

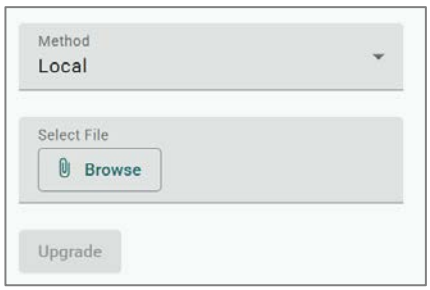
> **Warning**
>
> Upgrading the firmware should be only be done by qualified personnel, as it is possible to render the device inoperable if the upgrade is not done properly. If you are not familiar with the process, please request the assistance of qualified personnel. You can also consult with Moxa 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).



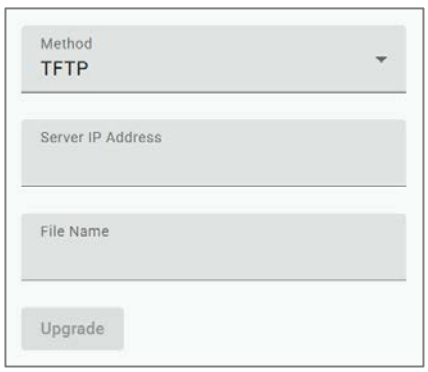
UI Setting	Description	Valid Range	Default Value
Select File	Select the new firmware file (*.rom) to use from your computer.	Select a file from your computer	N/A

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.

Note

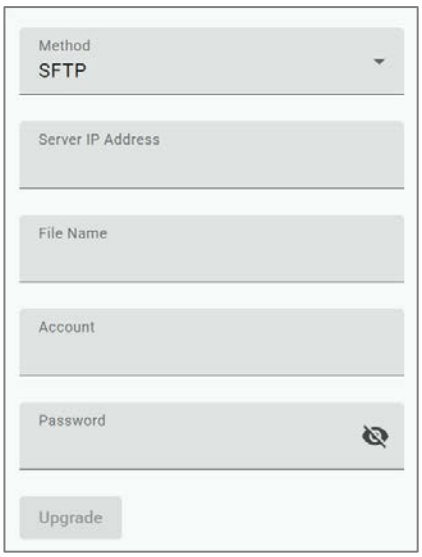
This feature supports weaker authentication or encryption, and may not be secure over untrusted networks. Take appropriate security precautions.



UI Setting	Description	Valid Range	Default Value
Server IP Address	Specify the IP address of the TFTP server where the new firmware file (*.rom) is located.	Valid IP address	N/A
File Name	Specify the filename of the new firmware, including its full path on the server. Example: /path_to_firmware_file/firmware_file.rom **Note** If a path is not specified, the default folder for the server will be used.	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.



UI Setting	Description	Valid Range	Default Value
Server IP Address	Specify the IP address of the SFTP server where the new firmware file (*.rom) is located.	Valid IP address	N/A

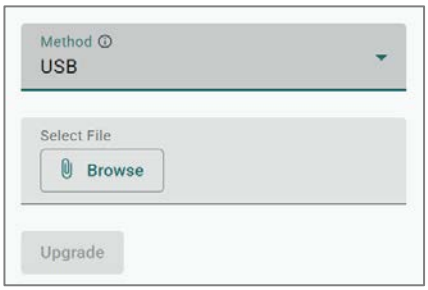
UI Setting	Description	Valid Range	Default Value
File Name	Specify the filename of the new firmware, including its full path on the server. Example: /path_to_firmware_file/firmware_file.rom **Note** If a path is not specified, the default folder for the server will be used.	File name can only contain A-Z, a-z, 0-9 or the symbols -._().	N/A
Account	Enter the SFTP server account name to use to connect to the SFTP server.	Account	N/A
Password	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.

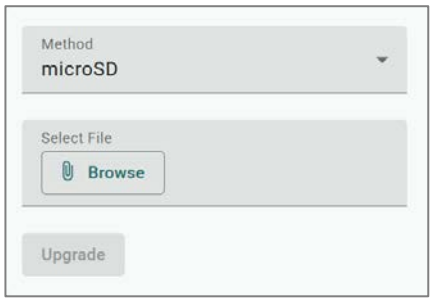


UI Setting	Description	Valid Range	Default Value
Select File	Select the new firmware file (*.rom) to use from your USB device.	Select a file from the USB device	N/A

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
Select File	Select the new firmware file (*.rom) to use from the microSD card.	Select a file from the microSD card	N/A

Creating a Configuration Backup

Backup known-good configurations to restore devices to secure states.

- Make sure all device has been configured to known-good, known-secure settings. Refer to the Security Hardening Guide for more information.
- Configure **File Signature** and **Import Custom Key** to help reduce the risk of tampering.
- Configure **File Encryption** to help avoid exposing sensitive information in the event of coconfiguration backup compromise.

1. Sign in to the device with administrator credentials.
2. Go to **System** > **System Management** > **Config Backup and Restore** > **Backup**.

3. For **Method**, select an option for backup.

Option	Description
Local	Backs up configuration to local host. For **Select Configuration**, select **Running Configuration** or **Startup Configuration**. For **Default Configuration**, select **Not Included** or **Included**.
TFTP	Uses a remote TFTP server. Specify **Server IP Address** and **File Name**. **Note** Specify a path as part of File Name in the format /path_to_configuration_file/configuration_file.conf. If a path is not specified, the default folder for the server will be used.
SFTP	As TFTP, with the addition of **Account** and **Password** for authentication.
USB	Uses a Moxa ABC-02 configuration tool connected to the device. **Note** Requires enabling USB Function under System > Management Interface > Hardware.
microSD	Uses a microSD card inserted into your device. **Note** Requires enabling USB Function under System > Management Interface > Hardware.

The configuration backup begins.

Note

Configure Auto Configuration Backup to automatically backup to USB or microSD whenever the configuration changes.

Specify Configuration Name and then select **Apply**.

Restoring a Configuration Backup

Restore previously-backed up configurations to recover devices to known-good, secure states.

If your backup has been configured with **File Signature** or **File Encryption**, make sure that the proper keys or passwords are configured before proceeding.

1. Sign in to the device with administrator credentials.

2. Go to **System** > **System Management** > **Config Backup and Restore** > **Restore**.
3. For **Method**, select an option for restoration.

Method	Description
Local	Restores a configuration from a file on the local host. To choose a file, select **Browse**.
TFTP	Uses a remote TFTP server. Specify **Server IP Address** and **File Name**.**Important:** Specify a path as part of **File Name** in the format `/path_to_configuration_file/configuration_file.conf`. If a path is not specified, the default folder for the server will be used.
SFTP	As TFTP, with the addition of **Account** and **Password** for authentication.
USB	Uses a Moxa ABC-02 configuration tool connected to the device.**Note:** Requires enabling **USB Function** under **System** > **Management Interface** > **Hardware**.
microSD	Uses a microSD card inserted into your device.**Note:** Requires enabling **USB Function** under **System** > **Management Interface** > **Hardware**.

4. Select **Restore** to start the restoration process.

The restoration process begins.

> **Note**
>
> Configure Auto Configuration Restore to automatically restore from USB or microSD whenever the device restarts.

Configuration Backup and Restore

Menu Path: System > System Management > Config 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

Backup

Menu Path: System > System Management > Config Backup and Restore - Backup

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

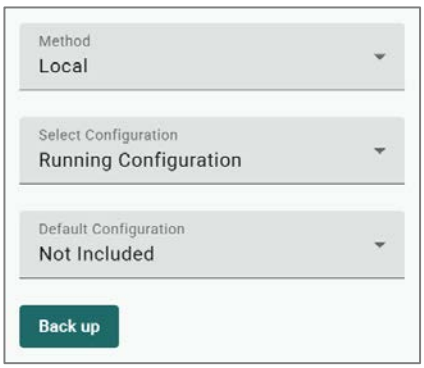
There are multiple methods of backing up the device configuration:

- 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.

Backup - Local

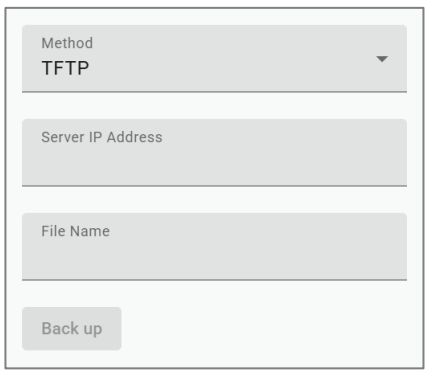
If you select **Local** as your **Method**, these settings will appear. The Local method will export the configuration backup file to the local host.



UI Setting	Description	Valid Range	Default Value
Select Configuration	Select whether to back up the running configuration or the startup configuration of the switch. Refer to Auto-save to Startup for more information.	Running Configuration / Startup Configuration	Running Configuration
Default Configuration	Choose to back up the configuration with or without default settings.	Not Included / Included	Not Included

Backup - TFTP

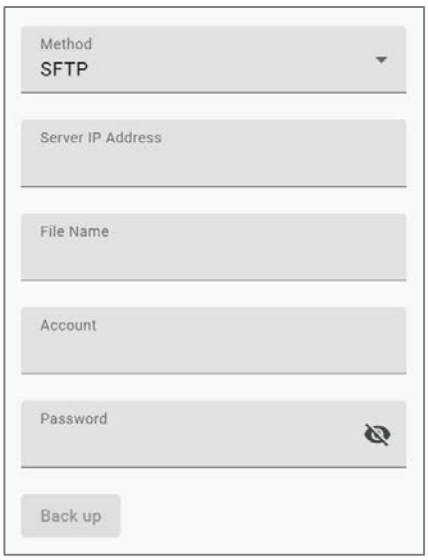
If you select **TFTP** as your **Method**, these settings will appear. The TFTP method lets you back up the startup configuration to a remote TFTP server.



UI Setting	Description	Valid Range	Default Value
Server IP Address	Specify the IP address of the TFTP server to upload the backup of the startup configuration to.	Valid IP address	N/A
File Name	Specify a filename for the backup, including its full path on the server. Example: /path_to_configuration_file/configuration_file.conf **Note** If a path is not specified, the default folder for the server will be used.	N/A	N/A

Backup - SFTP

If you select **SFTP** as your **Method**, these settings will appear. The SFTP method lets you back up the startup configuration to a remote SFTP server.



UI Setting	Description	Valid Range	Default Value
Server IP Address	Specify the IP address of the SFTP server to upload the backup of the startup configuration to.	Valid IP address	N/A
File Name	Specify a filename for the backup, including its full path on the server. Example: /path_to_configuration_file/configuration_file.conf **Note** If a path is not specified, the default folder for the server will be used.	File name can only contain A-Z, a-z, 0-9 or the symbols -._().	N/A
Account	Enter the SFTP server account name to use to connect to the SFTP server.	N/A	N/A
Password	Enter the SFTP server account password to use to connect to the SFTP server.	N/A	N/A

Backup - USB

If you select **USB** as your **Method,** these settings will appear. The USB method allows you to back up the startup configuration 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 startup configuration.

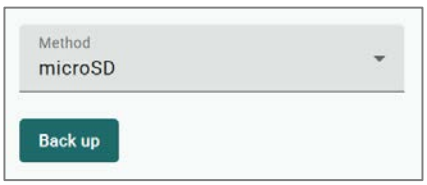
> **Note**
>
> To use this feature, USB Function must be enabled in System > Management Interface > Hardware Interface.



Backup - microSD

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

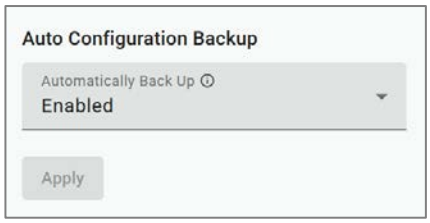
> **Note**
>
> To use this feature, microSD Function must be enabled in System > Management Interface > Hardware Interfaces.



Auto Configuration Backup

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

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



UI Setting	Description	Valid Range	Default Value
Automatically Back Up	When enabled, this will back up the startup configuration to an inserted ABC-02 configuration tool or microSD card whenever the startup configuration changes. **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.	Enabled / Disabled	Enabled

Restore

Menu Path: System > System Management > Config Backup and Restore - Restore

This page lets you restore a previously backed up configuration.

Note

Configurations are restored to the running configuration.

If Auto-save to Startup is disabled, the restored configuration will not be saved to the startup configuration, and the device will revert to its current startup configuration if the device is rebooted.

To save the restored configuration to the startup configuration, click the Save ( ) icon or enable Auto-save to Startup.

Refer to Auto-save to Startup for more information.

Note

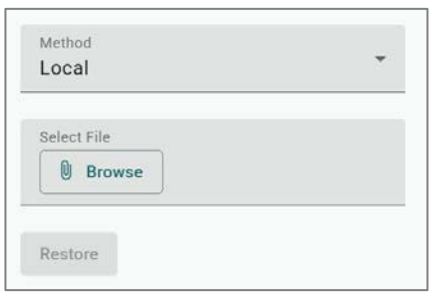
To ensure that configuration files can be imported successfully, do not modify the configuration files manually.

There are multiple methods of restoring the device configuration:

- Local
- TFTP
- SFTP
- USB
- microSD

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.

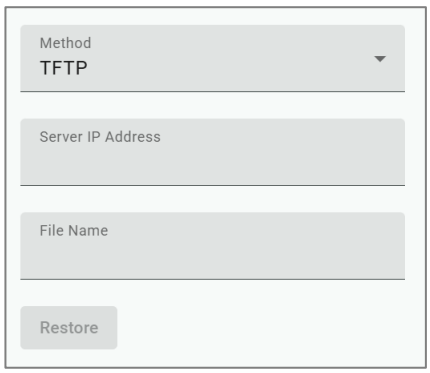


UI Setting	Description	Valid Range	Default Value
Select File	Select the configuration file to use from your computer.	Select a file from your computer	N/A

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.

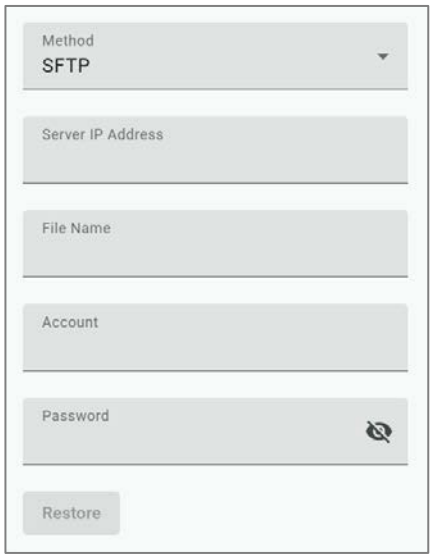
> **Note**
>
> This feature supports weaker authentication or encryption, and may not be secure over untrusted networks. Take appropriate security precautions.



UI Setting	Description	Valid Range	Default Value
Server IP Address	Specify the IP address of the TFTP server.	Valid IP address	N/A
File Name	Specify the file name of the configuration file to restore from, including its full path on the server. Example: /path_to_configuration_file/configuration_file.conf **Note** If a path is not specified, the default folder for the server will be used.	Up to 54 characters, including file extension. File name can only contain the characters A-Z, a-z, 0-9, and special characters -._().	N/A

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.



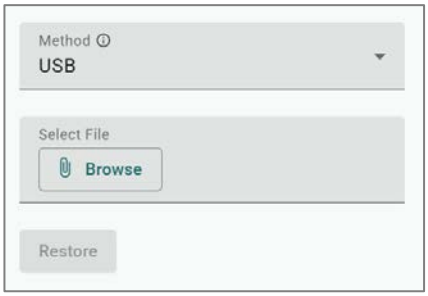
UI Setting	Description	Valid Range	Default Value
Server IP Address	Specify the IP address of the SFTP server where the configuration file is stored.	Valid IP address	N/A
File Name	Specify the file name of the configuration file to restore from, including its full path on the server. Example: /path_to_configuration_file/configuration_file.conf **Note** If a path is not specified, the default folder for the server will be used.	File name can only contain the characters A-Z, a-z, 0-9, and special characters -._().	N/A
Account	Enter the SFTP server account name to use to connect to the SFTP server.	Account	N/A
Password	Enter the SFTP server account password to use to connect to the SFTP server.	Password	N/A

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.



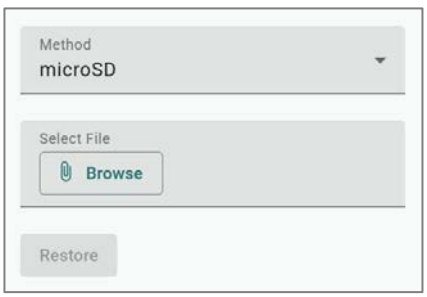
UI Setting	Description	Valid Range	Default Value
Select File	Select the configuration file to use from your USB device.	Select a file from the USB device	N/A

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.

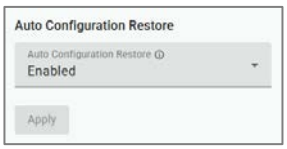


UI Setting	Description	Valid Range	Default Value
Select File	Select the configuration file to use from the microSD card.	Select a file from the microSD card	N/A

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
Automatically Restore	When enabled, this will restore the device's configuration from an inserted ABC-02 configuration tool or microSD card whenever the device is rebooted. **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.	Enabled / Disabled	Enabled

File Encryption

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

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



UI Setting	Description	Valid Range	Default Value
Configuration File Encryption	Select which file encryption mode to use. **Encrypt sensitive information only:** Only sensitive information will be encrypted in the configuration file. **Encrypt the entire file:** The entire configuration file will be encrypted. **Note** Sensitive information includes passwords used for authentication and the encryption key used to encrypt data.	Encrypt sensitive information only / Encrypt whole file	Encrypt sensitive information only
Encryption Key	Specify an encryption key to use for configuration files. **Note** If no encryption key is specified, then the Moxa encryption key will be used.	0 to 60 characters	Blank (the Moxa encryption key will be used)

File Signature

Menu Path: System > System Management > Config 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



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

File Signature Key List



UI Setting	Description
Label	Shows the label used to help identify the key.
Algorithm	Shows the algorithm used for the key, such as RSA or ECDSA.
Length	Shows the length of the key in bits.

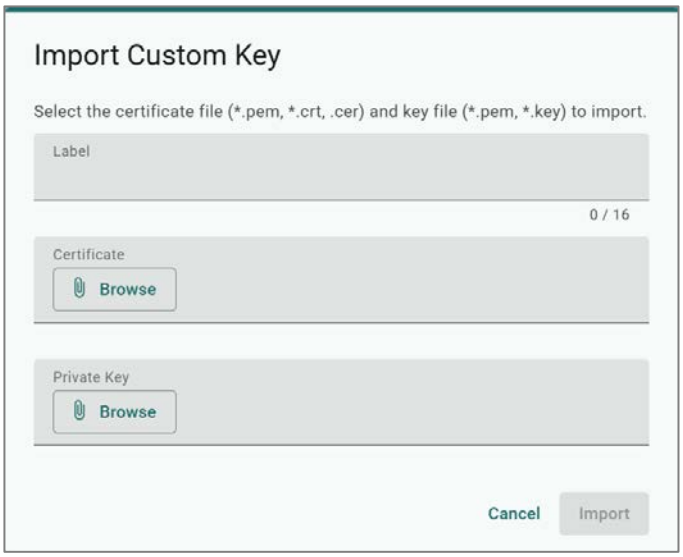
Import Custom Key

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

Clicking the **Import Custom Key** button on the **System > System Management > Config 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 **Import** to save your changes and add the new key.

Once the File Signature Key is imported, you can click the **Manage** button to: edit the label, import a new custom key, or delete the current key.



UI Setting	Description	Valid Range	Default Value
Label	Specify a label to help describe the certificate and the key.	0 to 16 characters	N/A

UI Setting	Description	Valid Range	Default Value
Certificate	Select a certificate file to import from your computer.	Select a certificate file from your computer	N/A
Key	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

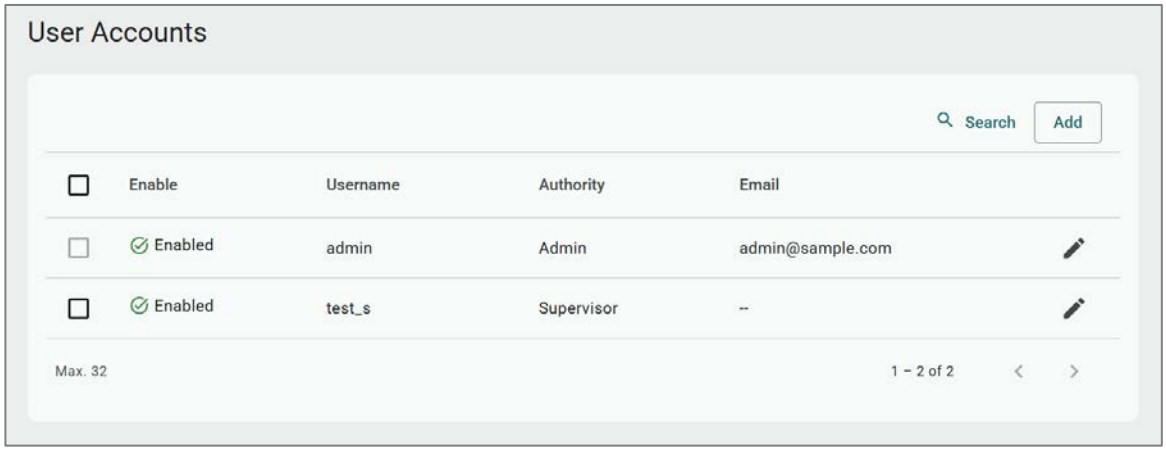
This page lets you manage the user accounts for your device.

Note

By default, there is only one account: admin

Limitations

You can create up to 32 users.



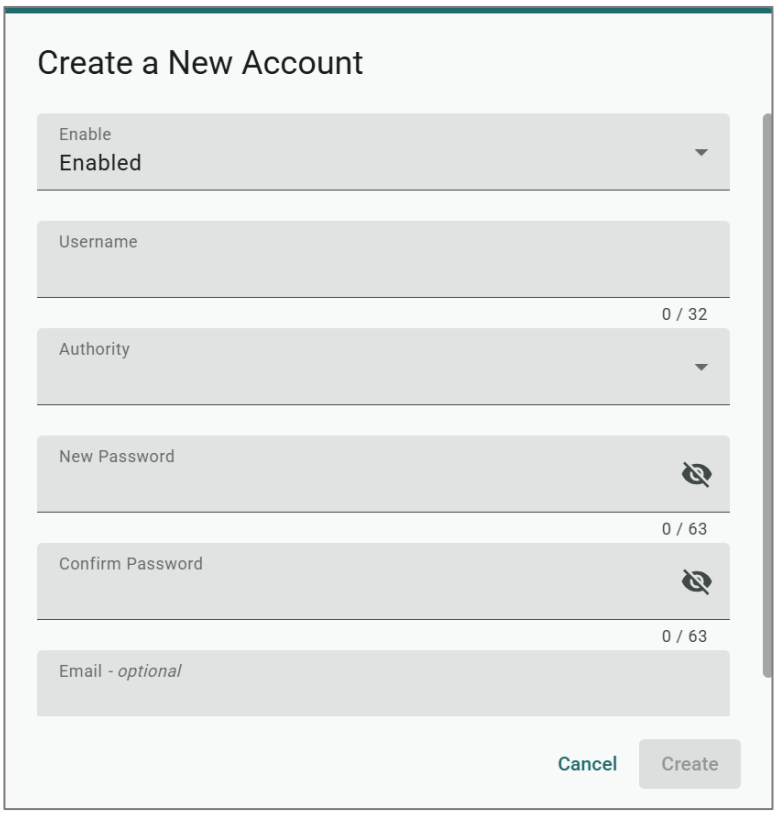
UI Setting	Description
Enable	Shows whether the account is enabled or disabled.
Username	Shows the username of the account.
Authority	Shows the authority level of the account.
Email	Shows the email address of the account.

User Accounts - Create a New Account

Menu Path: System > Account Management > User Accounts

Clicking the **Create** button on the 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.



UI Setting	Description	Valid Range	Default Value
Enable	Enable or disable the user account.	Enabled / Disabled	Enabled
Username	Specify a username for this account.	4 to 32 characters	N/A
Authority	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. • **Admin**: This account has read/write access of all configuration parameters. • **Supervisor**: This account has read/write access for a limited set of configuration parameters. • **User**: This account can only view a limited set of configuration parameters. **Note** In order to enhance security, we suggest you create a new account with the User authority.	Admin / Supervisor / User	N/A

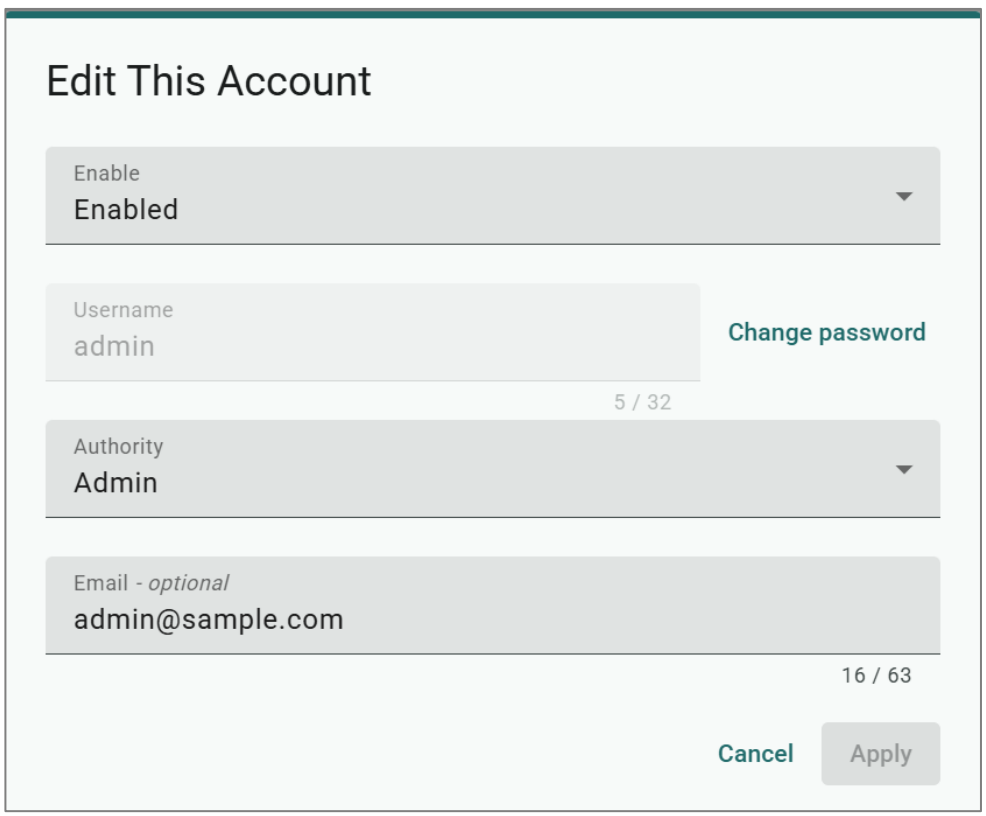
UI Setting	Description	Valid Range	Default Value
New Password	Specify the new password for this account.	4 to 63 characters, additional requirements are based on settings in **System > Account Management > Password Policy**	N/A
Confirm Password	Reenter the password to confirm.	4 to 63 characters, must match **New Password**	N/A
Email	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 for an account on the **System > Account Management > User Accounts** page will open this dialog box. This dialog lets you edit an existing user account.

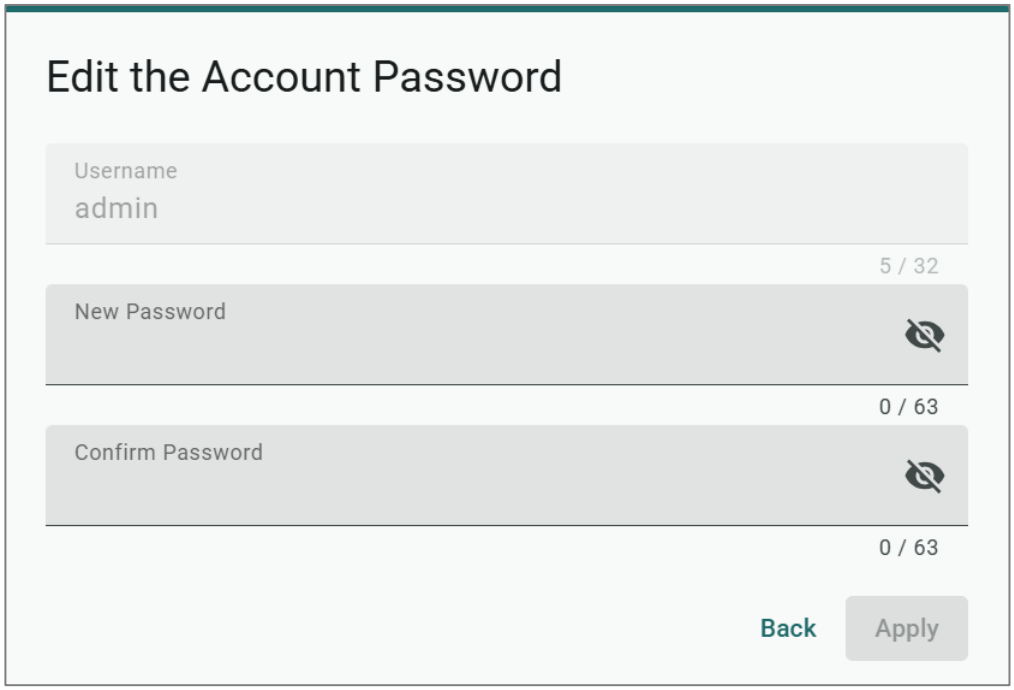
Click **Apply** to save your changes.



UI Setting	Description	Valid Range	Default Value
Enable	Enable or disable the user account.	Enabled / Disabled	Enabled
Username	Shows the username of the account. **Note** The username cannot be edited after creating an account.	N/A	N/A
Change Password	Click **Change password** to change the account password. Refer to Edit the Account Password for more information.	N/A	N/A
Authority	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. • **Admin**: This account has read/write access of all configuration parameters. • **Supervisor**: This account has read/write access for a limited set of configuration parameters. • **User**: This account can only view a limited set of configuration parameters.	Admin / Supervisor / User	N/A
Email	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.



UI Setting	Description	Valid Range	Default Value
Username	Shows the username of the account. **Note** The username cannot be edited after creating an account.	N/A	N/A
New Password	Specify the new password for this account.	4 to 63 characters, additional requirements are based on settings in **System > Account Management > Password Policy**	N/A
Confirm Password	Reenter the password to confirm.	4 to 63 characters, must match **New Password**	N/A

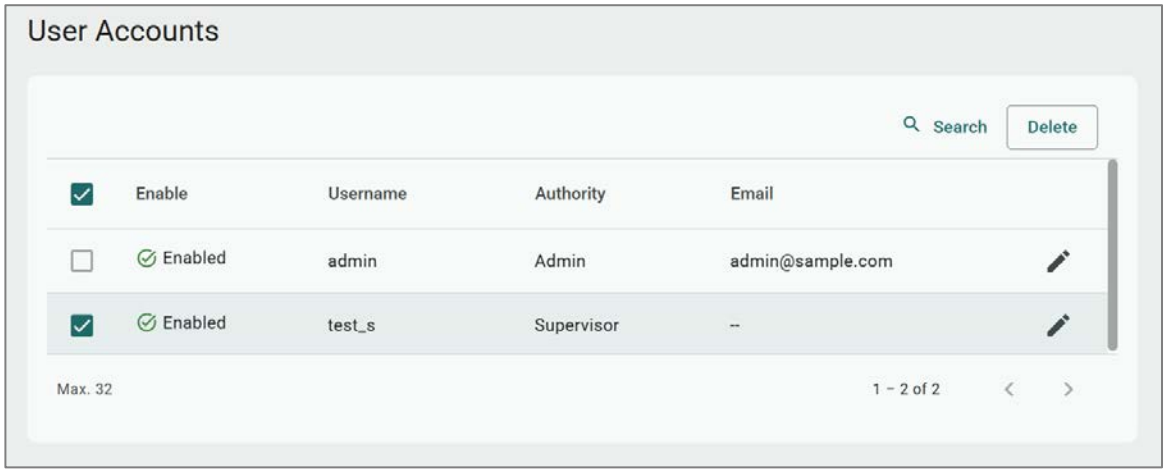
User Accounts - Delete Account

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** button.

Note

The "admin" account cannot be removed, but can be disabled if not in use.



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.



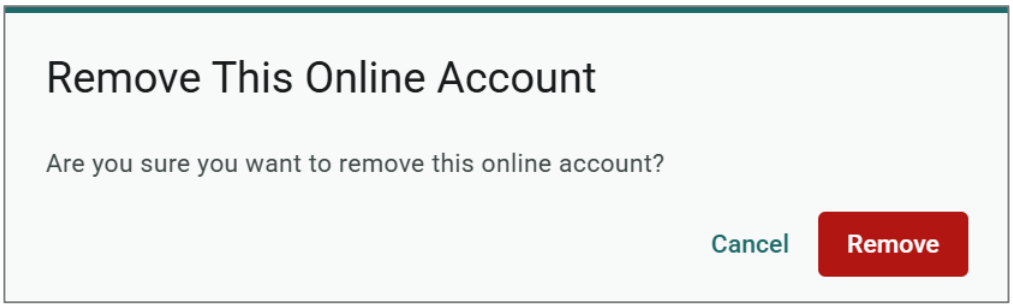
UI Setting	Description
Username	Shows the username of the online account.
Authority	Shows the authority level of the online account.
IP Address	Shows the IP address of the online account.

UI Setting	Description
Interface	Shows the interface that the online account is using.
Idle Time (sec.)	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

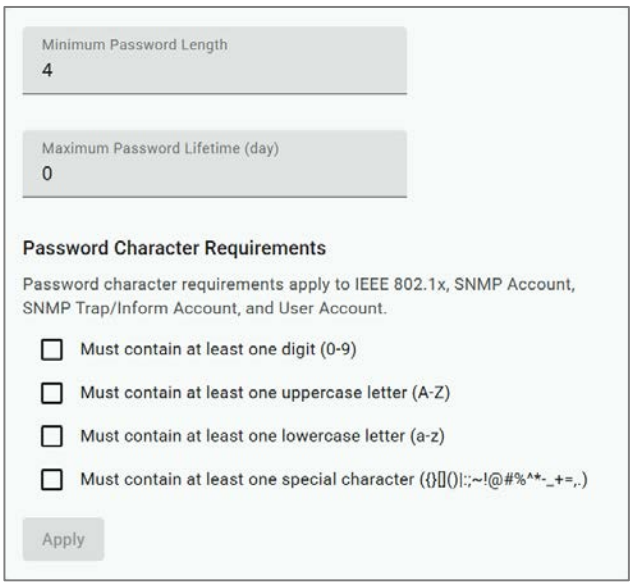
This page lets you create a robust password policy to safeguard your system against hackers. By enforcing minimum length and complexity requirements, you can empower users to choose strong passwords that are difficult to crack. Additionally, you can set a maximum password lifetime to ensure regular password 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 8
- Set a Maximum Password Lifetime to ensure that users change their password regularly
- Enable all the Password Character Requirements to ensure a minimum level of complexity



UI Setting	Description	Valid Range	Default Value
Minimum Password Length	Specify the minimum required password length.	4 to 16 characters	4
Maximum Password Lifetime (day)	Specify how long in days passwords will be valid for. When the password expires, the system will require the user to change their password. If this is set to 0, passwords will not expire.	0 to 365 days	0
Password Character Requirements	Select the complexity requirements that will apply to new passwords. **Note** 1. Password character requirements apply to IEEE 802.1x, SNMP Account, SNMP Trap/Inform Account, and User Account. 2. New requirements will only apply when creating or changing a password. They will not apply to existing passwords.	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

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

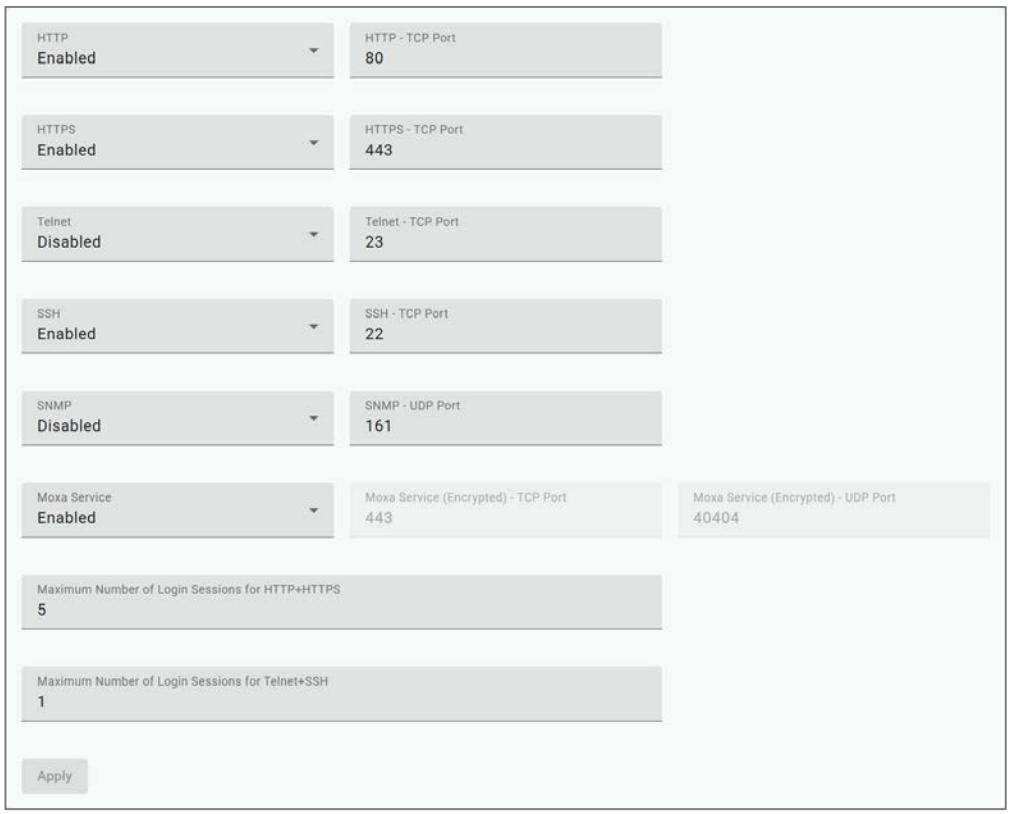
User Interface

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.



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

UI Setting	Description	Valid Range	Default Value
HTTPS	Enable or disable HTTPS connections. **Note** 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. **Note** The encryption algorithm of keys should be selected based on internationally recognized and proven security practices and recommendations. The lifetime of certificates generated for web server (HTTPS) services should be short and in accordance with the organization's security procedures and requirements.	Enabled / Disabled	Enabled
HTTPS - TCP Port	Specify the TCP port to use for HTTPS connections.	443, 1024 to 65535	443
Telnet	Enable or disable Telnet connections.	Enabled / Disabled	Disabled
Telnet - TCP Port	Specify the TCP port to use for Telnet connections.	23, 1024 to 65535	23
SSH	Enable or disable SSH connections.	Enabled / Disabled	Enabled
SSH - TCP Port	Specify the TCP port to use for SSH connections.	22, 1024 to 65535	22
SNMP	Enable or disable SNMP connections.	Enabled / Disabled	Disabled
SNMP - UDP Port	Specify the UDP port to use for SNMP connections.	161, 1024 - 65535	161

UI Setting	Description	Valid Range	Default Value
Moxa Service **(Only in Advanced Mode)**	Enable or disable Moxa Service connectivity. **Note** Moxa Service is only used for Moxa network management software, and is only available for user accounts with admin privileges.	Enabled / Disabled	Enabled
Moxa Service (Encrypted) - TCP Port **(Only in Advanced Mode)**	Shows the TCP port used for Moxa Service. This setting cannot be changed.	N/A	443
Moxa Service (Encrypted) - UDP Port **(Only in Advanced Mode)**	Shows the UDP port used for Moxa Service. This setting cannot be changed.	N/A	40404
Maximum Number of Login Sessions for HTTP+HTTPS	Specify the maximum combined number of users that can be logged in using HTTP and HTTPS.	1 to 10	5
Maximum Number of Login Sessions for Telnet+SSH	Specify the maximum combined number of users that can be logged in using Telnet and SSH.	1 to 5	1

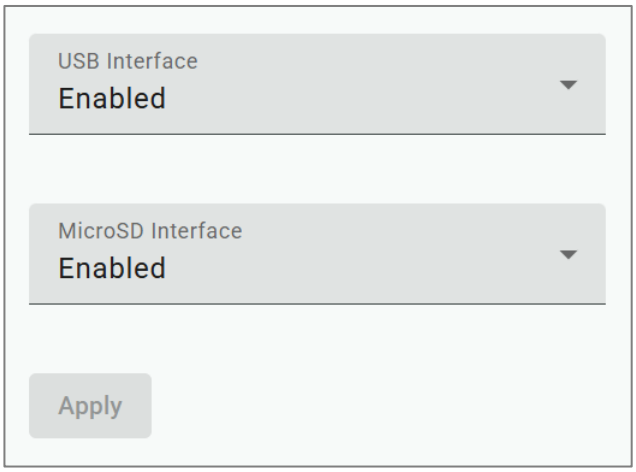
Hardware Interfaces

Menu Path: System > Management Interface > Hardware Interfaces

This page lets you enable or disable the USB/MicroSD interface on the device.

Click **Apply** to save your changes.

Hardware Interfaces Settings



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

Configuring Simple Network Management Protocol

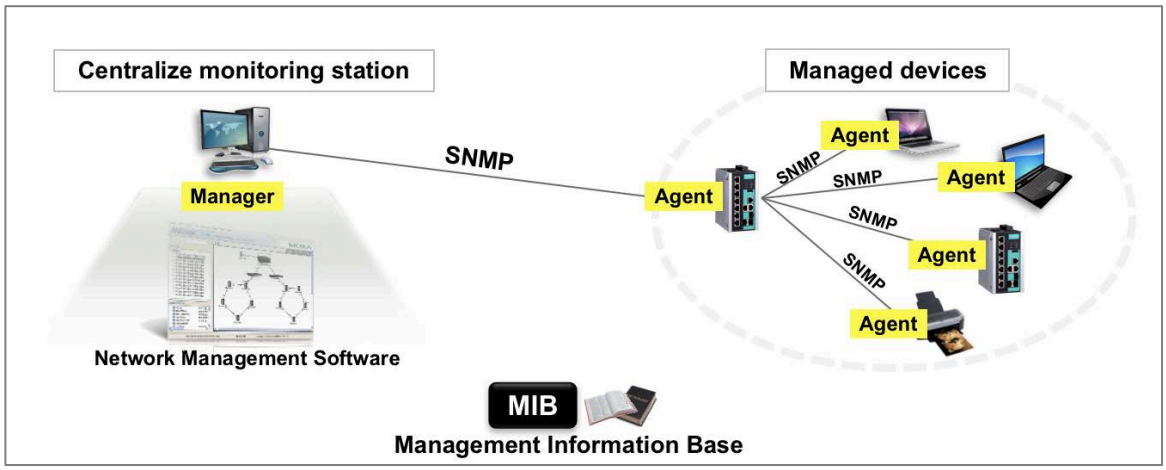
Simple Network Management Protocol (SNMP) be used to manage and monitor network devices.

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**, select **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 select **SNMP Account**.
3. Select **Create**.

   The Create an SNMP Account screen appears.
4. Specify all of the following, and then select **Create**:

Option	Value
Username	Specify a username for the account with up to 32 characters
Authority	Choose from: • **Read / Write** • **Read**

Option	Value
Authentication Type	Choose from: • **None** • **MD5** • **SHA** • **SHA-256** • **SHA-512** **Note** Authentication requires SNMP v3.
Authentication Password	If an authentication type has been specified, specify a password for the account between 8 and 64 characters long.
Encryption Method	• **Disabled** • **DES** • **AES** **Note** Encryption requires SNMP v3.
Encryption Key	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.

To edit or delete accounts:

From the **SNMP Account** table, select the corresponding **[Edit]** or **[Delete Forever]** icon.

SNMP

Menu Path: System > Management Interface > SNMP

This page lets you configure SNMP settings for your device.

This page includes these tabs:

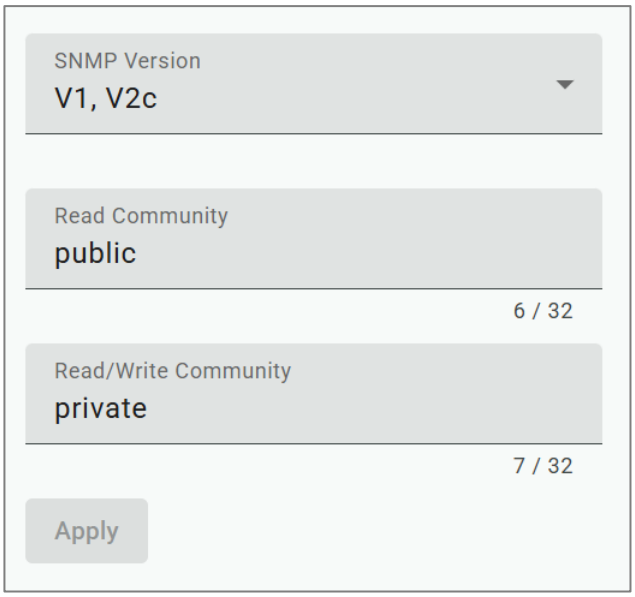
- General
- SNMP Account

SNMP - General

Menu Path: System > Management Interface > SNMP - General

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

Click **Apply** to save your changes.



UI Setting	Description	Valid Range	Default Value
SNMP Version	Specify the SNMP protocol version used to manage your device. • **V1, V2c, V3**: Enable SNMP V1, V2c, and V3. • **V1, V2c**: Enable SNMP V1 and V2c only. • **V3 only**: Enable SNMP V3 only.	V1, V2c, V3 / V1, V2c / V3 only	V1, V2C
Read Community	Specify a string name for the SNMP Read Community.	4 to 32 characters	public
Read/Write Community	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



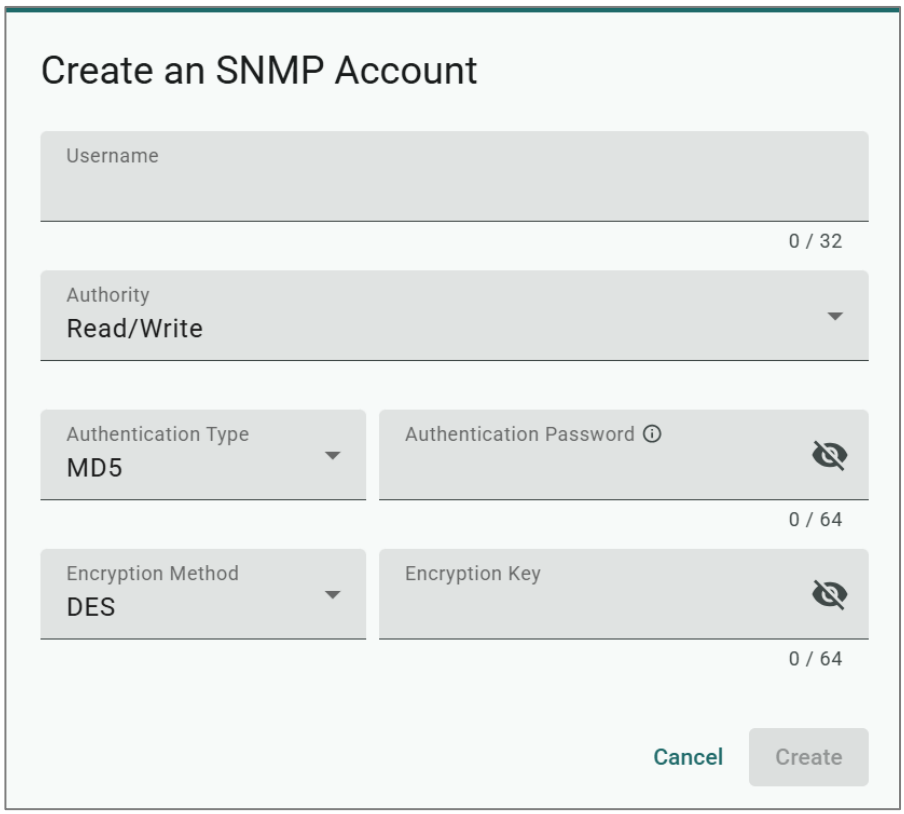
UI Setting	Description
Username	Shows the username of the SNMP account.
Authority	Shows the authority level of the management account.
Authentication Type	Shows the authentication type used for the account.
Authentication Password	Shows ******** if there is an authentication password for the account.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

Creating an SNMP Account

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

Clicking the **Create** button 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.



UI Setting	Description	Valid Range	Default Value
Username	Specify a username for the SNMP account.	1 to 32 characters • Valid characters: a-z, A-Z, 0-9 • Valid special characters: ._-	N/A
Authority	Specify the authority level of the management account. • **Read/Write**: Can read and write configuration settings • **Read**: Can only read configuration settings	Read/Write / Read	Read/Write
Authentication Type	Specify the authentication type to use for the account.	None / MD5 / SHA / SHA-256 / SHA-512	N/A

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

Editing an SNMP Account

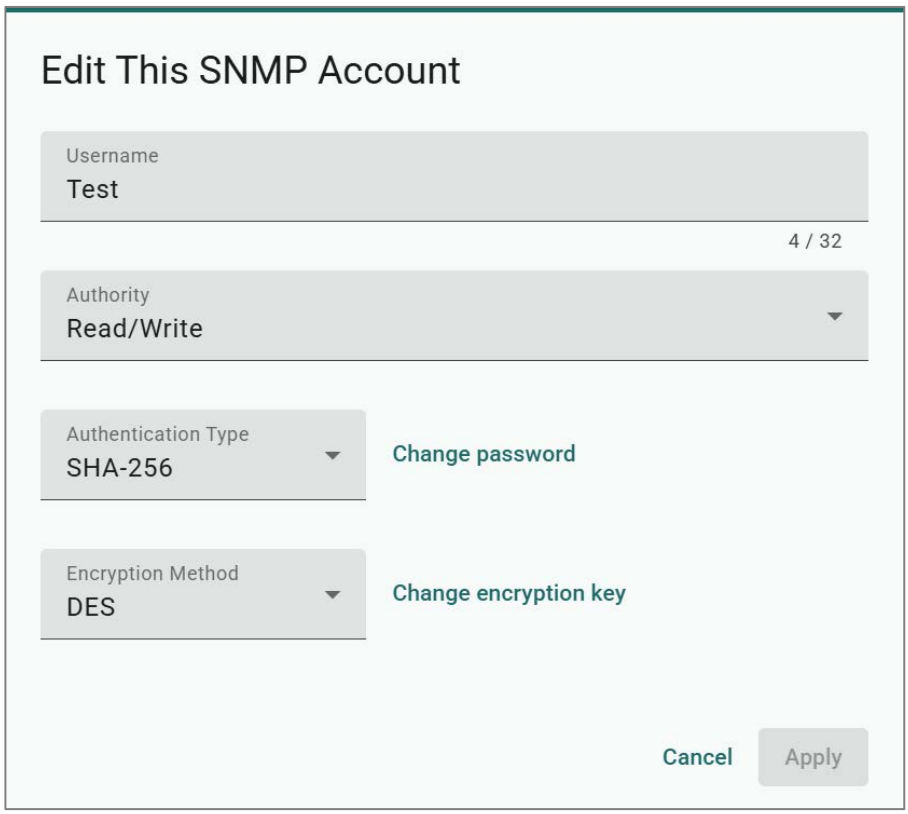
Menu Path: System > Management Interface > SNMP - SNMP Account

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.



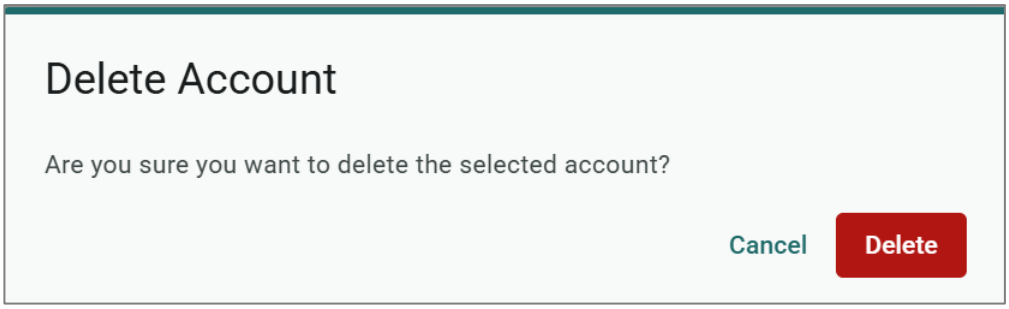
UI Setting	Description	Valid Range	Default Value
Username	Specify a username for the SNMP account.	1 to 32 characters • Valid characters: a-z, A-Z, 0-9 • Valid special characters: ._-	N/A
Authority	Select the authority level of the management account. • **Read/Write**: Can read and write configuration settings • **Read**: Can only read configuration settings	Read/Write / Read	Read/Write
Authentication Type	Select the authentication type to use for the account.	None / MD5 / SHA / SHA-256 / SHA-512	N/A
Encryption Method **(If Authentication Type is not None)**	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

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

Click **Delete** to save your changes.



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:

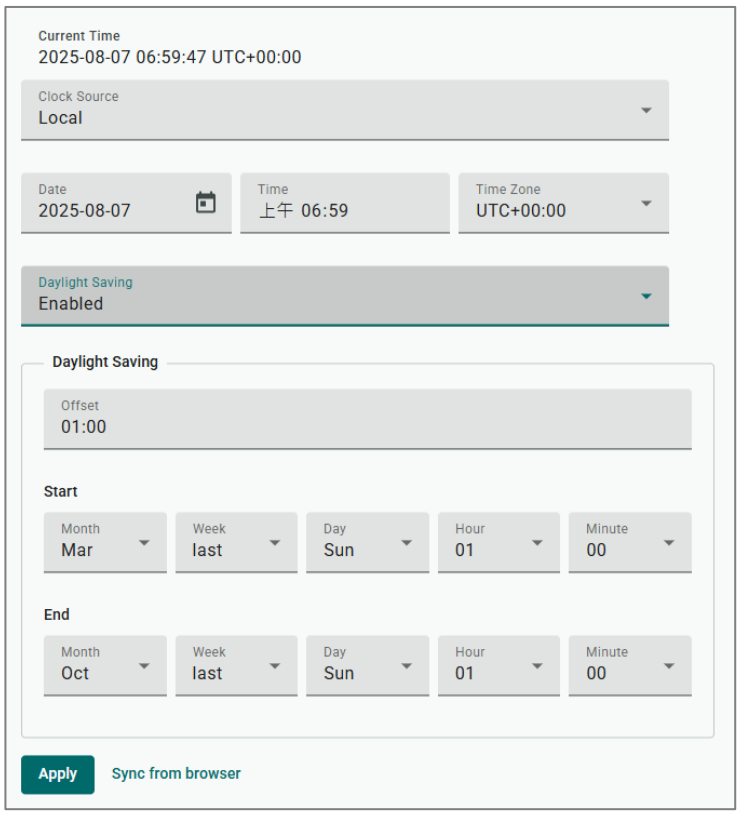
- Time
- NTP Authentication

System Time - Time

Menu Path: System > Time > System Time - Time

This page allows you to configure your device's system time by selecting a clock source or by synchronizing with your browser.

Click **Apply** to save your changes.



UI Setting	Description	Valid Range	Default Value
Current Time	Show the current time according to your local default settings.	N/A	N/A
Clock Source	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
Date **(If Clock Source is Local)**	Select the current date from the calendar.	Calendar	Local Date
Time **(If Clock Source is Local)**	Specify the current time. You can manually input the time, or you can click **SYNC FROM BROWSER** to set the time based on the time used by your web browser.	Timestamp	N/A
Time Zone	Specify the time zone used for the device.	Drop-down list of time zones	UTC+00:00

UI Setting	Description	Valid Range	Default Value
1st Time Server: IP Address/Domain Name **(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, time.stdtime.gov.tw, or time.nist.gov).	Valid IP address or domain name	time.nist.gov
2nd Time Server: IP Address/Domain Name **(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
Authentication **(If Clock Source is NTP)**	Select an NTP authentication key to use, or disable authentication for the time server. **Note** To use authentication, you need to create an NTP authentication entry first. Refer to NTP Authentication for more information.	Disabled / Drop-down list of NTP key IDs	Disabled

Daylight Saving

UI Setting	Description	Valid Range	Default Value
Daylight Saving	Enable or disable use of daylight saving time adjustment.	Enabled / Disabled	Disabled
Offset	Specify the number of hours and minutes to add during the daylight saving time period.	00:30 / 01:00	01:00
Start **Month/Week/Day/Hour/Minute**	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

UI Setting	Description	Valid Range	Default Value
End **Month / Week / Day / Hour / Minute**	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
Key ID	Shows the key ID for NTP authentication.

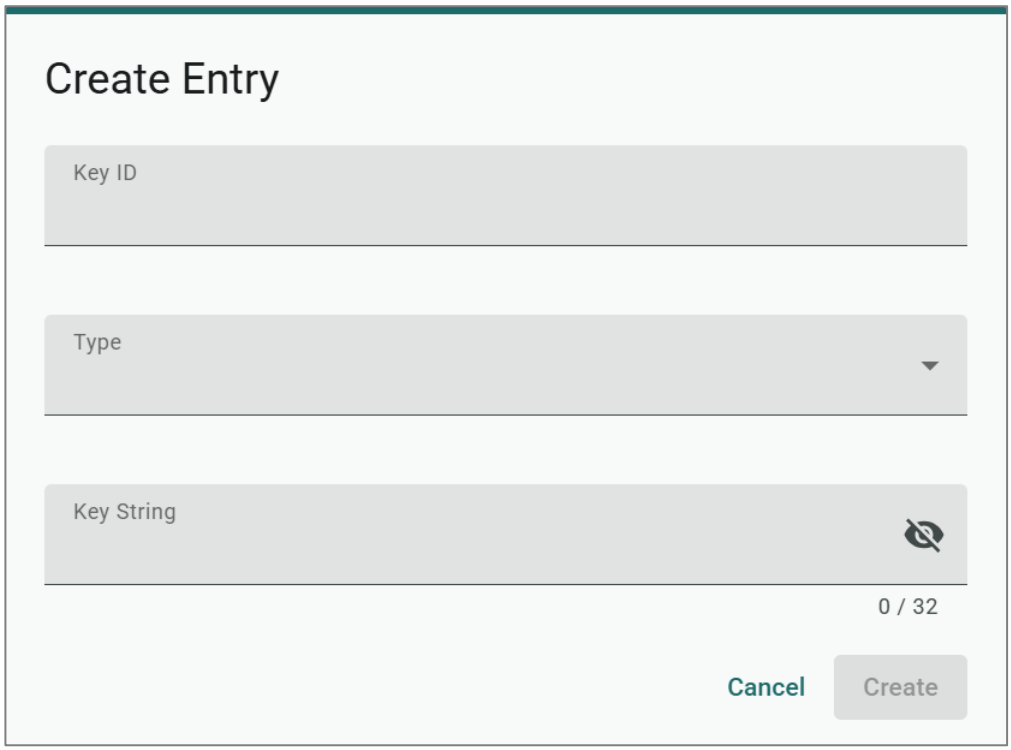
UI Setting	Description
Type	Shows the authentication type.
Key String	Shows the password used for authentication.

Creating an NTP Authentication Entry

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

Clicking the **Create** button 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.



UI Setting	Description	Valid Range	Default Value
Key ID	Specify the Key ID to use for NTP authentication.	1 to 65535	N/A
Type	Specify the authentication type.	MD5 / AES128CMAC	N/A

UI Setting	Description	Valid Range	Default Value
Key String	Specify the password to use for the authentication key.	0 to 32 characters	N/A

About NTP Server

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.

> **Note**
>
> This feature supports weaker authentication or encryption, and may not be secure over untrusted networks. Take appropriate security precautions.

NTP Server 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 an NTP client and provide the device's time to the client.

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**:

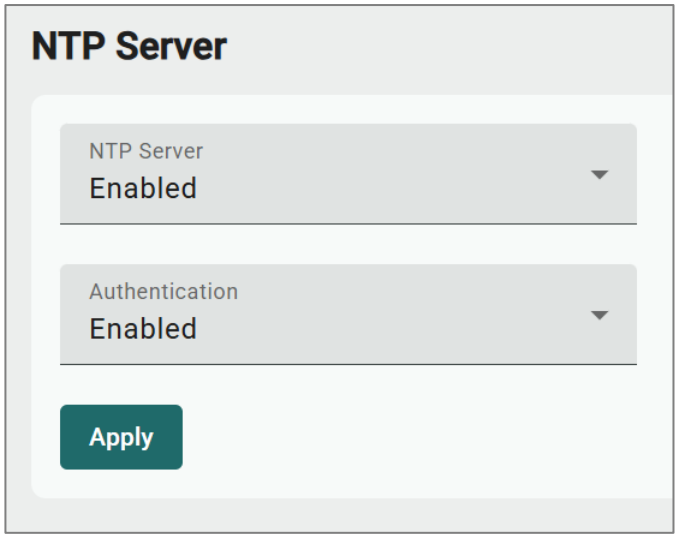
Option	Value
Key ID	Specify a number to identify the key
Type	Specify the authentication type.
Key String	Specify a key at least one character long.

NTP Server

Menu Path: System > Time > NTP Server

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

Click **Apply** to save your changes.



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

About Time Synchronization

Time synchronization aligns the clocks of different devices to the same time for fault-tolerant synchronization of real-time clocks.

Note

The IEEE 1588 working group now uses timeTransmitter and timeReceiver instead of "master" and "slave." This document adopts these terms.

Note

For MDS-G4000 Series and MDS-G4000-4XGS Series devices, if PTP must be used with multiple modules, slot M2 must be used for cross-module sync.

- Hot-swapping modules with PTP enabled may cause timing jitter.
- Hot-swapping the module in the M2 slot will remove the master clock, resulting in timing fluctuations.
- PTP will stay active when hot-swapping, but will resynchronize after the new module is inserted.

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.

This device supports the following IEEE 1588 profiles:

- **IEEE 1588 Default 2008** - The default protocol for industrial systems. Nanosecond-level accuracy.
- **IEC 61850-9-3-2016**: A profile of IEEE 1588 designed specifically for power system applications, such as digital substations and grid automation. Mandates additional requirements to ensure compliance with other power systems. Millisecond-level accuracy.
- **IEEE C37.238-2017**: A profile of IEEE 1588 designed for broader power system applications, such as for fault logging, real-time monitoring, and wider networks. Sub-microsecond accuracy.

PTP uses several roles for different clock roles, which dictate whether the device is a source or destination of time data:

- `GrandMaster`: Primary reference clock for network, usually with a precise time source, such as an atomic clock or satellite link.
- `timeTransmitter`: Receives time information from `GrandMaster` and distributes correct time further downstream.
- `timeReceiver`: Receives correct time from `timeTransmitter`. Usually only have a single network connection.

Clock roles are used across multiple clock types.

This device supports serving as one of the following clock types:

- **Boundary Clock**: Synchronizes its internal clock to the Grandmaster, distributes time data to downstream clocks as `timeTransmitter`.

- **Transparent Clock**: Corrects PTP messages to include their own delay information, then relays further downstream. Does not synchronize its internal clock. Used for maintaining multiple layers of network devices.

Intermediate clock types support two clock modes:

- **One Step**: One step synchronization sends all time sync data in a single message, reducing overhead, but may require specialized hardware that supports inline time stamping.
- **Two Step**: Two step synchronization sends `Follow_Up` message to synchronize time information. This may generate additional latency, but is widely used by substations, and may be suitable for a wider range of networking devices.

> **Note**
>
> This feature supports weaker authentication or encryption, and may not be secure over untrusted networks. Take appropriate security precautions.

Configuring Time Synchronization

Enable and configure Time Synchronization global settings before configuring individual ports.

1. Sign in to the device with administrator credentials.
2. Go to **System** > **Time** > **Time Synchronization**, and then click on the **General** tab.
3. To enable Time Synchronization, click **Time Synchronization**, and then choose **Enable** from the drop-down menu.
4. Configure the following:

Option	Value
Profile	Choose the time synchronization profile to use.
Clock type	Choose the clock type to use: **Boundary Clock** or **Transparent Clock**

Option	Value
Delay Mechanism	For **Profile**: **IEEE 1588 Default-2008**, choose a delay mechanism to compensate for network delay between `timeTransmitter` and `timeReceiver`: • **End-to-End** uses central delay requests and response between `timeTransmitter` and `timeReceiver`. Assumes symetric delays. Does not require PTP-aware networking equipment, but may have reduced performance in large or congested networks. • **Peer-to-Peer** calculates delay at each network node. Requires PTP-aware networking equipment, but scales reliably and can accommodate asymmetric delays.
Transport Mode	For **Profile**:**IEEE 1588 Default-2008**, choose a transport mode.
Priority 1	For **Clock Type**: **Boundary Clock**, specify priority value to override the default election method. Lower values take precedence. Default: `128`
Priority 2	For **Clock Type**: **Boundary Clock**, specify a secondary priority value to serve as a tiebreaker in the event that two candidates match the default criteria. Default: `128`
Domain Number	Specify a domain number, which allows multiple clock systems to share the same medium. Each `GrandMaster` clock should be in its own domain, with receiving clocks configured to match. The default domain is `0`.
Clock Mode	Choose **One Step** or **Two Step** (default).
Accuracy Alert	Specify an accuracy alert threshold in nanoseconds. Exceeding this threshold sends an event notification. Default: `1000`
Maximum Steps Removed	For **Clock Type**: **Boundary Clock**, specify the maximum number of steps before time synchronization packets will be dropped, prompting `GrandMaster` re-election. Default: `255`
Grandmaster ID	For **Profile**: **C37.238-2017** and **Clock Type**: **Boundary Clock**, specify the ID to use if this device becomes `GrandMaster`. Default: `255`

Option	Value
BMCA Best Master Clock Algorithm	For **Clock Type**: **Transparent Clock**, choose whether to **Enabled** (default) or **Disabled** the Best Master Clock Algorithm. Disabling may be preferable for sensitive applications where there is a requirement to use a specific `GrandMaster`. **Note** Only appears under Advanced Mode on sor models.

5. Click **Apply** to save your settings.

Time Synchronization is now be enabled globally.

Continue to enable Time Synchronization on specific ports to make the feature fully operational.

Enabling Time Synchronization on Ports

Once Time Synchronization is enabled globally, you can configure which ports will support timing messages.

Make sure you have chosen a **Profile** under the **General** tab in **System** > **Time** > **Time Synchronization**.

1. Go to **System** > **Time** > **Time Synchronization**, and then click on the **Port Settings** tab.

2. Locate the corresponding port to configure, and then click **[Edit]**.

   The Edit Port Settings screen appears.

3. Set **Time Synchronization** to **Enabled**.

4. For **Profile**: **IEEE 1588 Default-2008** selected under the **General** tab, configure the following:

Option	Description and Guidance
Announce Interval	Choose how often the timeTransmitter sends Announce messages to advertise itself. Lower values result in faster detection of failures but increase network traffic. Higher values reduce traffic but may slow failover detection. Default: **1 (2 sec.)**
Announce Receipt Timeout	Specify the number of missed Announce messages before assuming the timeTransmitter is lost and starts a re-election. Lower values detect failures quickly but may trigger unnecessary re-elections. Higher values allow more tolerance for occasional packet loss. Default: 3
Sync Interval	Choose how often Sync messages are sent by the timeTransmitter. More frequent updates improve precision but increase bandwidth usage. Less frequent updates reduce overhead but may lower accuracy. Default: **0 (1 sec.)**
Delay-Request Interval	Choose a Peer-to-Peer (P2P) delay measurement, which determines how often delay request messages are sent. Lower intervals provide more frequent updates for dynamic networks. Higher values reduce network load but may impact precision. Default: **-0 (1 sec.)**

5. To apply your changes to more than one port, click **Copy configurations to ports**, and then select the ports to also use your settings.
6. Click **Apply** to save your changes.

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

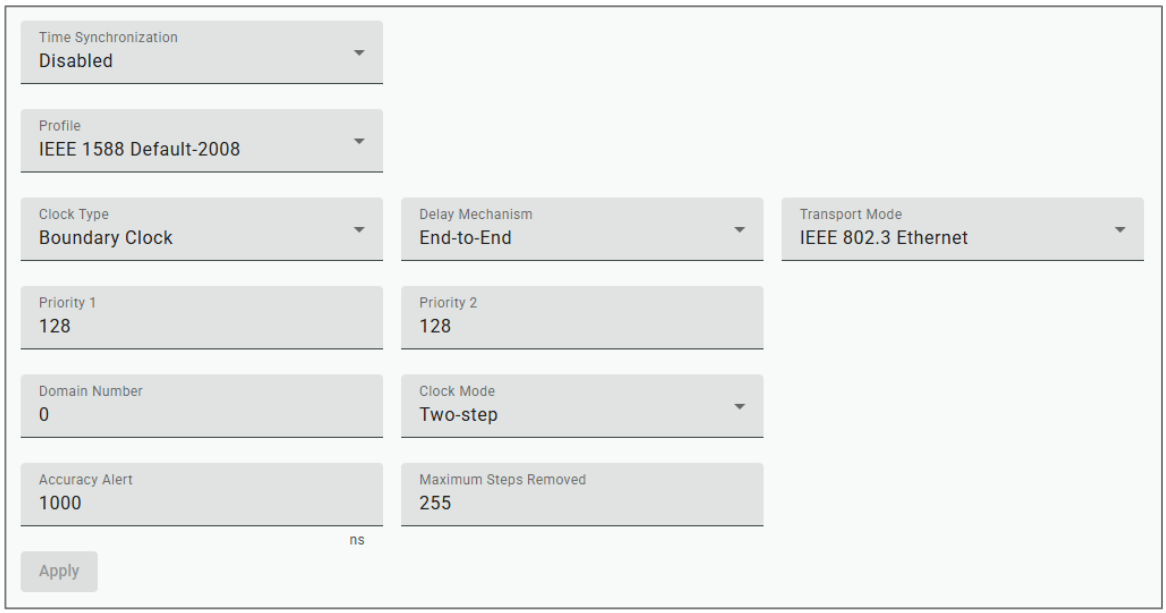
This feature is only available on RKS Series devices.

Time Synchronization - General

Menu Path: System > Time > Time Synchronization - General

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

Click **Apply** to save your changes.



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

UI Setting	Description	Valid Range	Default Value
Delay Mechanism **(If Profile is IEEE 1588 Default-2008)**	Select the delay mechanism to use. **Note** For IEC 61850-9-3-2016 and IEEE C37.238-2017 profiles, Delay Mechanism is fixed to Peer-to-Peer.	End-to-End / Peer-to-Peer	End-to-End
Transport Mode **(If Profile is IEEE 1588 Default-2008)**	Select the transport mode to use. **Note** For IEC 61850-9-3-2016 and IEEE C37.238-2017 profiles, Transport Mode is fixed to 802.3 Ethernet.	802.3 Ethernet / UDP IPv4	802.3 Ethernet
Priority 1 **(If Clock Type is Boundary Clock)**	Set the priority 1 value.	0 to 255	128
Priority 2 **(If Clock Type is Boundary Clock)**	Set the priority 2 value.	0 to 255	128
Domain Number	Set domain number value.	0 to 255	0
Clock Mode	Select the clock mode to use.	One-step / Two-step	Two-step
Accuracy Alert	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
Maximum Steps Removed **(If Clock Type is Boundary Clock)**	Specify the maximum number of steps that can be removed.	2 to 255	255
Grandmaster ID **(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

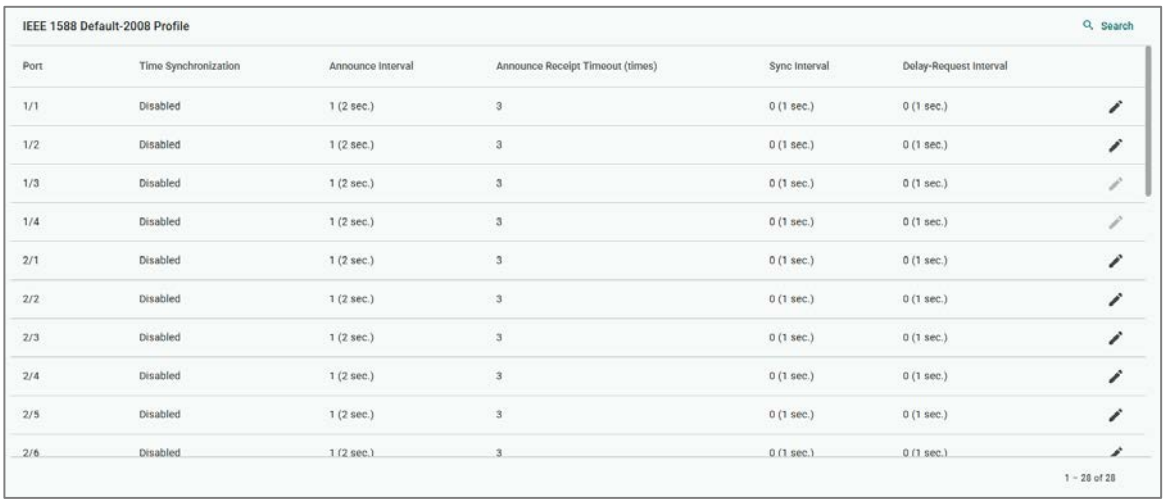
UI Setting	Description	Valid Range	Default Value
BMCA **(Only in Advanced Mode, if Clock Type is Transparent Clock)**	Enable or disable use of the Best Master Clock Algorithm (BMCA) when using transparent clock.	Enabled / Disabled	Enabled

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.

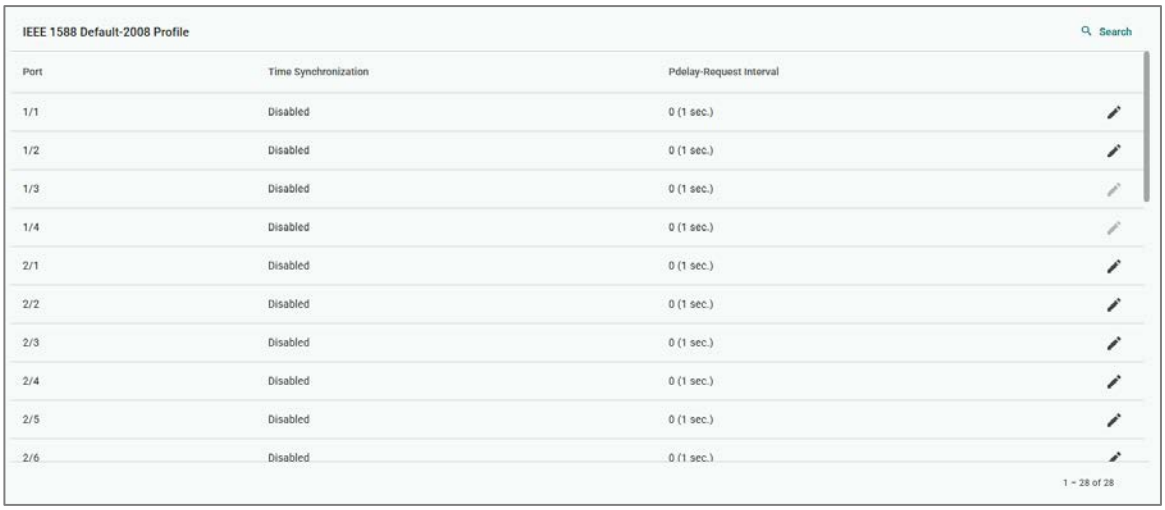
If the profile's **Clock Type** is **Boundary Clock**, this table will appear.



UI Setting	Description
Port	Shows which port the entry describes.
Time Synchronization	Shows whether time synchronization is enabled for the port.
Announce Interval	Shows the interval for sending PTP announce messages for the port.
Announce Receipt Timeout	Shows the announce message receipt timeout value for the port.

UI Setting	Description
Sync Interval	Shows the synchronization message transmit interval for the port.
Delay-Request Interval **(If the profile's Delay Mechanism is End-to-End)**	Shows the interval for sending delay request messages for the port.
Pdelay-Request Interval(If the profile's Delay Mechanism is Peer-to-Peer)	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.



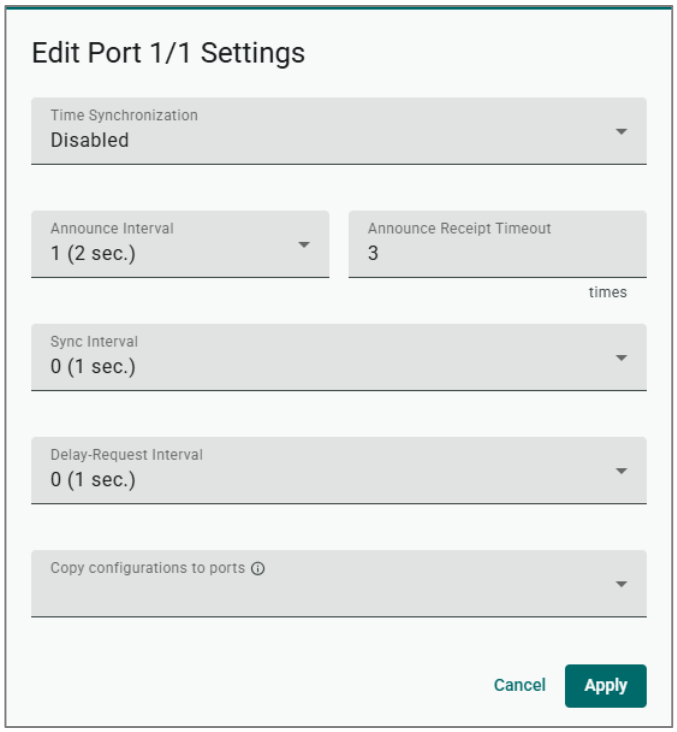
UI Setting	Description
Port	Shows which port the entry describes.
Time Synchronization	Shows whether time synchronization is enabled for the port.
Pdelay-Request Interval(If the profile's Delay Mechanism is Peer-to-Peer)	Shows the interval for sending peer delay request messages for the port.

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.



UI Setting	Description	Valid Range	Default Value
Time Synchronization	Enable or disable time synchronization for the port.	Enabled / Disabled	Disabled
Announce Interval	Select the interval to send announce messages for the port. **Note** For IEC 61850-9-3-2016 and IEEE C37.238-2017 profiles, Announce Interval is fixed to 0 (1 sec.).	0 (1 sec.) / 1 (2 sec.) / 2 (4 sec.) / 3 (8 sec.) / 4 (16 sec.)	1 (2 sec.)
Announce Receipt Timeout	Specify the number of timeouts allowed for announce receipts for the port. **Note** For IEC 61850-9-3-2016 and IEEE C37.238-2017 profiles, Announce Receipt Interval is fixed to 3.	2 to 10 (times)	3

UI Setting	Description	Valid Range	Default Value
Sync Interval	Select the synchronization interval for the port. **Note** For IEC 61850-9-3-2016 and IEEE C37.238-2017 profiles, Sync Interval is fixed to 0 (1 sec.).	-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.)
Delay-Request Interval **(If the profile's Delay Mechanism is End-to-End)**	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.)
Pdelay-Request Interval **(If the profile's Delay Mechanism is Peer-to-Peer)**	Select the interval for sending peer delay-request messages for the port. **Note** For IEC 61850-9-3-2016 and IEEE C37.238-2017 profiles, Pdelay-Request Interval is fixed to 0 (1 sec.).	-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.)
Copy configurations to ports	Select the ports you want to copy this configuration to.	Drop-down list of ports	N/A

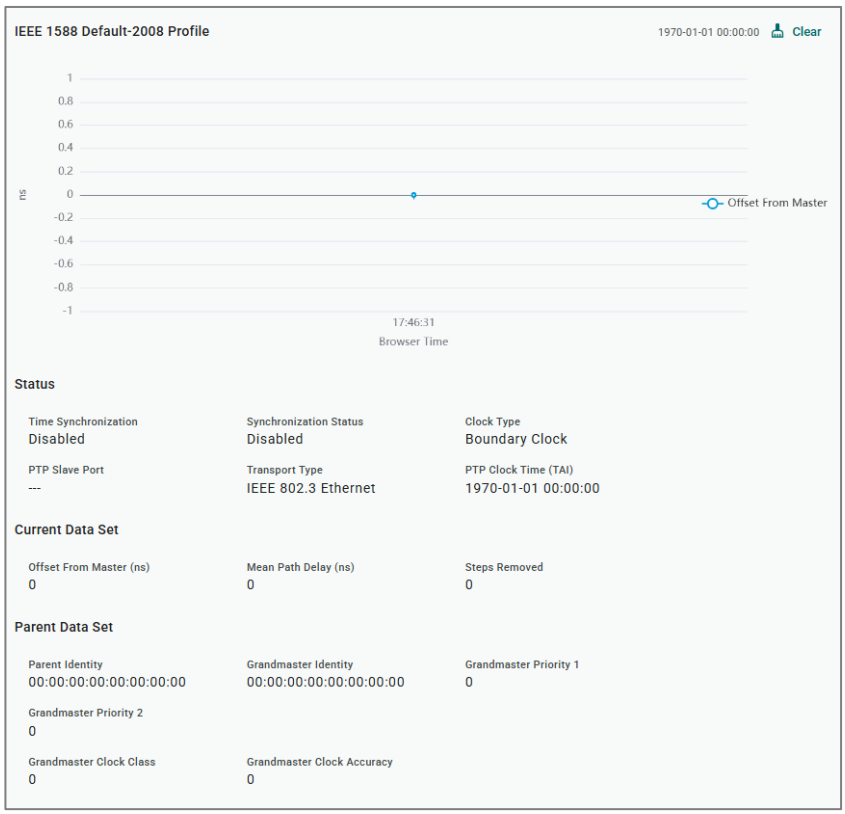
Time Synchronization - Status

Menu Path: System > Time > Time Synchronization - Status

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

Time Synchronization Status - Boundary Clock

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

Current Data Set

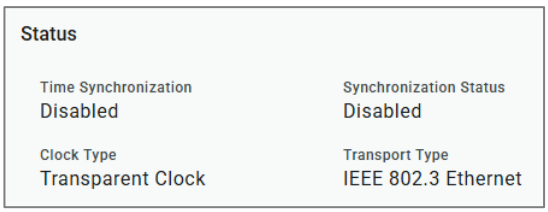
UI Setting	Description
Offset From Master (ns)	Shows the current offset from the master clock in nanoseconds.
Mean Path Delay (ns)	Shows the mean path delay in nanoseconds.
Steps Removed	Shows the number of steps removed.

Parent Data Set

UI Setting	Description
Parent Identity	Shows the clock ID of the parent identity.
Grandmaster Identity	Shows the clock ID of the grandmaster identity.
Grandmaster Priority 1	Shows the priority 1 value for the grandmaster clock.
Grandmaster Priority 2	Shows the priority 2 value for the grandmaster clock.
Grandmaster Clock Class	Shows the class value for the grandmaster clock.
Grandmaster Clock Accuracy	Shows the accuracy value for the grandmaster clock.

Time Synchronization Status - Transparent Clock

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



Status

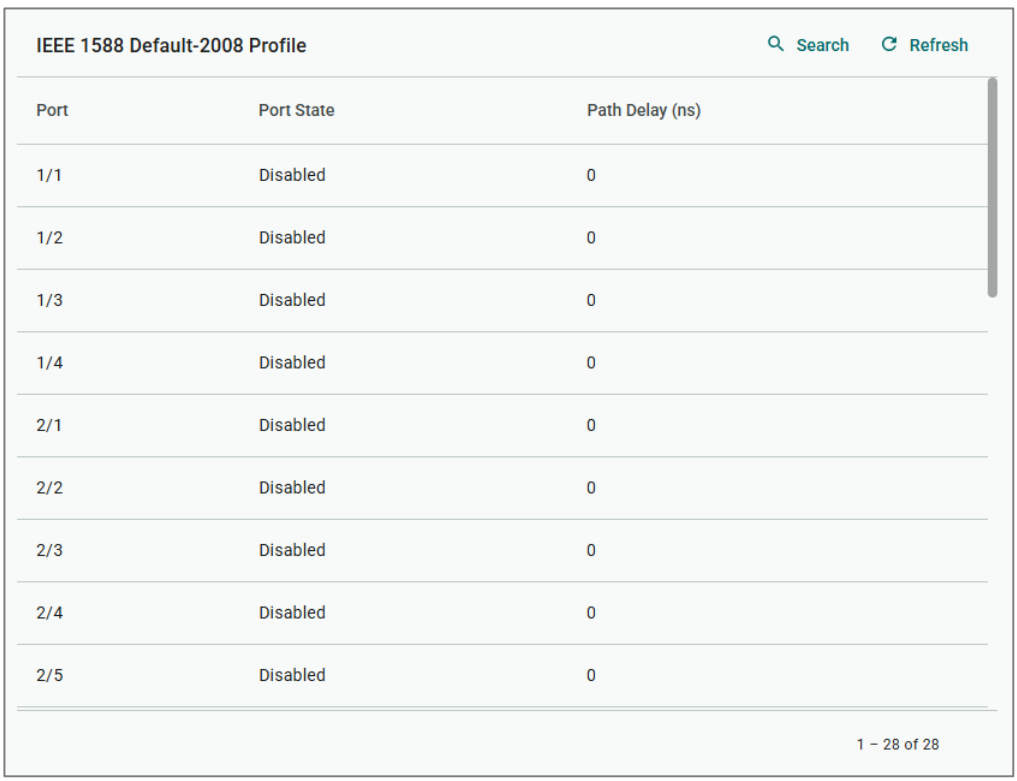
UI Setting	Description
Time Synchronization	Shows whether time synchronization is enabled.
Synchronization Status	Shows the current synchronization status. **Disabled** means that the time synchronization feature is disabled.
Clock Type	Shows the clock type being used.
Transport Type	Shows the transport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



UI Setting	Description
Port	Shows the port the entry is for.
Port State	Shows the operating state of time synchronization for the port.
Path Delay (ns)	Shows the path delay in nanoseconds for the port.

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

Port - User Privileges

Privileges to settings are granted to the different authority levels as follows. Refer to User Accounts for more information on user accounts.

Settings	Admin	Supervisor	User
Port Interface			
Port Settings	R/W	R/W	R
Linkup Delay	R/W	R/W	R
Link Aggregation	R/W	R/W	R
PoE **(for PoE models)**	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.

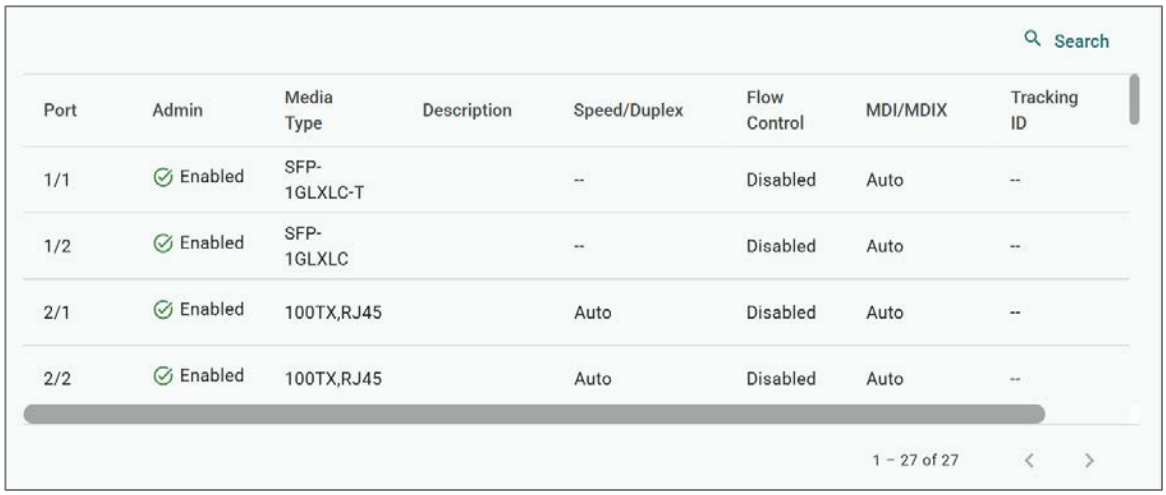
This page includes these tabs:

- Settings
- Status

Port Settings - Settings

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

This page lets you configure basic port settings.



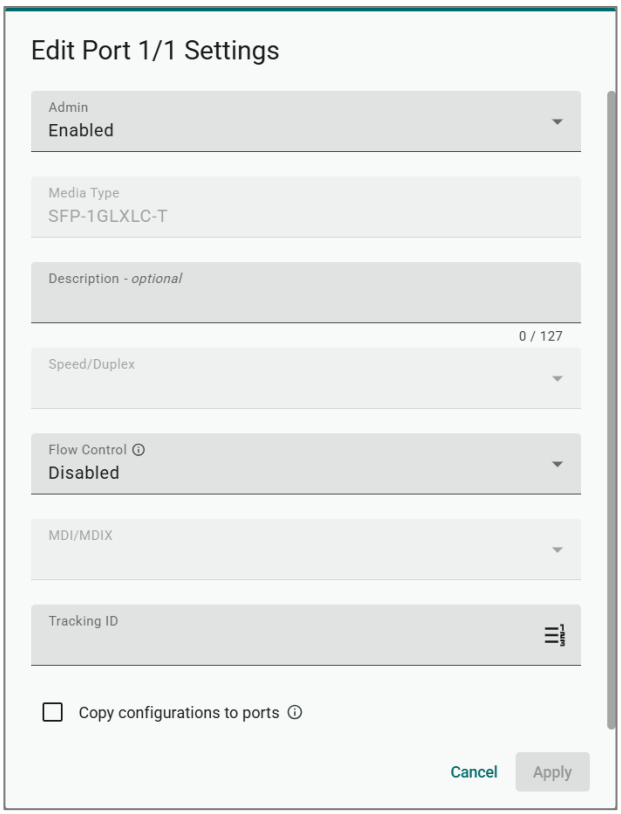
UI Setting	Description
Port	Shows which port the entry describes.
Admin	Shows whether admin status is enabled for data transmission through the port.
Media Type	Shows the detected media type for the port.
Description	Shows the description used to help identify the port.
Speed/Duplex	Shows the port speed and duplex option selected for the port.
Flow Control	Shows whether flow control is enabled for the port.
MDI/MDIX	Shows the MDI/MDIX option used for the port.
Tracking ID **(If the device is a L3 switch)**	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.



UI Setting	Description	Valid Range	Default Value
Admin	Enable or disable data transmission through the port.	Enabled / Disabled	Enabled
Media Type	Displays the detected media type for each port. This setting cannot be changed.	Detected media type	N/A
Description	Specify a description to help identify the port.	0 to 127 characters	N/A

UI Setting	Description	Valid Range	Default Value
Speed/Duplex	Select the speed/duplex mode to use for the port. Select **Auto** 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. 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. **Note** Speed/Duplex cannot be set for fiber ports.	Auto / 10M Half / 10M Full / 100M Half / 100M Full	Auto
Flow Control	Enable or disable flow control for the port. **Note** The switch and connected device will automatically determine the final result. **Note** Flow control can be enabled/disabled, but it is only effective at full duplex. Back pressure can be enabled/disabled, but it is only effective at half duplex.	Enabled / Disabled	Disabled
MDI/MDIX	Select the MDI/MDIX mode to use for the port. Select **Auto** to allow the port to auto-detect the port type of the connected Ethernet device, and change the port type accordingly. Alternatively, manually select **MDI** or **MDIX** if the device has trouble auto-detecting the port type. **Note** MDI/MDIX cannot be set for fiber ports.	Auto / MDI / MDIX	Auto
Tracking ID **(If the device is an L3 switch)**	Specify a tracking ID for the port, or select the **Select Tracking ID ( )** icon to select a currently used tracking ID. This setting is optional.	1 to 16	N/A

UI Setting	Description	Valid Range	Default Value
Copy configurations to ports	Select the ports you want to copy this configuration to. **Note** The copy configuration feature cannot be used with fiber ports.	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.



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

About Linkup Delay

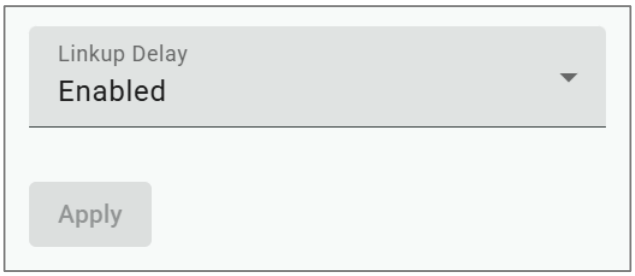
Linkup delay, also known as link flap prevention, is used to prevent a port alternating between link up and link down statuses, and is useful when a link connection is unstable. An unstable connection might be caused by situations such as a faulty cable, faulty fiber transceiver, duplex mismatch, etc. 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



UI Setting	Description	Valid Range	Default Value
Linkup Delay	Enable or disable the linkup delay feature for the device. **Note** After enabling linkup delay, you will still need to configure and enable linkup delay for each port you want to use it on. Refer to Linkup Delay - Edit Port Settings for more information.	Enabled / Disabled	Enabled

Linkup Delay - Port List



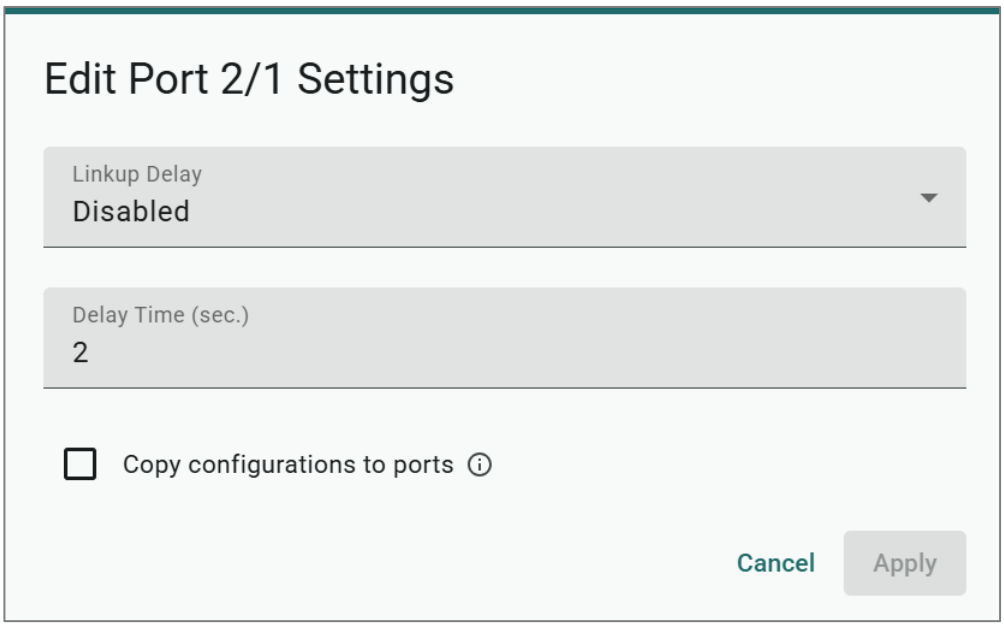
UI Setting	Description
Port	Shows the port index.
Status	Shows whether linkup delay is enabled or disabled for the port. **Note** To enable linkup delay for a port, both the linkup delay setting for the port and the global linkup delay setting must be enabled. Refer to Linkup Delay Settings for more information.
Delay Time	Shows the delay time in seconds for the port.
Remaining Time	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
Linkup Delay	Enable or disable linkup delay for the port. **Note** To enable linkup delay for a port, both the linkup delay setting for the port and the global linkup delay setting must be enabled. Refer to Linkup Delay Settings for more information.	Enabled / Disabled	Disabled
Delay Time	Specify the delay time in seconds before the port alternates between link up and link down.	1 to 1000	2
Copy configurations to ports	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, different 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.
- **MAC (SA, DA) + IP (SA, DA)**: Source and destination MAC addresses are used together with source and destination IP addresses for the hash algorithm. This is useful when using MAC addresses for the hash algorithm is not sufficient for

managing load balancing, such as in environments with a single server to Layer 3 network environment.

- **MAC (SA, DA) + IP (SA, DA) + L4 (SPort, DPort)**: SMAC, DMAC, source and destination IP addresses, and source and destination L4 ports are used together for the hash algorithm. This is useful for environments running multiple services on the network, such as a network with many TCP/UDP connections (client sessions) between IPs.

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

The maximum number of Link Aggregation groups is half of the device's total number of ports. For example, users can create up to 14 link aggregation groups on 28-port models.

Link Aggregation List Algorithm

Note

This appears only in Advanced Mode.

Note

The link aggregation algorithm can only be set globally; all port channels use the same algorithm.

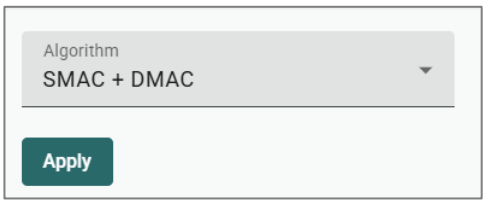
Note

The following algorithms were added in MX-NOS V6:

- MAC(SA, DA)+IP(SA, DA)
- MAC(SA, DA)+IP(SA, DA) + L4(SPort, DPort)

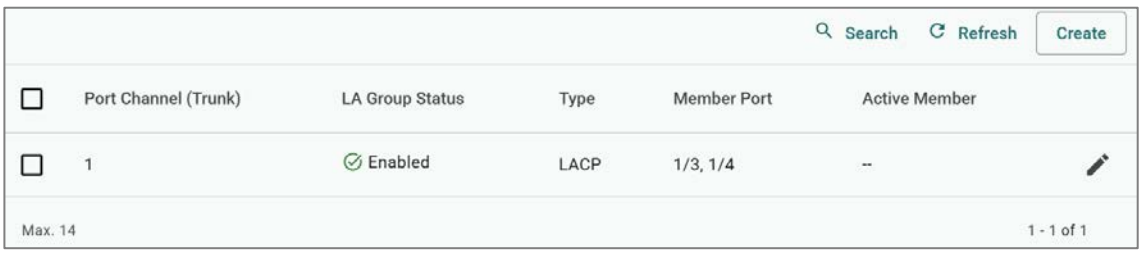
If you select one of these algorithms, please note the following behaviors:

- For connected devices running a version of MX-NOS before V6, the link to the device will be disconnected.
- Saved MX-NOS V6 configurations that use one of these algorithms cannot be imported to devices running a version of MX-NOS before V6.



UI Setting	Description	Valid Range	Default Value
Algorithm	Select the load-sharing hash algorithms to be used for configuring link aggregation.	SMAC / DMAC / SMAC+DMAC / MAC(SA, DA)+IP(SA, DA) / MAC(SA, DA)+IP(SA, DA) + L4(SPort, DPort)	SMAC+DMAC

Link Aggregation List



UI Setting	Description
Port Channel (Trunk)	Shows the Port Channel (Trunk) number of the link aggregation group.
LA Group Status	Shows whether the link aggregation group is enabled.

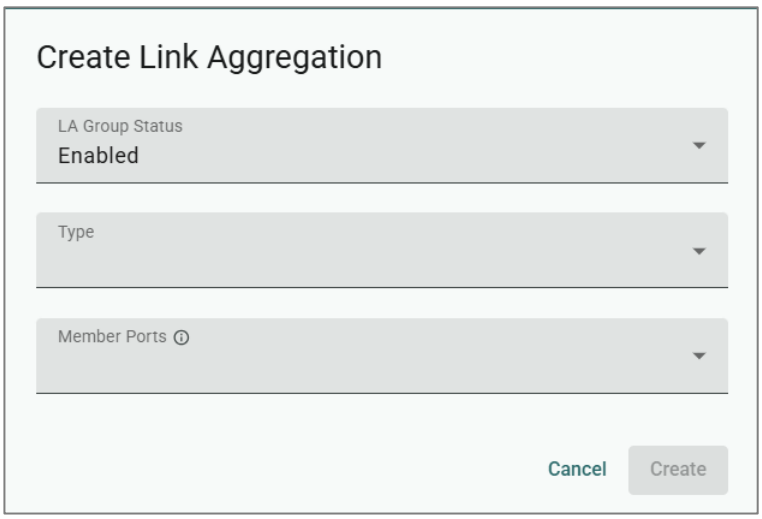
UI Setting	Description
Type	Shows the method for configuring the link aggregation group.
Member Ports	Shows the configured member ports in the link aggregation group.
Active Member	Shows the active member ports in the link aggregation group.

Creating a Link Aggregation Group

Menu Path: Port > Link Aggregation

Clicking the **Create** button 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.



UI Setting	Description	Valid Range	Default Value
LA Group Status	Enable or disable the link aggregation group.	Enabled / Disabled	Enabled
Type	Select the method to use for configuring the link aggregation group. **Manual**: This allows you to specify the ports to be included in the LA Group. **LACP**: LACP protocol will be used to automatically negotiate link aggregation configuration between devices.	Manual / LACP	N/A

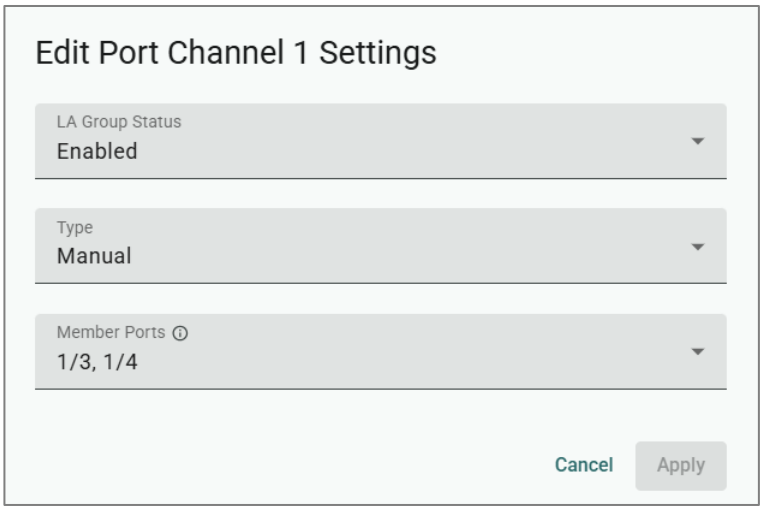
UI Setting	Description	Valid Range	Default Value
Member Ports	Select the ports to add to the link aggregation group. **Note** A port cannot be assigned to multiple link aggregation groups. This is because each port can only be a member of a single link aggregation group at a time. A link aggregation group (Port-channel) cannot be created when selected ports are operating at different speeds.	Drop-down list of ports	N/A

Editing a Link Aggregation Group

Menu Path: Port > Link Aggregation

Clicking the **Edit (✎)** icon for an entry in the Link Aggregation List 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.



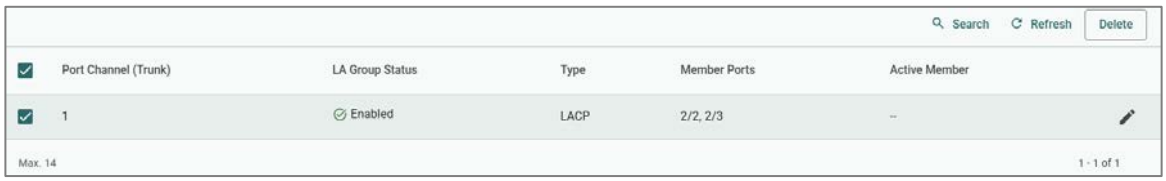
UI Setting	Description	Valid Range	Default Value
LA Group Status	Enable or disable the link aggregation group.	Enabled / Disabled	Enabled

UI Setting	Description	Valid Range	Default Value
Type	Select the method to use for configuring the link aggregation group. **Manual**: This allows you to specify the ports to be included in the LA Group. **LACP**: LACP protocol will be used to automatically negotiate link aggregation configuration between devices.	Manual / LACP	N/A
Member Ports	Select the ports to add to the link aggregation group. **Note** 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.	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** button.



Link Aggregation Port List

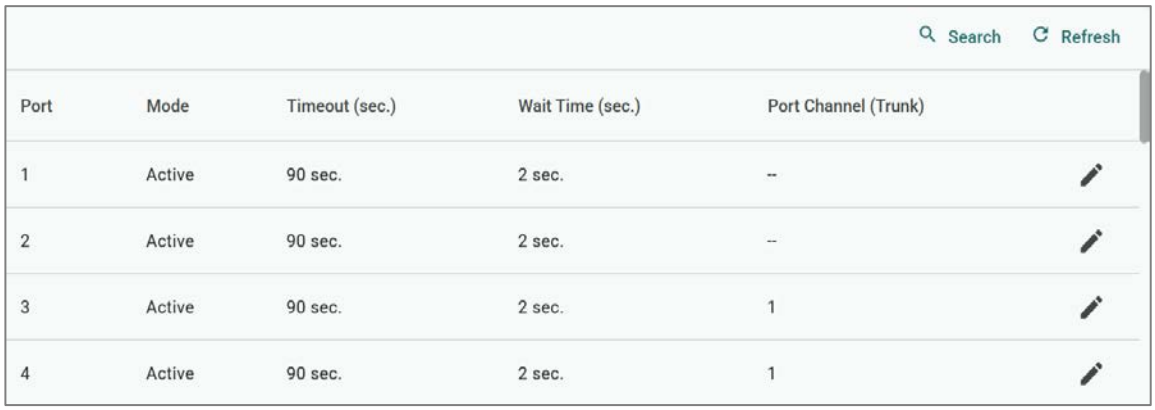
This table lets you see the LACP settings for each port.

Note

This appears only in Advanced Mode.

Note

This feature supports weaker authentication or encryption, and may not be secure over untrusted networks. Take appropriate security precautions.



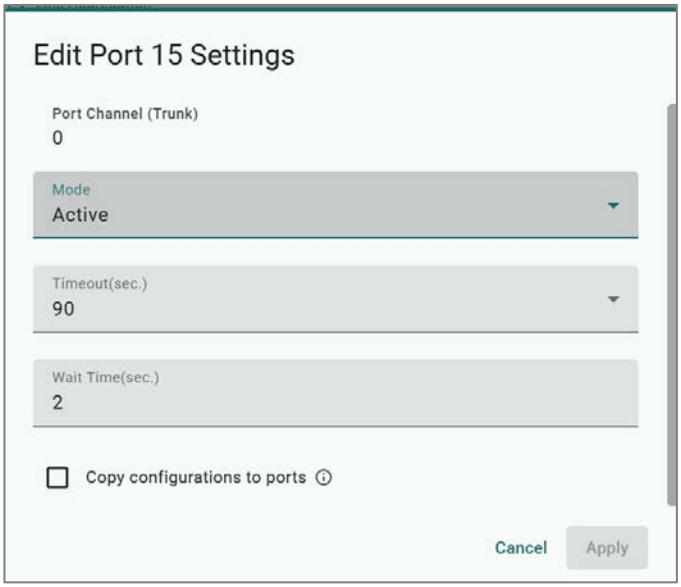
UI Setting	Description
Port	Shows which port the entry describes.
Mode	Shows the LACP mode for the port.
Timeout (sec.)	Shows the LACP inactivity timeout in seconds for the port.
Wait Time (sec.)	Shows the LACP wait time in seconds for the port.
Port Channel (Trunk)	Shows the link aggregation group (Port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

Editing LACP Port Settings

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
Port Channel (Trunk)	Shows the link aggregation group (Port channel) number of the port. This setting cannot be changed.	Port Channel Number	N/A
Mode	Select the LACP mode to decide how the ports establish LACP links. • **Active**: 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. • **Passive**: Ports can respond to LACP queries from active ports and passively establish LACP links. They will not initiate any LACP negotiation on their own. **Note** 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.	Active / Passive	Active
Timeout	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
Wait Time	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

UI Setting	Description	Valid Range	Default Value
Copy configurations to ports	Select the ports you want to copy this configuration to.	Drop-down list of ports	N/A

About 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 support high-power PoE+ and PoE++ standards as well as 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

Limitations

PoE functionality is only available on specific PoE-enabled Moxa device models. Connected PoE devices must support the IEEE 802.3af/at/bt standard in order to use this feature, with a maximum of 90 W per port.

PoE - General

Menu Path: Port > PoE - General

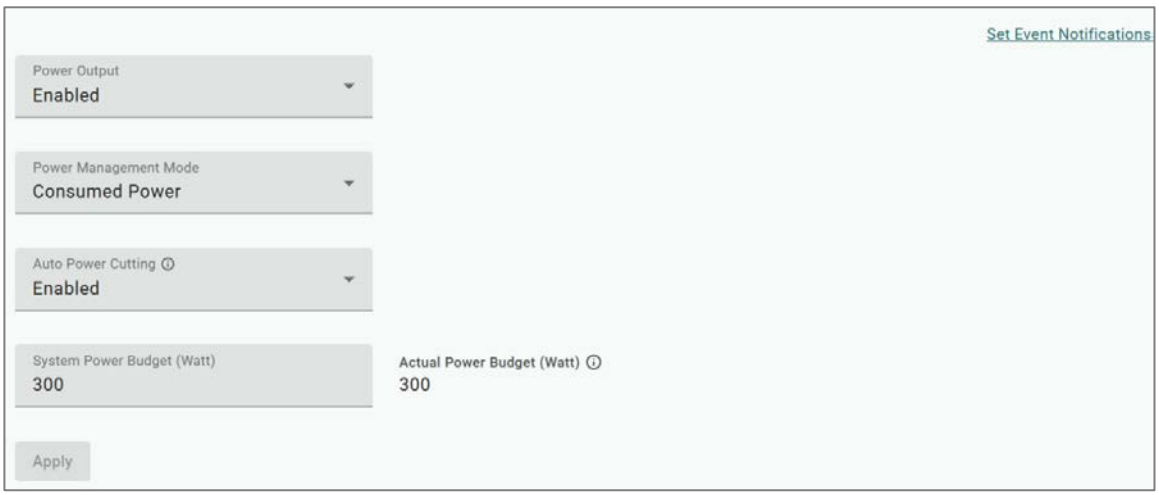
This page lets you enable PoE power output and configure system-level PoE settings.

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

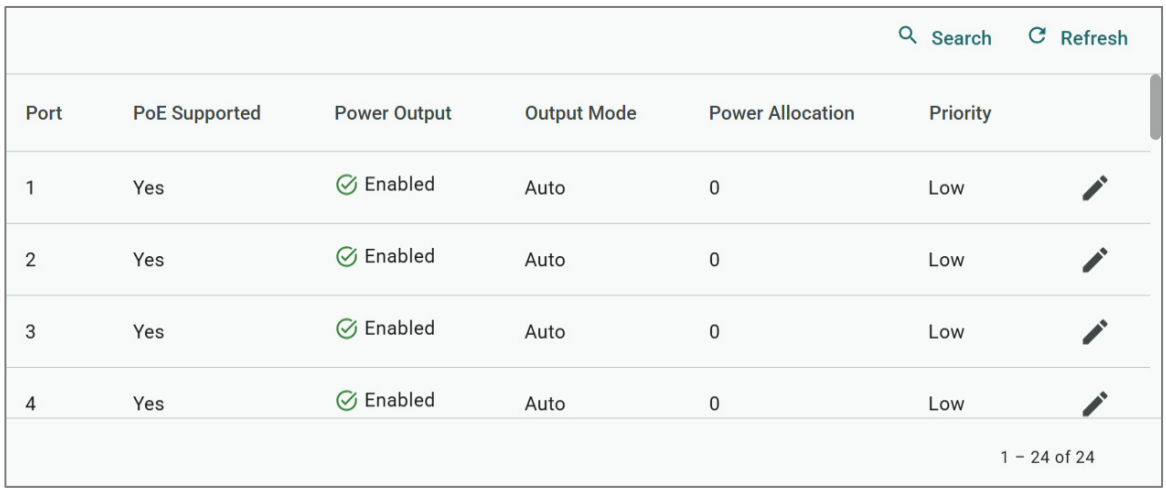


UI Setting	Description	Valid Range	Default Value
Power Output	Enable or disable PoE.	Enabled / Disabled	Enabled

UI Setting	Description	Valid Range	Default Value
Power Management Mode	Specify whether the power budget for all ports should be calculated. • **Allocated Power**: This calculates the power budget based on the Power Allocation settings of all ports. For more information on per-port power allocation, refer to PoE - Edit Port Settings. • **Consumed Power**: This calculates the power budget based on actual power consumed by all ports.	Allocated Power / Consumed Power	Consumed Power
Auto Power Cutting	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
System Power Budget	Specify the "total measured power" limit in watts to use for all PoE ports combined.	*(Depends on your device model)*	*(Depends on your device model)*
Actual Power Budget **(View-only)**	Shows the system power budget in watts. This setting cannot be changed.	N/A	*(Depends on your device model)*

PoE - Port List





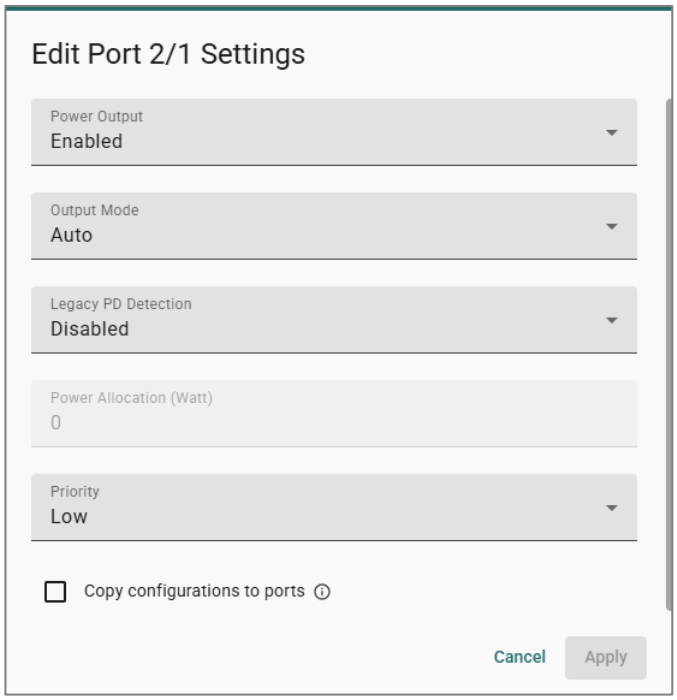
UI Setting	Description
Port	Shows which port the entry describes.
PoE Supported	Shows whether the port supports PoE.
Power Output	Shows whether PoE is enabled for the port.
Output Mode	Shows the output mode for the port.
Power Allocation	Shows the power allocation value for the port. When the output mode is **Auto**, this value is fixed as 0.
Legacy PD Detection	Shows whether Legacy PD Detection is enabled or disabled.
Priority	Shows the port priority: Critical (highest) / High / Low.

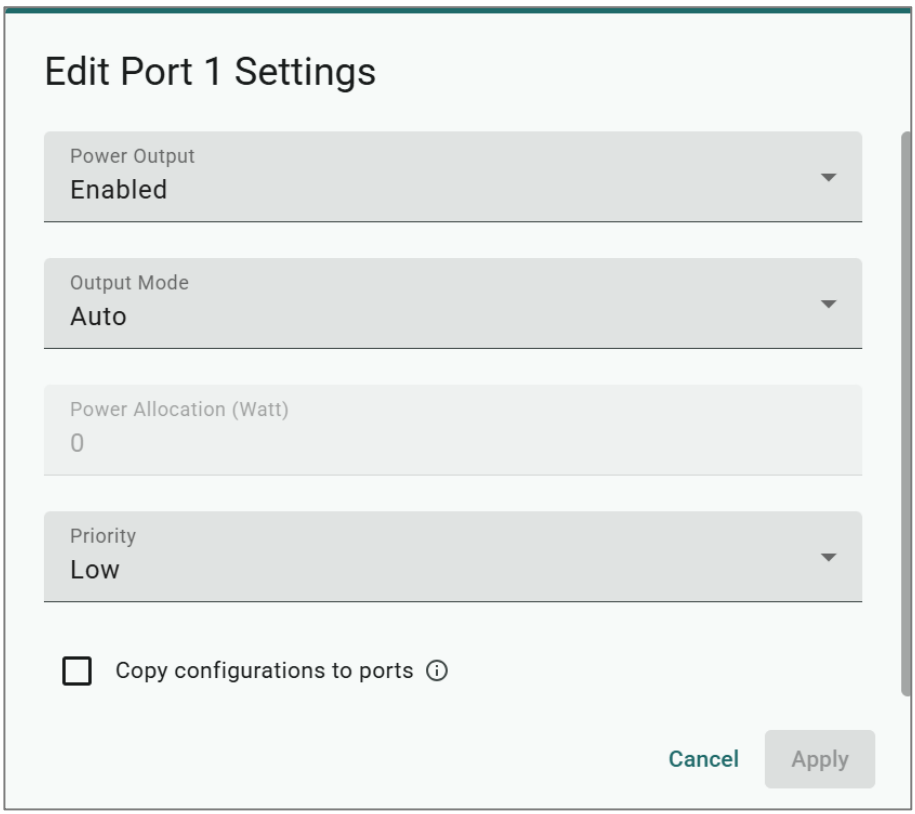
PoE - Edit Port Settings

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 2/1 Settings
Power Output
Enabled
Output Mode
Auto
Legacy PD Detection
Disabled
Power Allocation (Watt)
0
Priority
Low
Copy configurations to ports
Cancel
Apply


Edit Port 1 Settings
Power Output
Enabled
Output Mode
Auto
Power Allocation (Watt)
0
Priority
Low
Copy configurations to ports
Cancel
Apply

UI Setting	Description	Valid Range	Default Value
Power Output	Enable or disable PoE for this port.	Enabled / Disabled	Enabled
Output Mode	Specify whether to set the PoE output mode to Auto or Force. **Auto**: Power output will be determined by using 802.3bt auto-detection. **Force**: Power output will be determined by the **Power Allocation** setting for the port. This may be necessary for PDs that do not follow 802.3af/at/bt standards.	Auto / Force	Auto
Legacy PD Detection	Enable or disable legacy PD detection for the port. Legacy PD detection will trigger the system to output power to the connected PD when the capacitance of the PD is higher than 2.7 µF and less than 10 µF. It will take a few seconds for PoE power to be output through the port (if triggered) after enabling legacy PD detection.	Enabled / Disabled	Disabled
Power Allocation (Watt)	Specify the power in watts to allocate to a connected PD when the **Output Mode** is set to **Force**. • When the output mode is **Auto**, the value is fixed as 0. • When the output mode is set to **Force**, specify a value from 0 to 90.	0 to 90	N/A
Priority	Specify the priority of the port to use with the **Auto Power Cutting** 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 PoE - General for more information.	Critical / High / Low	Low
Copy configurations to ports	Select the ports you want to copy this configuration to.	Drop-down list of ports	N/A

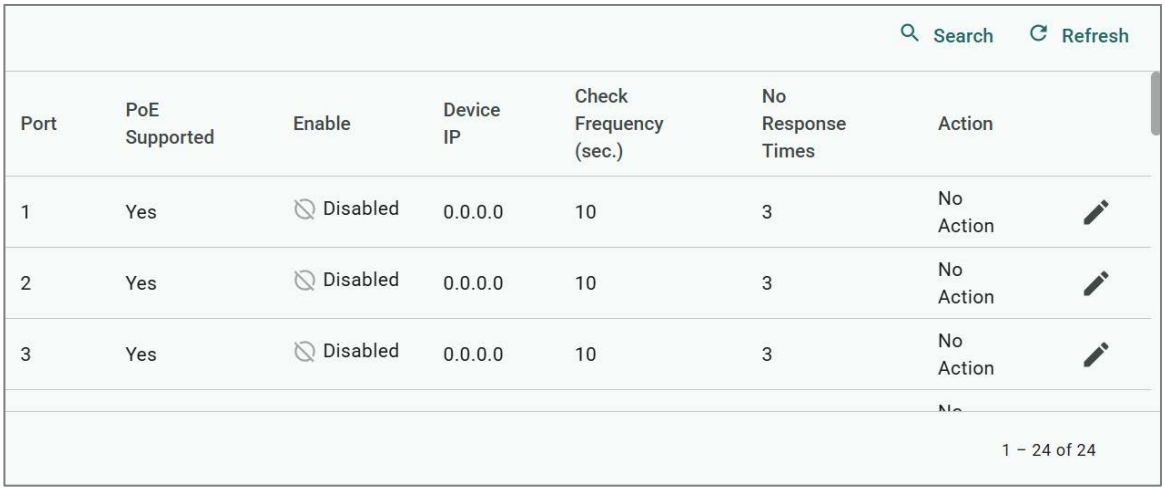
UI Setting	Description	Valid Range	Default Value
Power Output	Enable or disable PoE for this port.	Enabled / Disabled	Enabled

UI Setting	Description	Valid Range	Default Value
Output Mode	Specify whether to set the PoE output mode to Auto or Force. **Auto**: Power output will be determined by using 802.3at auto-detection. **Force**: Power output will be determined by the **Power Allocation** setting for the port. This may be necessary for PDs that do not follow 802.3af/at standards.	Auto / Force	Auto
Power Allocation (Watt)	Specify the power in watts to allocate to a connected PD when the **Output Mode** is set to **Force**. • When the output mode is **Auto**, the value is fixed as 0. • When the output mode is set to **Force**, input a value from 0 to 30.	0 to 30	N/A
Priority	Specify the priority of the port to use with the **Auto Power Cutting** 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 PoE - General for more information.	Critical / High / Low	Low
Copy configurations to ports	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 page 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.



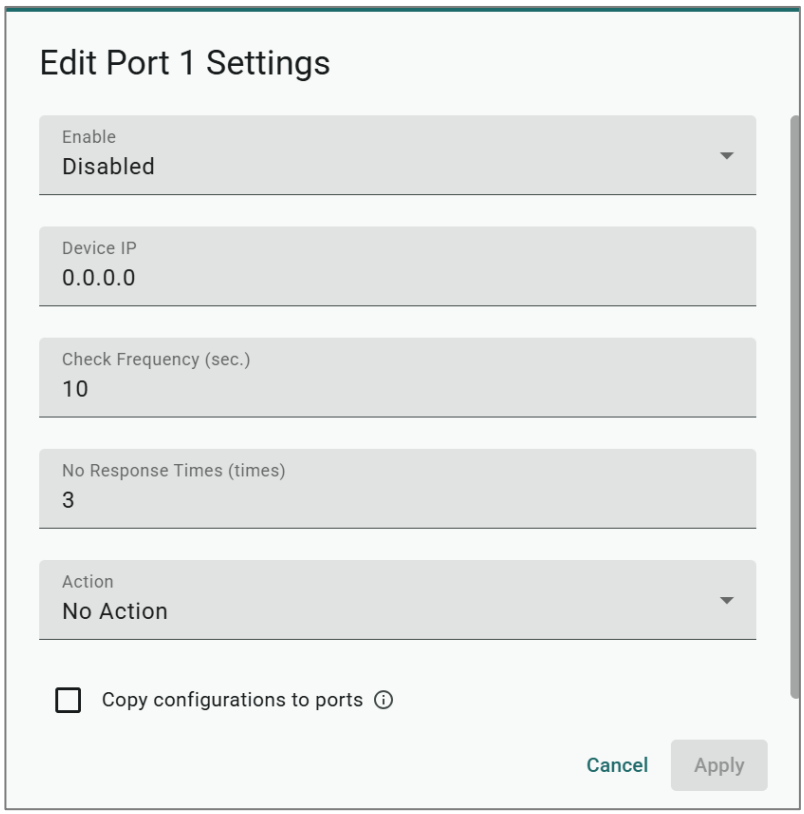
UI Setting	Description
Port	Shows which port this row describes.
PoE Supported	Shows whether the port supports PoE.
Enable	Shows whether PD failure checking is enabled or disabled for the port.
Device IP	Shows what IP will be monitored for PD failure checking for the port.
Check Frequency (sec.)	Shows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

Click **Apply** to save your changes.



UI Setting	Description	Valid Range	Default Value
Enable	Enable or disable PD failure checks for the port to check the status of PDs via ICMP.	Enabled / Disabled	Disabled
Device IP	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
Check Frequency (sec.)	Specify how frequently in seconds ping packets will be sent to to the **Device IP**. If there is no reply, a "no response" will be detected.	5 to 300	10
No Response Times (times)	Specify the number of consecutive "no response" events required to detect a PD connection failure and execute the specified **Action**.	1 to 10	3
Action	Specify the action to take when the number of **No Response Times** is reached. • **No Action**: No action will be taken. • **Restart PD**: PoE power to the PD will be stopped, then started again to restart the PD. • **Shut Down PD**: PoE power to the PD will be stopped.	No Action / Restart PD / Shut Down PD	No Action

UI Setting	Description	Valid Range	Default Value
Copy configurations to ports	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.

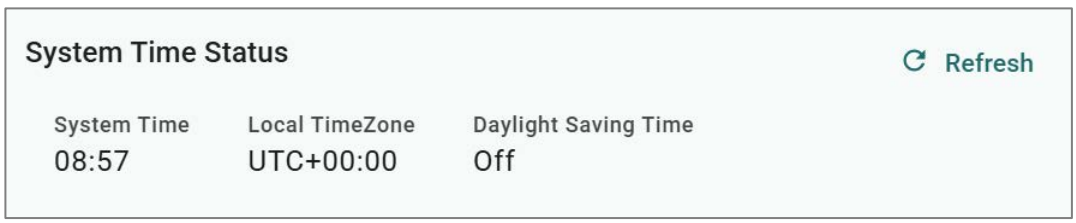
Note

This appears only in Advanced Mode.

Limitations

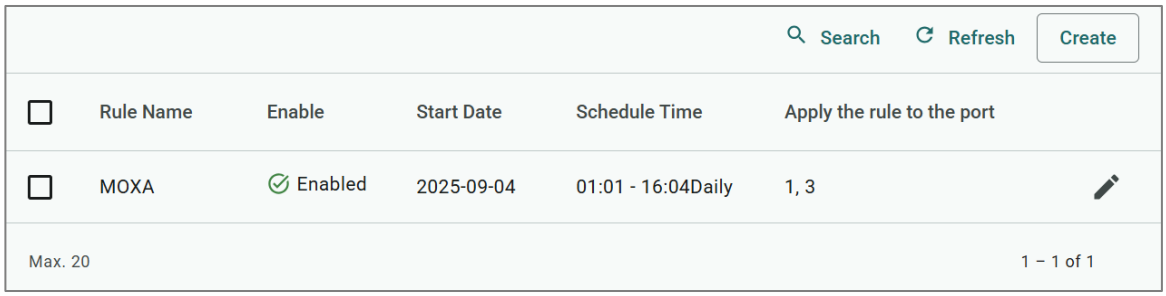
You can create up to 20 PoE scheduling rules

PoE - System Time Status



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

PoE Scheduling - Rule List



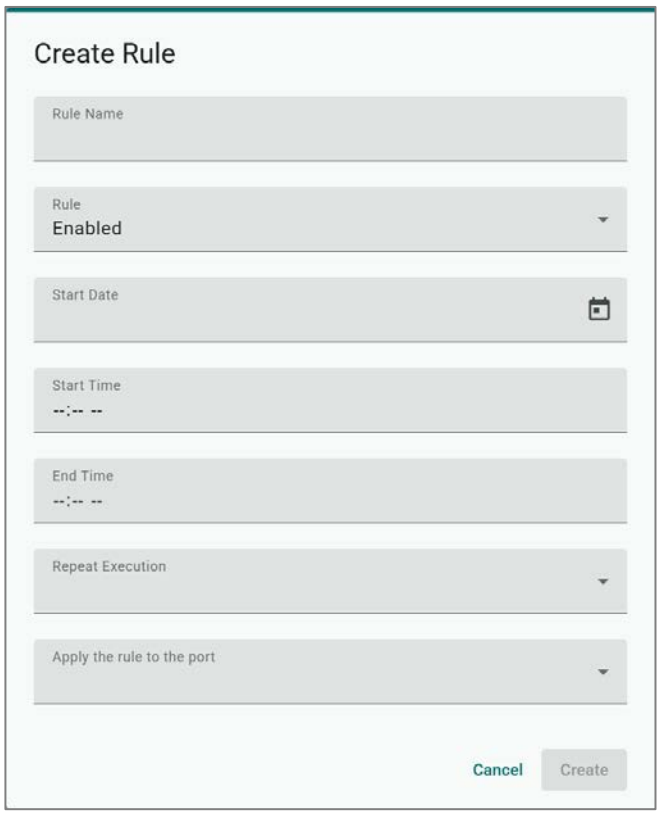
UI Setting	Description
Rule Name	Shows the name of the scheduling rule.
Enable	Shows whether the rule is enabled or disabled.
Start Date	Shows when this rule will become active.
Schedule Time	Shows when the PoE will supply power for the specified ports. The system will not supply PoE power outside the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

PoE Scheduling - Create Rule

Menu Path: Port > PoE - Scheduling

Clicking the **Create** button 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.



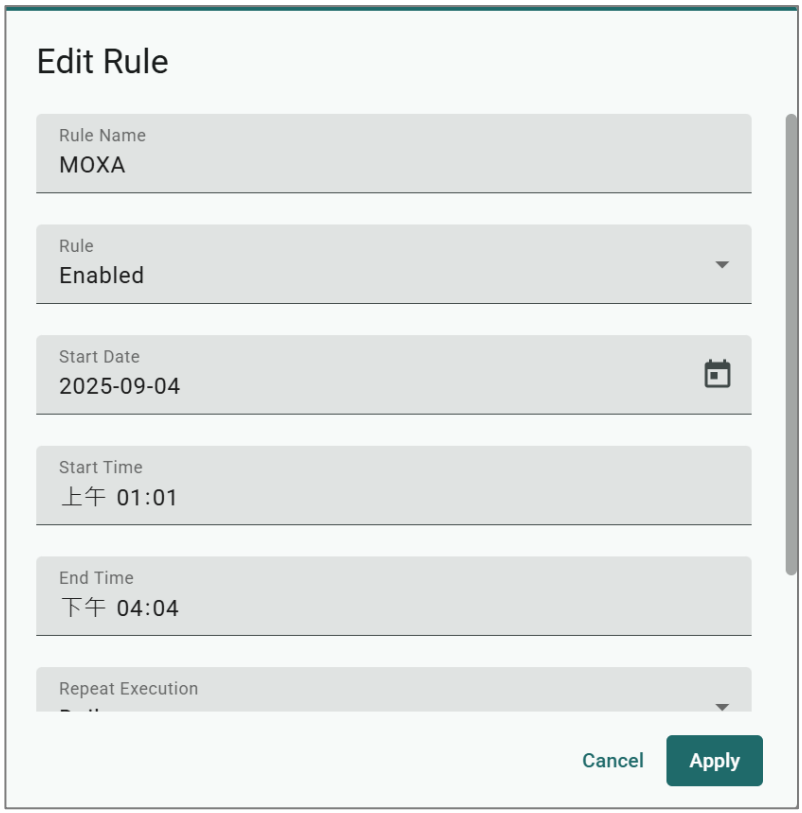
UI Setting	Description	Valid Range	Default Value
Rule Name	Specify a name for the scheduling rule.	1 to 63 characters	N/A
Rule	Enable or disable the scheduling rule.	Enabled / Disabled	Enabled
Start Date	Specify a start date for the rule to become active.	yyyy/mm/dd	N/A
Start Time	Specify a start time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

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.



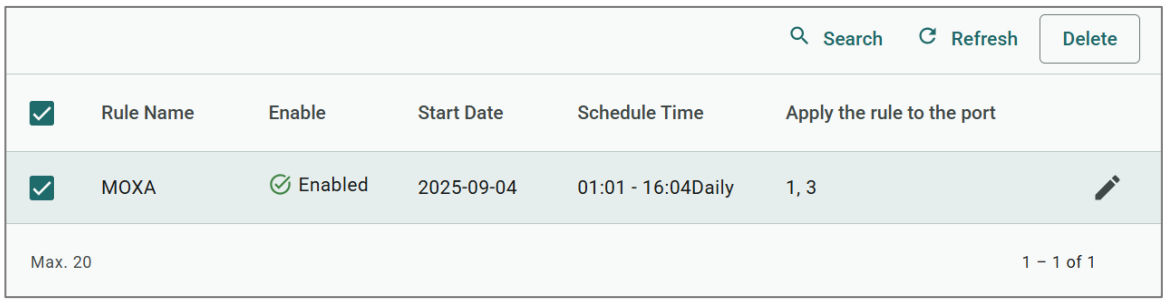
UI Setting	Description	Valid Range	Default Value
Rule Name	Specify a name for the scheduling rule.	1 to 63 characters	N/A
Rule	Enable or disable the scheduling rule.	Enabled / Disabled	Enabled
Start Date	Specify a start date for the rule to become active.	yyyy/mm/dd	N/A
Start Time	Specify a start time to enable PoE.	AM/PM hh/mm	N/A
End Time	Specify an end time to disable PoE.	AM/PM hh/mm	N/A
Repeat Execution	Specify whether to repeat execution of the rule on a daily or weekly basis.	None / Daily / Weekly	N/A

UI Setting	Description	Valid Range	Default Value
Apply the rule to the port	Specify which ports should use this rule.	Select port(s) from the drop-down list	N/A

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** button.

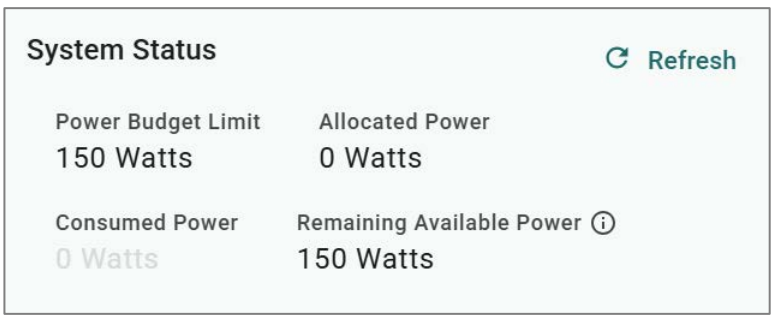


PoE - Status

Menu Path: Port > PoE - Status

This page lets you view PoE system and port status.

PoE - System Status

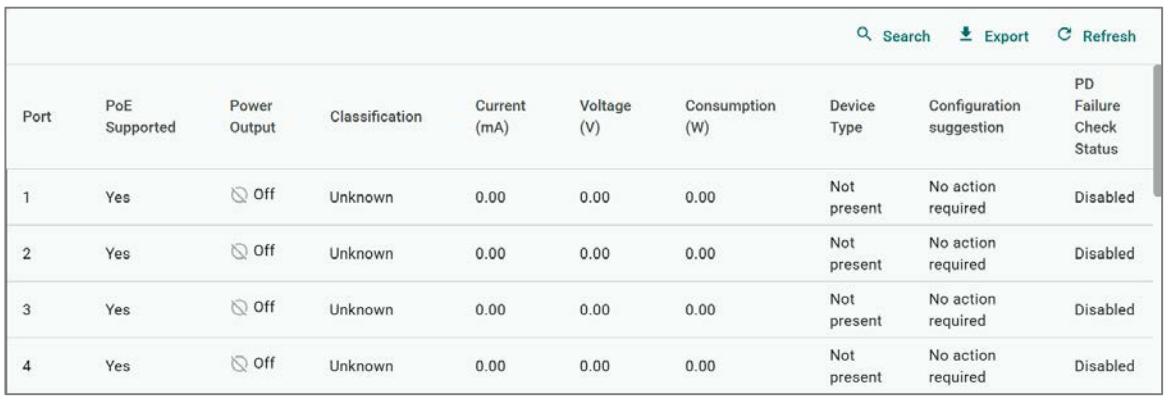


UI Setting	Description
Power Budget Limit	Shows the PoE power budget limit.
Allocated Power	Shows the total allocated PoE power.
Consumed Power	Shows the total consumed PoE power.
Remaining Available Power	Shows the remaining power available for the device. **Note** Remaining Available Power is Maximum 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 situation, the classification and device type of the PD will appear as Class 4 and 802.3at because of inherent device limitations.



UI Setting	Description
Port	Shows the number of the PoE port.
PoE Supported	Shows whether the port supports PoE.
Power Output	Shows whether PoE power output is on or off for the port.

UI Setting	Description
Classification	Shows the PoE power classification of the port. Each PoE power classification has a different maximum power (in watts) by PSE output as follows: • **0**: 15.4 watts • **1**: 4 watts • **2**: 7 watts • **3**: 15.4 watts • **4**: 30 watts
Current (mA)	Shows the amount of current (in mA) being supplied to the port.
Voltage (V)	Shows the voltage (in V) being used for the port.
Consumption (W)	Shows the power consumption (in W) of the device connected to the port.
Device Type	Shows the device type of the device currently connected to the port. • **Not Present**: There are no active connections to the port. • **Legacy PoE Device**: 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. • **802.3at**: An IEEE 802.3at PD is connected to the port. • **802.3af**: An IEEE 802.3af PD is connected to the port. • **NIC**: A NIC is connected to the port. • **Unknown**: An unknown PD is connected to the port. • **N/A**: The PoE function is disabled.
Configuration Suggestion	Shows configuration suggestions based on detected conditions. • **Disable PoE power output**: A NIC or unknown PD was detected; you may want to disable PoE power output for the port. • **Select Force Mode**: A higher/lower resistance or higher capacitance was detected; you may want to select **Force Mode** for the port. • **Select high power output**: An unknown classification was detected; you may want to select **High Power** output. • **Raise the external power supply voltage to greater than 46 VDC**: When the external supply voltage is detected at less than 46 V, the system suggests raising the voltage. • **Enable PoE function for detection**: The system suggests enabling the PoE function. • **Select IEEE 802.3at auto mode**: When detecting an IEEE 802.3at PD, the system suggests selecting 802.3at Auto mode. • **Select IEEE 802.3af auto mode**: When detecting an IEEE 802.3af PD, the system suggests selecting 802.3af Auto mode.

UI Setting	Description
PD Failure Check Status	Shows the results of the last PD failure check, if checking is enabled. Refer to PD Failure Check for more information. • **Disable**: PD failure checking is not enabled for the port. • **Alive**: The port is alive, and passed the last PD failure check. • **Not Alive**: The port is not alive, and failed the last PD failure check.

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 User Accounts for more information on user accounts.

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

Settings	Admin	Supervisor	User
Egress Shaper	R/W	R/W	R
Multicast			
IGMP Snooping	R/W	R/W	R
GMRP	R/W	R/W	R
Static Multicast	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 the 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

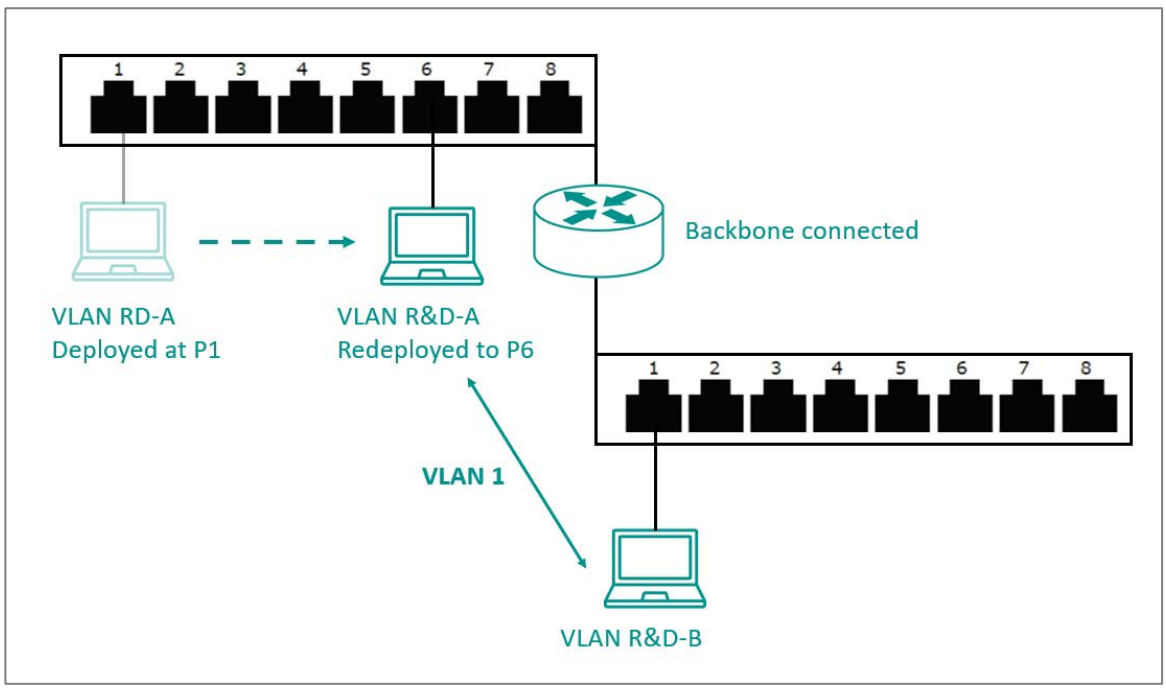
The main benefit of VLANs is that they provide a network segmentation system that is far more flexible than traditional networks. Using VLANs also provides you with three other benefits:

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.

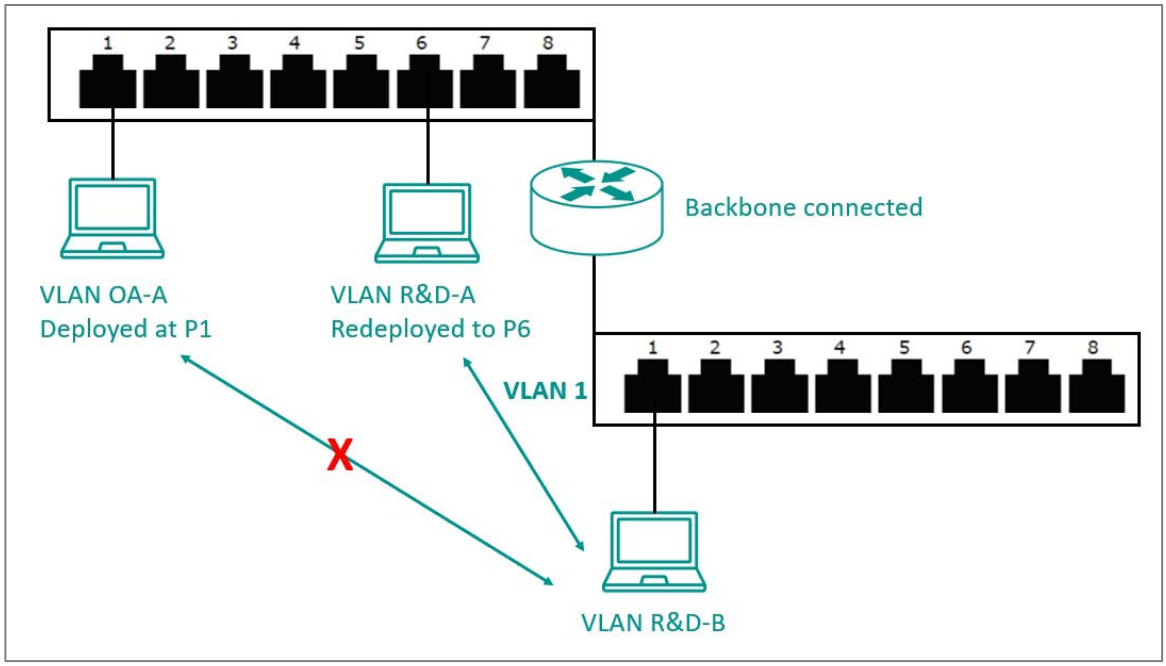
VLANs simplify device relocation

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

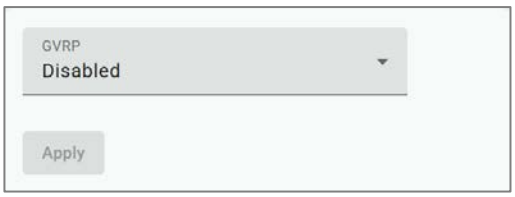
VLAN - Global

Menu Path: Layer 2 Switching > VLAN - Global

This page lets you configure the global VLAN settings.

Click **Apply** to save your changes.

VLAN Global Settings



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

VLAN - Settings

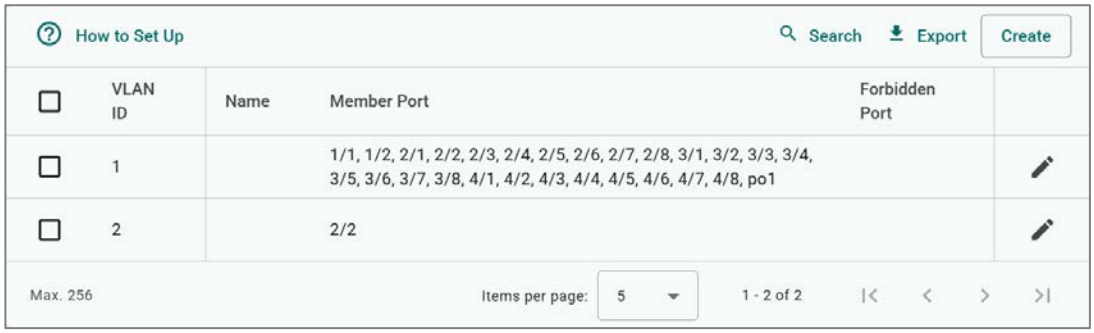
Menu Path: Layer 2 Switching > VLAN - Settings

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

Limitations

You can create up to 256 VLAN IDs.

VLAN List



UI Setting	Description
VLAN ID	Shows the ID of the VLAN.
Name	Shows the name of the VLAN.
Member Port	Shows the member port(s) of the VLAN.
Forbidden Port **(Only in Advanced Mode)**	Shows the forbidden port(s) of the VLAN.

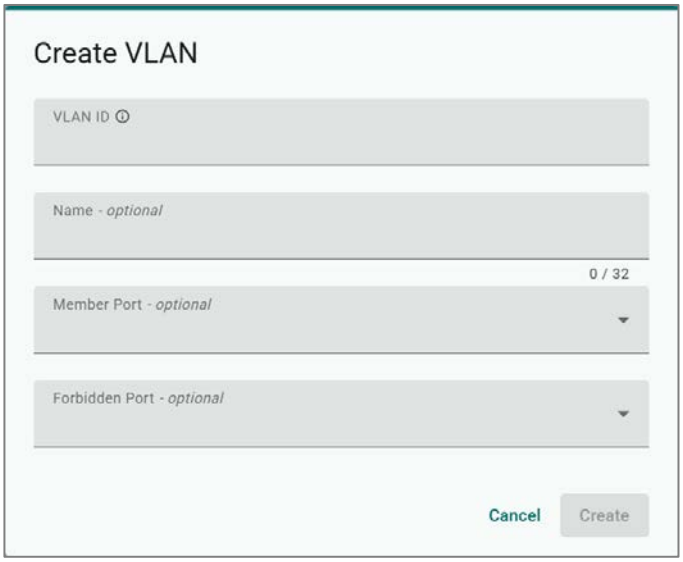
VLAN - Create VLAN

Menu Path: Layer 2 Switching > VLAN - Settings

Clicking **Create** on the **Layer 2 Switching > VLAN - Settings** page will open this dialog box. This dialog lets you create a VLAN.

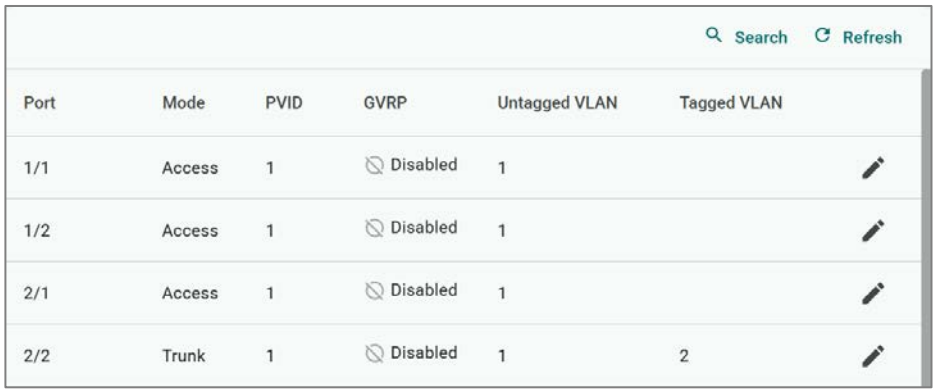
Click **Create** to save your changes.

Create VLAN



UI Setting	Description	Valid Range	Default Value
VLAN ID	Specify the VLAN ID.	1 to 4094	N/A
Name	Specify the name of the VLAN.	0 to 32 characters, must start with a letter (a-z, A-Z)	N/A
Member Port	Specify the member port(s) of the specific VLAN.	Drop-down list of ports	N/A
Forbidden Port **(Only in Advanced Mode)**	Specify the forbidden port(s) of the specific VLAN.	Drop-down list of ports	N/A

VLAN Port List



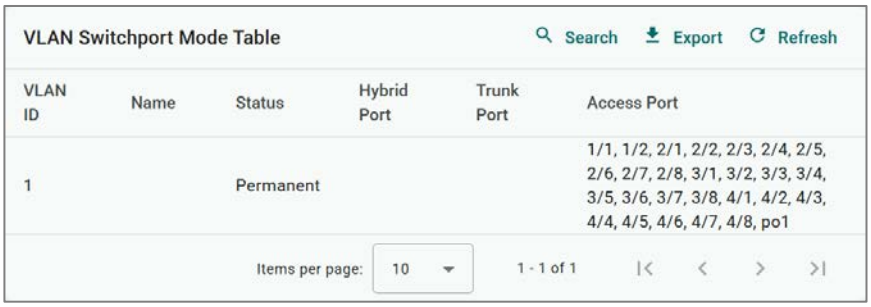
UI Setting	Description
Port	Shows the port number.
Mode	Shows the mode of the port. • **Access**: The port is connected to a single device, without tags. • **Trunk**: The port is connected to another 802.1Q VLAN aware switch. • **Hybrid**: The port is connected to another 802.1Q VLAN aware switch or another LAN that combines tagged and/or untagged devices.
PVID	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.
GVRP	Shows whether GVRP is enabled for the port.
Untagged VLAN	When the port is using **Hybrid** VLAN mode, this shows all VLAN IDs that will be removed from egress packets.
Tagged VLAN	When the port is using **Trunk** or **Hybrid** VLAN mode, this shows all VLAN IDs will be carried to connected devices.

VLAN - Status

Menu Path: Layer 2 Switching > VLAN - Status

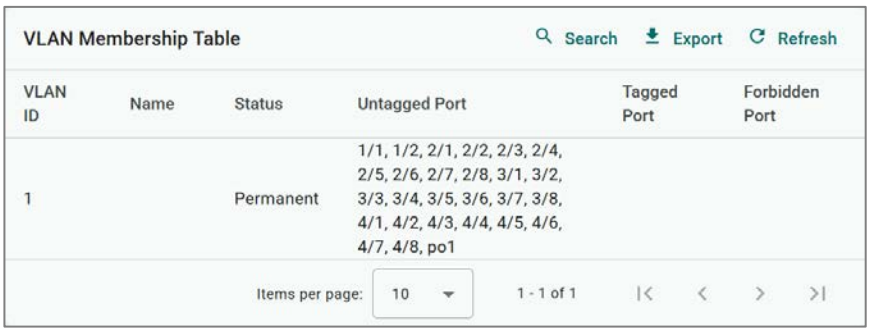
This page lets you monitor the status of the VLANs on your device.

VLAN Switchport Mode Table



UI Setting	Description
VLAN ID	Shows the ID of the VLAN.
Name	Shows the name of the VLAN.
Status	Shows the status of the VLAN.
Hybrid Port	Shows ports acting as a Hybrid Port for the VLAN.
Trunk Port	Shows ports acting as a Trunk Port for the VLAN.
Access Port	Shows ports acting as an Access Port for the VLAN.

VLAN Membership Table



UI Setting	Description
VLAN ID	Shows the ID of the VLAN.
Name	Shows the name of the VLAN.

UI Setting	Description
Status	Shows the status of the VLAN.
Untagged Port	Shows the untagged port(s) for the VLAN.
Tagged Port	Shows the tagged port(s) for the VLAN.
Forbidden Port **(Only in Advanced Mode)**	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.

Note

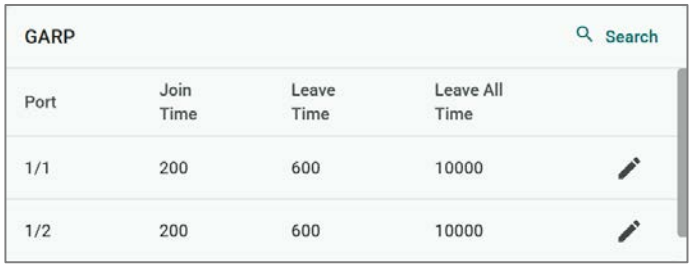
This feature supports weaker authentication or encryption, and may not be secure over untrusted networks. Take appropriate security precautions.

GARP Settings

Menu Path: Layer 2 Switching > GARP

This page lets you configure GARP settings for each port.

GARP List



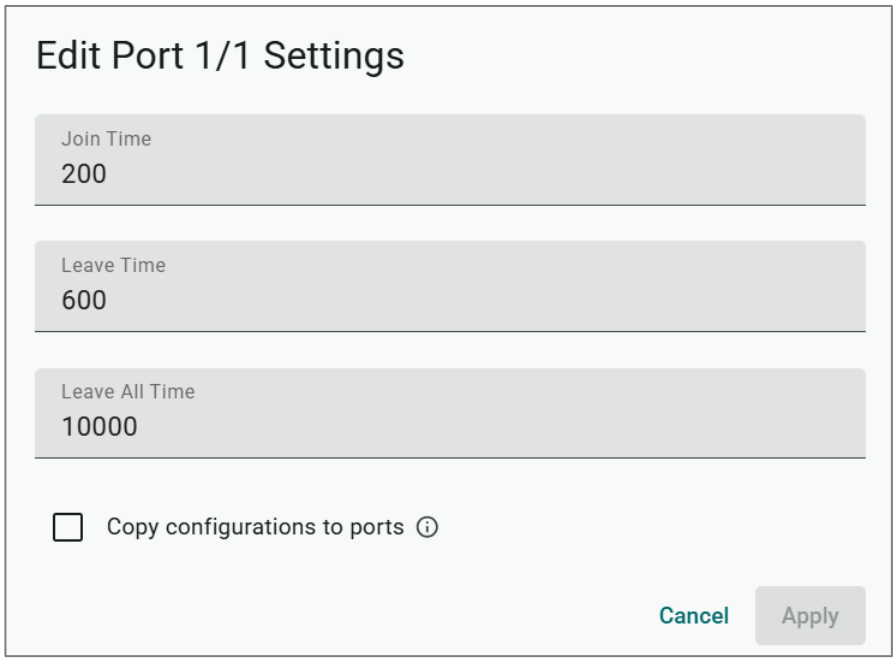
UI Setting	Description
Port	Shows which port the entry is for.
Join Time (sec.)	Shows the join time in seconds for the port.
Leave Time (sec.)	Shows the leave time in seconds for the port.
Leave All time (sec.)	Shows the leave all time in seconds for the port.

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.



UI Setting	Description	Valid Range	Default Value
Join Time (sec.)	Specify the join time in seconds.	10 to 499999980	200
Leave Time (sec.)	Specify the leave time in seconds.	30 to 499999980	600
Leave All time (sec.)	Specify the leave all time in seconds.	30 to 499999990	10000
Copy configurations to ports	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

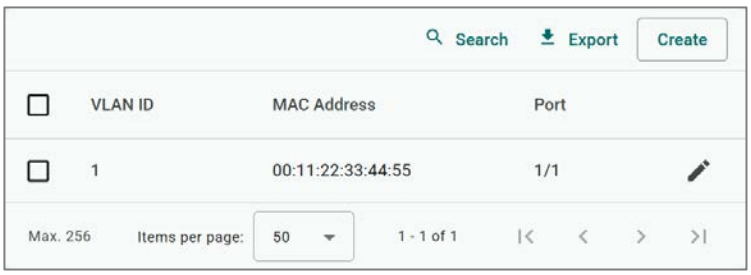
Menu Path: Layer 2 Switching > MAC > Static Unicast

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

Limitations

You can create up to 256 static unicast entries.

Unicast Table



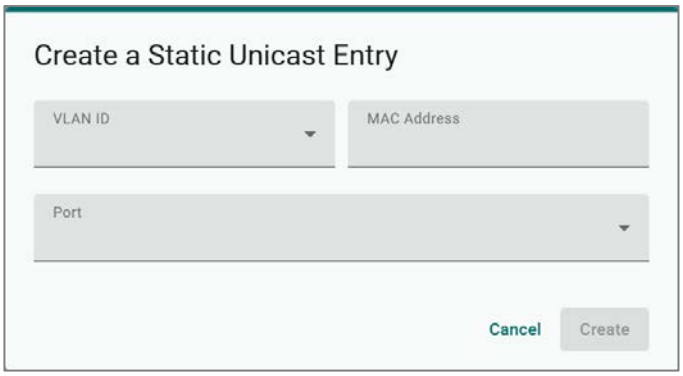
UI Setting	Description
VLAN ID	Shows the VLAN ID used for the static unicast entry.
MAC Address	Shows the MAC address used for the static unicast entry.
Port	Shows which ports are included for the static unicast entry.

Add a Static Unicast Entry

Menu Path: Layer 2 Switching > MAC > Static Unicast

Clicking **Create** 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.



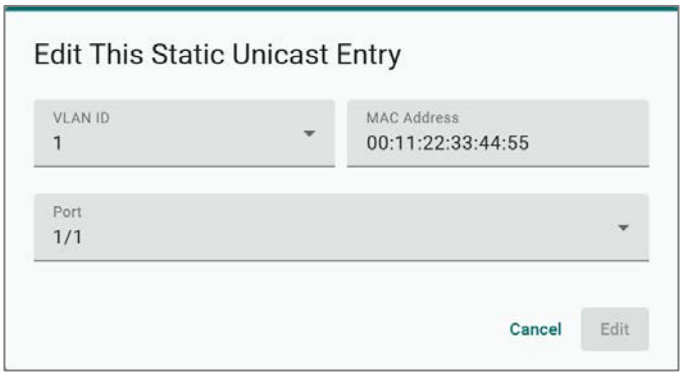
UI Setting	Description	Valid Range	Default Value
VLAN ID	Specify the VLAN ID.	Drop-down list of VLAN IDs	N/A
MAC Address	Specify the static unicast MAC address of the port.	Valid unicast MAC address	N/A
Port	Specify which ports you want to include in the static unicast group	Drop-down list of ports	N/A

Edit a Static Unicast Entry

Menu Path: Layer 2 Switching > MAC > Static Unicast

Clicking the **Edit (✎)** icon for an entry on the **Layer 2 Switching > MAC > Static Unicast** page will open this dialog box. This dialog lets you edit the static unicast entry.

Click **Apply** to save your changes.



UI Setting	Description	Valid Range	Default Value
VLAN ID	Specify the VLAN ID.	Drop-down list of VLAN IDs	N/A
MAC Address	Specify the static unicast MAC address of the port.	Valid unicast MAC address	N/A
Port	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.

Click **Apply** to save your changes.

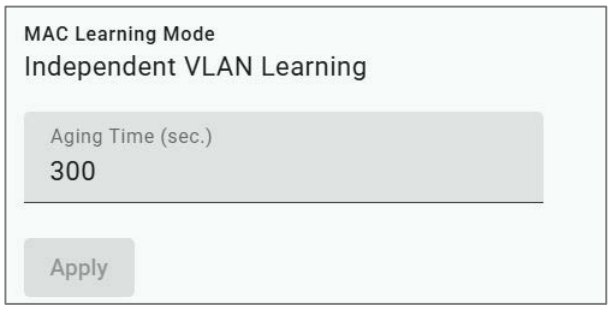
Limitations

The MAC address table can hold up to 16384 entries.

Note

MAC Sticky entries are not shown in the MAC address table; they are only shown on the Security > Network Security > Port Security - MAC Sticky page.

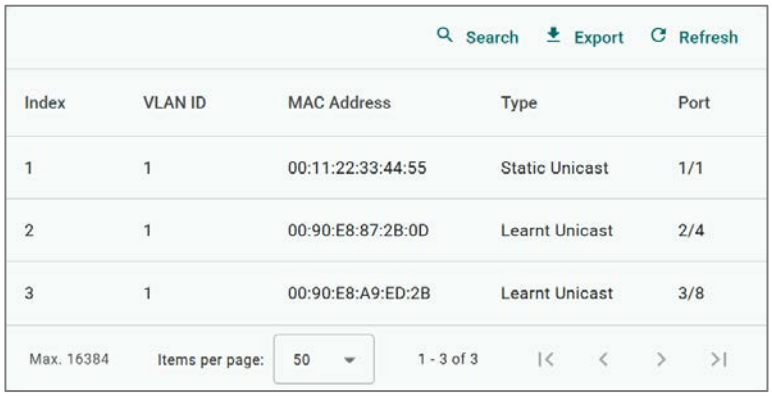
MAC Address Settings



UI Setting	Description	Valid Range	Default Value
MAC Learning Mode	Shows the current MAC learning mode.	N/A	Independent VLAN Learning

UI Setting	Description	Valid Range	Default Value
Aging Time	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

MAC Address Table List



UI Setting	Description
Index	Shows the index number of the MAC address.
VLAN ID	Shows which VLAN ID is being used for the MAC address.
MAC Address	Shows the MAC address of the device.
Type	Shows what kind of MAC address entry this is: **Learnt Unicast**: Used for all learnt unicast MAC addresses. **Learnt Multicast**: Used for all learnt multicast MAC addresses. **Static Unicast**: Used for all static unicast MAC addresses. **Static Multicast**: Used for all static multicast MAC addresses.
Port	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.

Network administrators can use Strict Priority and Weighted Round Robin scheduling algorithms—as well as a mix of the two—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 devices will exhibit identical QoS behavior.

About 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.

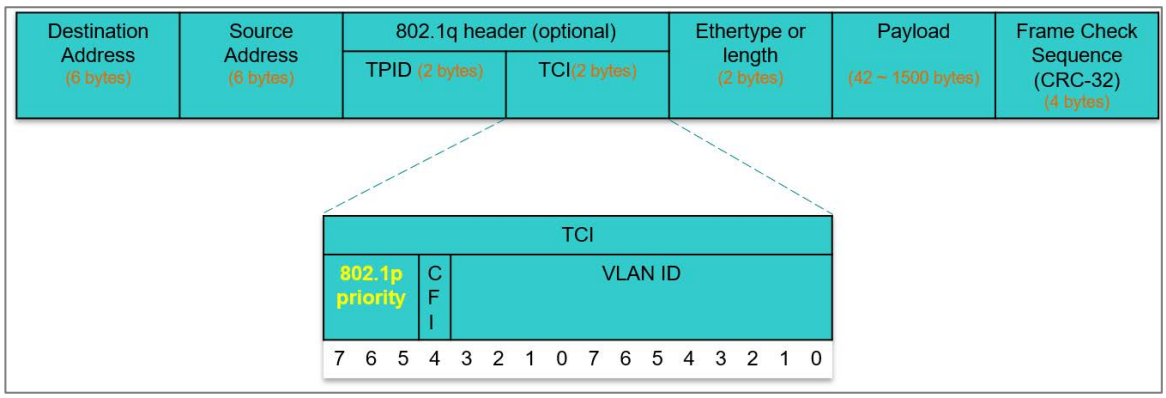
Traffic classification and prioritization for your Moxa device is based on two standards:

- **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)

IEEE 802.1p Priority (decimal)	IEEE 802.1p Priority (binary)	IEEE 802.1D Traffic Type
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

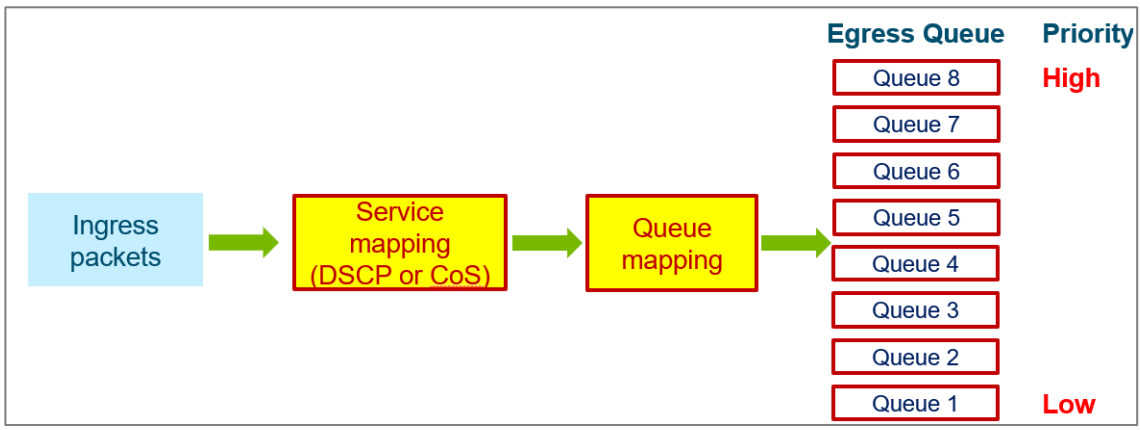
reaches the head of its queue and is about to be transmitted, the device determines whether or not the egress port belongs to the VLAN group. If it is, then the new 802.1p tag is used in the extended 802.1D header.

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 is 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



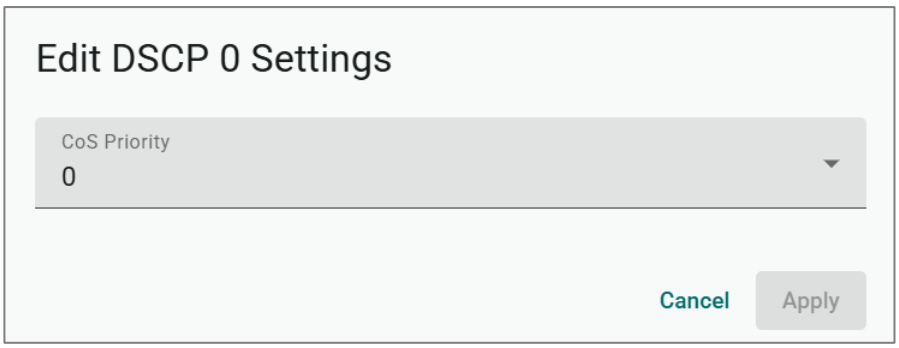
UI Setting	Description
DSCP	Shows the DSCP value for the entry.
CoS Priority	Shows the CoS priority mapped to the DSCP value.

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.



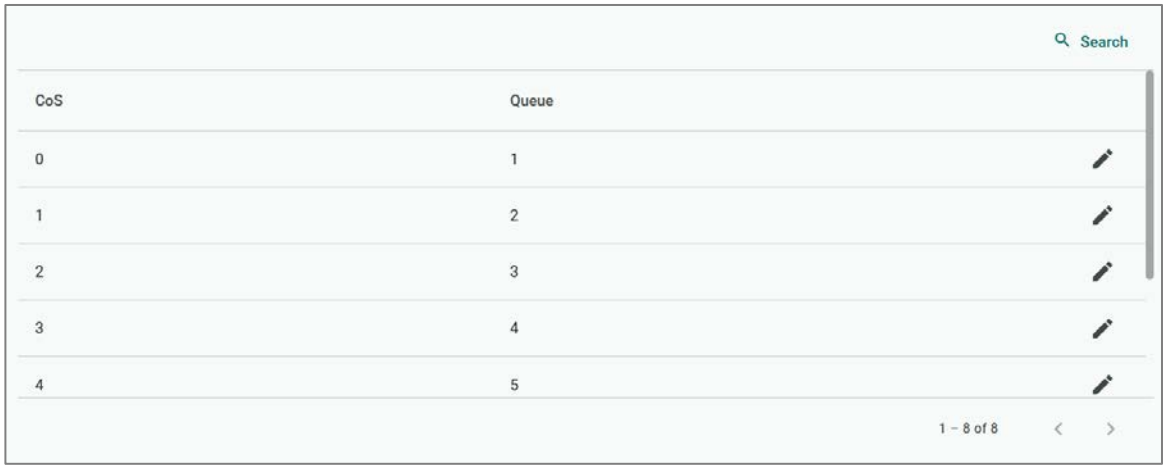
UI Setting	Description	Valid Range	Default Value
CoS Priority	Specify the CoS priority to assign to the DSCP value. Higher numbers have higher priority.	0 to 7	DSCP 0 to 7: 0 DSCP 8 to 15: 1 DSCP 16 to 23: 2 DSCP 24 to 31: 3 DSCP 32 to 39: 4 DSCP 40 to 47: 5 DSCP 48 to 55: 6 DSCP 56 to 63: 7

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



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



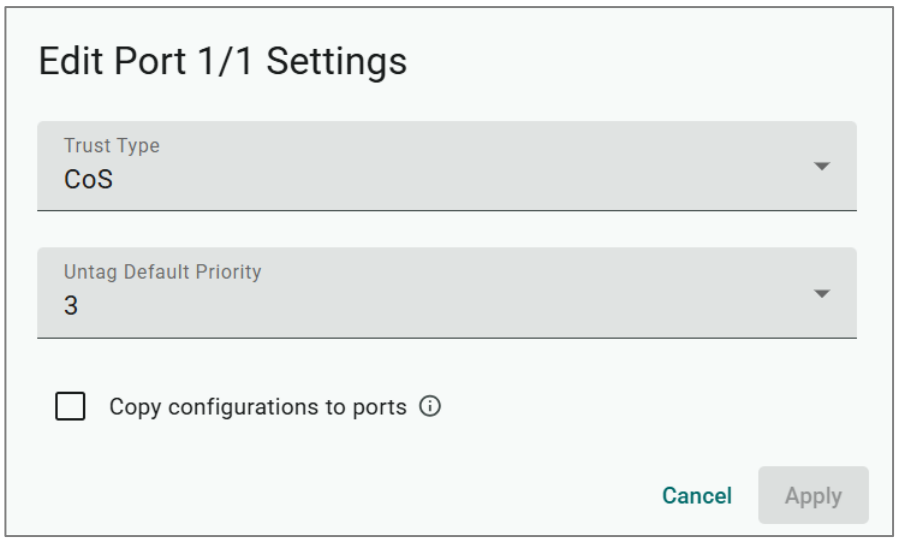
UI Setting	Description
Port	Shows the port number for the entry.
Trust Type	Shows the trust type used to classify traffic for the port.
Priority	Shows the CoS value to use for untagged packets for the port.

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.



UI Setting	Description	Valid Range	Default Value
Trust Type	Select the trust type used to classify traffic for the port.	CoS / DSCP	CoS
Untag Default Priority	Specify a CoS value to use for untagged packets for the port. Higher values will have higher priority.	0 to 7	3
Copy configurations to ports	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.

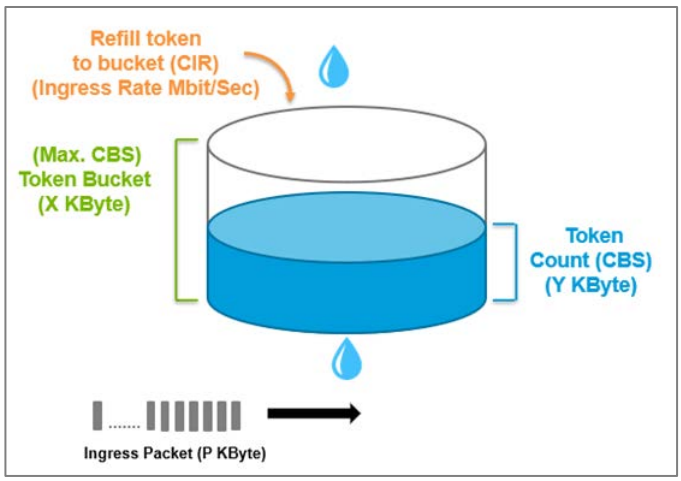
In general, any user shall not consume unlimited bandwidth and influence others' access. One particular scenario is that a malfunctioning switch or mis-configured network might cause "broadcast storms". Moxa industrial Ethernet switches not only prevent broadcast storms, but can also regulate ingress 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.

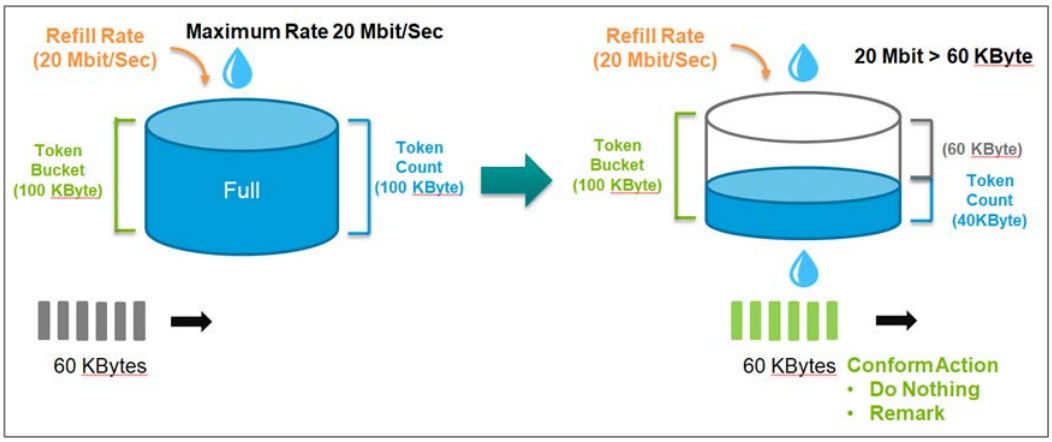
About Token Buckets

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)

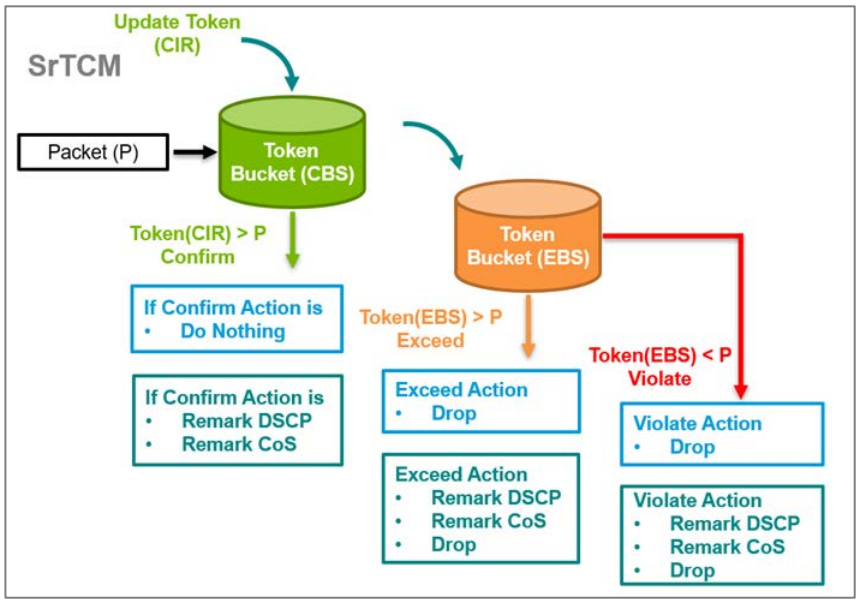
A packet is marked green if it does not exceed the CBS, yellow if it does exceed the CBS, but not the EBS, and red otherwise.

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

You can set up the ingress rate limits to 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
Type	**Simple Token Bucket**
Ingress Rate (CIR)	5 Mbps
Conform Action	**Remark DSCP**
Conform Action > Remark Value	**0**
Violate Action	**Remark DSCP**
Violate Action > Remark Value	**7**

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

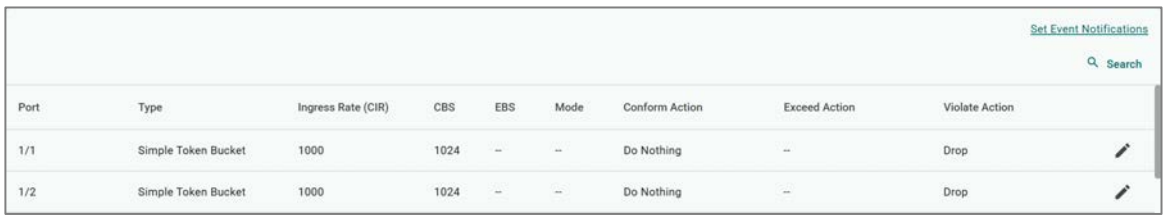
Ingress Rate Limit - General

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.



UI Setting	Description
Port	Shows the port number for the entry.
Type **(Only in Advanced Mode)**	Shows the ingress limit type for the port.
Ingress Rate (CIR)	Shows the ingress Committed Information Rate (CIR) value for the port.

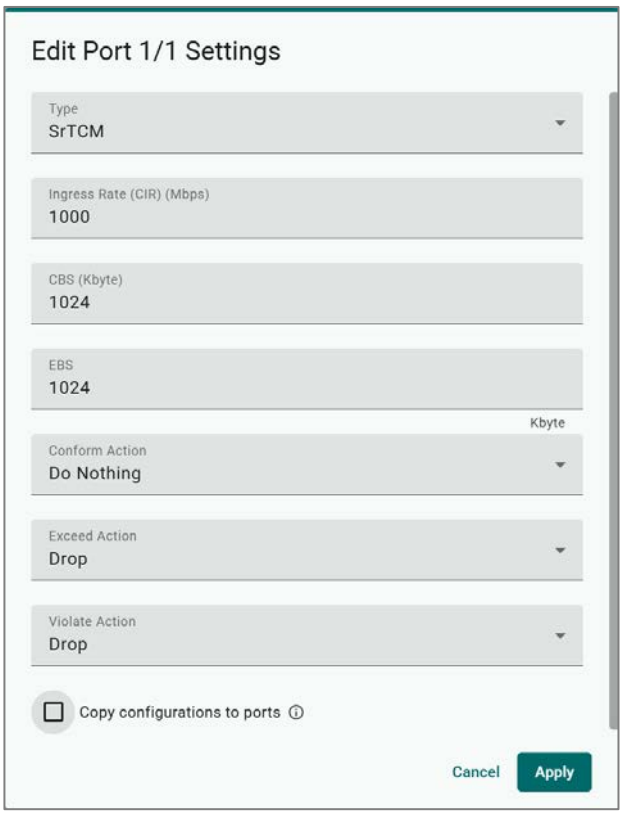
UI Setting	Description
CBS **(Only in Advanced Mode)**	Shows the ingress Committed Burst Size (CBS) value for the port.
EBS **(Only in Advanced Mode)**	Shows the ingress Excess Burst Size (EBS) value for the port.
Mode **(Only in Advanced Mode)**	Shows the meter mode for the port.
Conform Action **(Only in Advanced Mode)**	Shows the conform action for the port.
Exceed Action **(Only in Advanced Mode)**	Shows the exceed action for the port.
Violate Action	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.



UI Setting	Description	Valid Range	Default Value
Type **(Only in Advanced Mode)**	Specify the ingress limit type to use.	Simple Token Bucket / SrTCM	Simple Token Bucket
Ingress Rate (CIR)	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
CBS (Committed Burst Size) **(Only in Advanced Mode)**	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.	10 to 10240	1024
EBS (Excess Burst Size) **(Only in Advanced Mode, if Type is SrTCM)**	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.	10 to 10240	1024

UI Setting	Description	Valid Range	Default Value
Conform Action **(Only in Advanced Mode)**	Select a conform action for the port to take. If **Remark CoS** or **Remark DSCP** is selected, an additional input field will appear where a Remark value must be specified.	Do Nothing / Remark CoS / Remark DSCP	Do Nothing
Exceed Action **(Only in Advanced Mode, if Type is SrTCM)**	Select an action to take if the amount of data exceeds both the CBS and EBS buffers. • **Drop**: Packets marked as yellow will be dropped. • **Remark CoS**: Specify a CoS Remark value to use if a packet is marked as yellow. This is only available if **Remark CoS** is selected for the **Conform Action**. • **Remark DSCP**: Specify a DSCP Remark value to use if a packet is marked as yellow. This is only available if **Remark DSCP** is selected for the **Conform Action**.	Drop / Remark CoS / Remark DSCP	Drop
Violate Action	Select an action to take if a packet violates CIR and CBS. • **Drop:** Packets marked as violated will be dropped. • **Remark CoS**: Specify a CoS Remark value to use if a packet is marked as violated. This is only available if **Remark CoS** is selected for the **Conform Action**. • **Remark DSCP**: Specify a DSCP Remark value to use if a packet is marked as violated. This is only available if **Remark DSCP** is selected for the **Conform Action**.	Drop / Remark CoS / Remark DSCP	Drop
Copy configurations to ports	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



UI Setting	Description	Valid Range	Default Value
Port Shutdown	Enable or disable the port shutdown feature for the device. **Note** After enabling this, you will still need to configure port shutdown for each port you want to use the feature with.	Enabled / Disabled	Disabled
Release Interval	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



UI Setting	Description
Port	Shows the port number for the entry.
Port Shutdown	Shows whether port shutdown is enabled or disabled for the port.

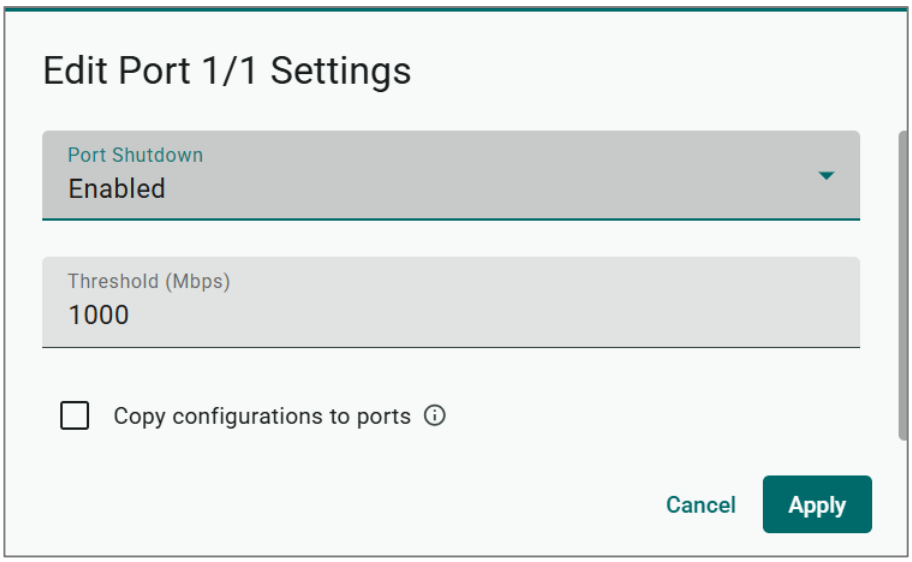
UI Setting	Description
Threshold (Mbps)	Shows the threshold in Mbps required to trigger port shutdown for the port.

Port Shutdown - Edit Port Settings

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

Clicking the **Edit (✎)** icon for a 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
Port Shutdown	Enable or disable port shutdown for this port.	Enabled / Disabled	Disabled
Threshold	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
Copy configurations to ports	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 the following scheduling algorithms: Strict Priority, Weighted Round Robin, and a mix of both.

- **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 Priority:** 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.
- **Strict Priority and Weighted Round Robin:** Supports one Strict Priority queue with seven Weighted Round Robin queues, or two Strict Priority queues with six Weighted Round Robin queues.

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 Scheduler for Strict Priority

Strict Priority switching ensures that higher priority packets always preempt lower priority packets.

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]**.

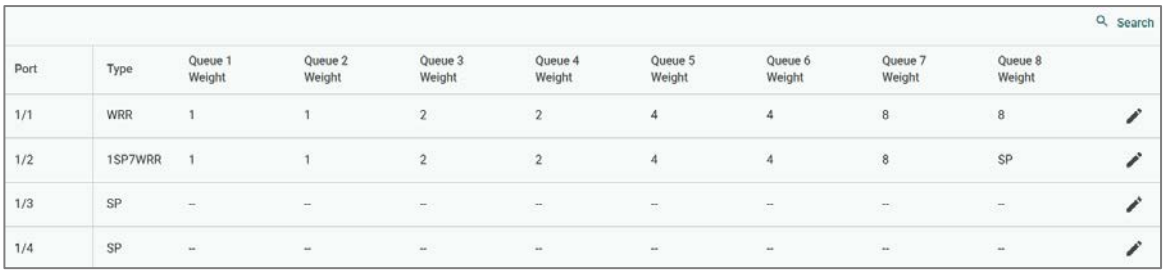
   The Edit Port Settings screen appears.
4. Make sure **Type** is set to **Strict Priority**, and then click **Apply**.

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



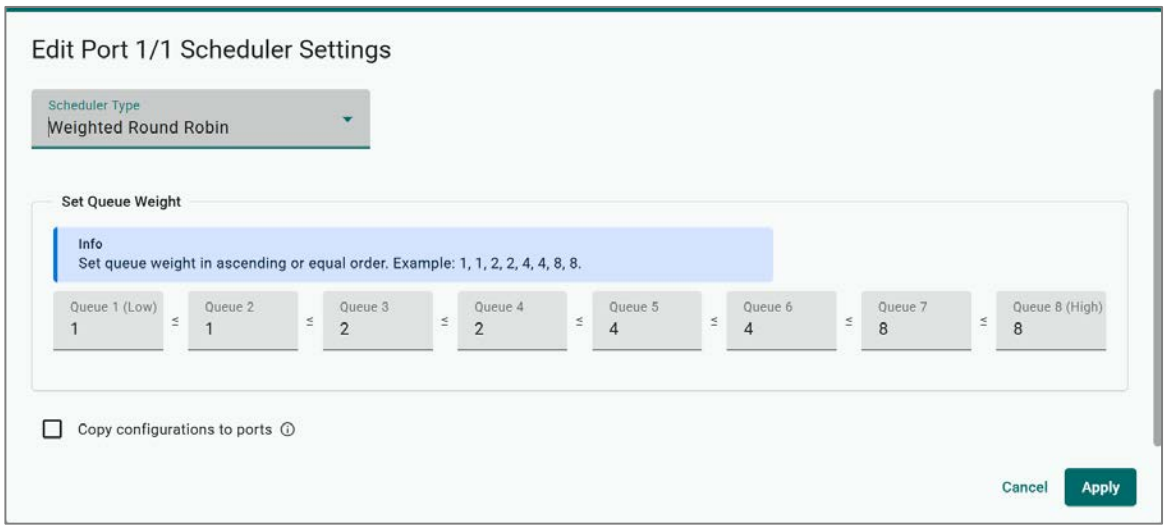
UI Setting	Description
Port	Shows the port number for the entry.
Type	Shows the scheduling algorithm selected for the port.
Queue 1 - 8 Weight	Shows the weight associated with the queue. SP indicates the queue uses strict priority.

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.



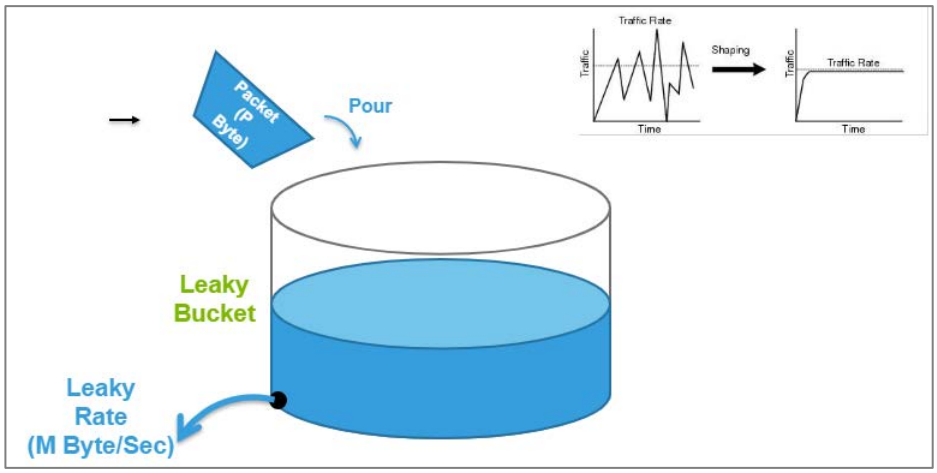
UI Setting	Description	Valid Range	Default Value
Scheduler Type	Select the scheduler algorithm to use for the port. • **Strict Priority**: Strict priority will be used. • **Weighted Round Robin**: Queued packets will be forwarded based on their associated weight. • **1SP7WRR**: Queue 8 will use Strict Priority and the packets in other queues will be forwarded based on their associated weight. • **2SP6WRR**: Queues 7 and 8 will use Strict Priority and the packets in other queues will be forwarded based on their associated weight.	Strict Priority / Weighted Round Robin / 1SP7WRR / 2SP6WRR	Strict Priority
Queue 1 - 8	Specify the weight for packets forwarded in each queue. **Note** If Scheduler Type is 1SP7WRR, Queue 8 will be fixed to strict priority (SP). If Scheduler Type is 2SP6WRR, Queues 7 and 8 will be fixed to strict priority (SP).	1 to 8 Subsequent queue weights must be equal or higher than the previous one.	1,1,2,2,4,4,8,8
Copy configurations to ports	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 queses 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:

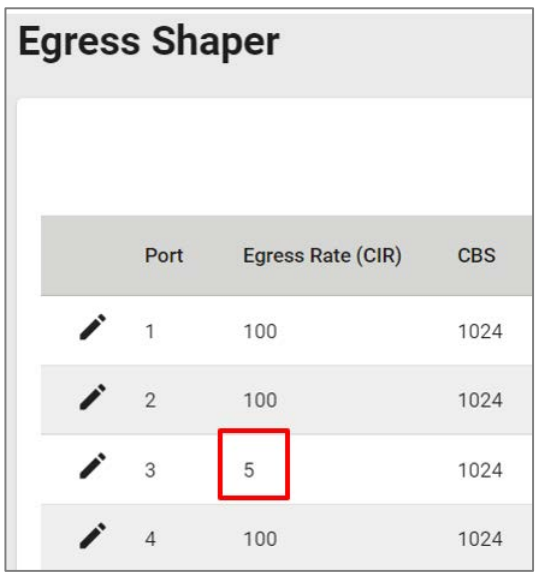
- Device A, connected to the switch at Port 1
- Device B, connected to the switch at Port 2
- Device C, connected to the switch at Port 3

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

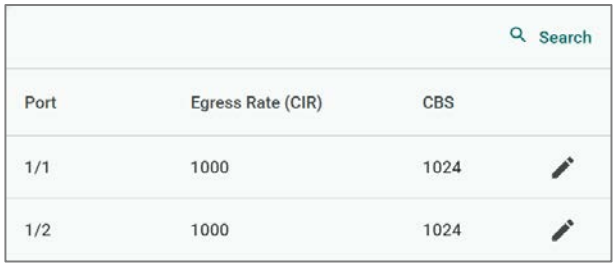
1. Sign in to the device using administrator credentials.
2. Go to **Layer 2 Switching > QoS > Egress Shaper**.
3. Click ***[Edit]*** corresponding to **Port 3**.
   Result: The **Edit Port Settings** dialogue appears.
4. In the **CIR** field, specify 5 Mbps, and then click **Apply**.
   Result: The new Egress Rate (CIR) will appear in the table.



Egress Shaper

Menu Path: Layer 2 Switching > QoS > Egress Shaper

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



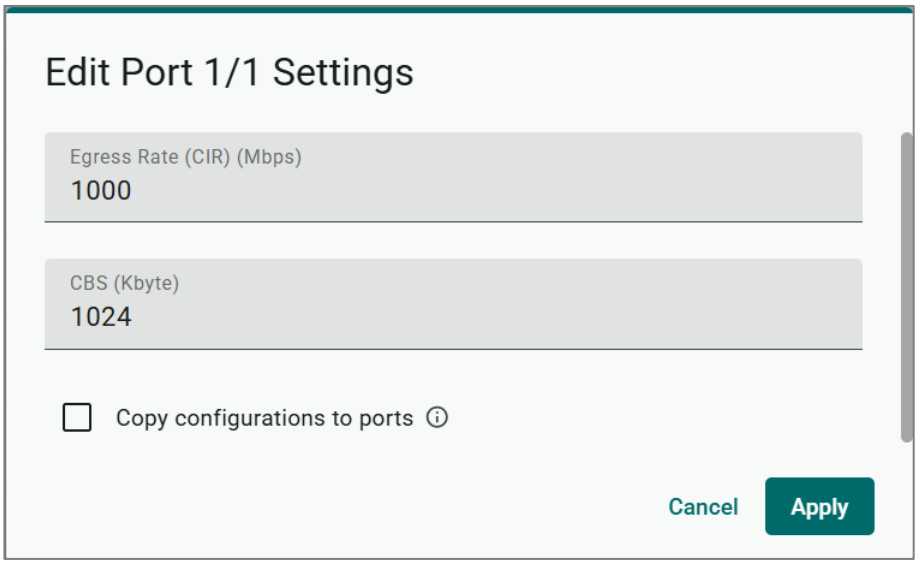
UI Setting	Description
Port	Shows the port number the entry is for.
Egress Rate (CIR)	Shows the egress Committed Information Rate (CIR) value for the port.
CBS **(Only in Advanced Mode)**	Shows the egress Committed Burst Size (CBS) value for the port.

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
Egress Rate (CIR)	Specify the egress Committed Information Rate (CIR) in Mbps.	Fast Ethernet ports: 1 to 100 Gigabit Ethernet ports: 1 to 1000	Fast Ethernet ports: 100 Gigabit Ethernet ports: 1000
CBS **(Only in Advanced Mode)**	Specify the Committed Burst Size (CBS) in KB. This is the maximum amount of data allowed to be transmitted in a burst, even if it would cause the CIR rate to be exceeded.	10 to 10240	1024
Copy configurations to ports	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

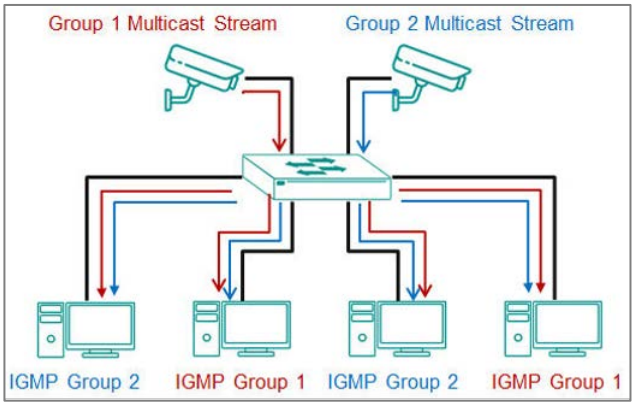
About IGMP Snooping

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.

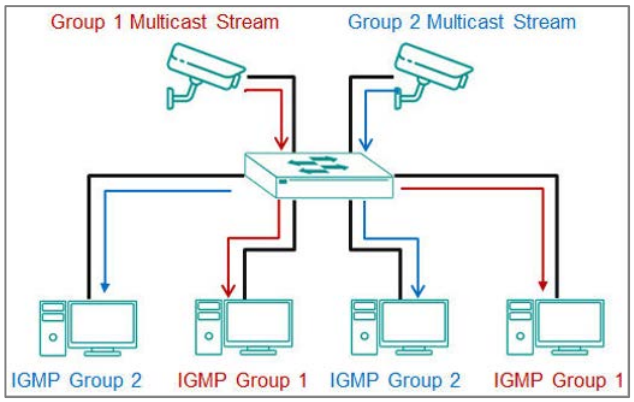
How IGMP Snooping Works

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:



Note

This feature supports weaker authentication or encryption, and may not be secure over untrusted networks. Take appropriate security precautions.

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
IGMP Snooping	**Enabled**
Version	Choose a version corresponding to device support and feature needs.
Query Interval	125
Static Router Port	This is optional.
Config Role	**Querier**

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	Features: • **Multicast Group Membership:** Host devices can join multicast groups, but there is no explicit leave message. The host will simply stop responding to membership queries. • **Membership Query:** Network devices periodically send membership queries to determine if any host devices are still interested in receiving multicast traffic. • **Membership Report:** 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. 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.	RFC-1112
v2	Additional features: • **Leave Group Message:** 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. • **Group-Specific Queries:** 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. • **Query Election:** Introduces a mechanism to elect a single query router on a subnet to avoid redundant queries, thereby optimizing network bandwidth.	RFC-2236
v3	Additional Features: • **Source-Specific Multicast (SSM):** 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. • **Include/Exclude Mode:** Host devices can explicitly include or exclude traffic from specified sources, providing more granular control over multicast group membership. • **Membership Report Enhancements:** The membership report format is enhanced to support the new source filtering capabilities.	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.

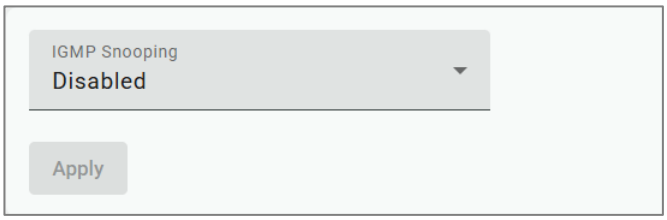
This page includes these tabs:

- 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.

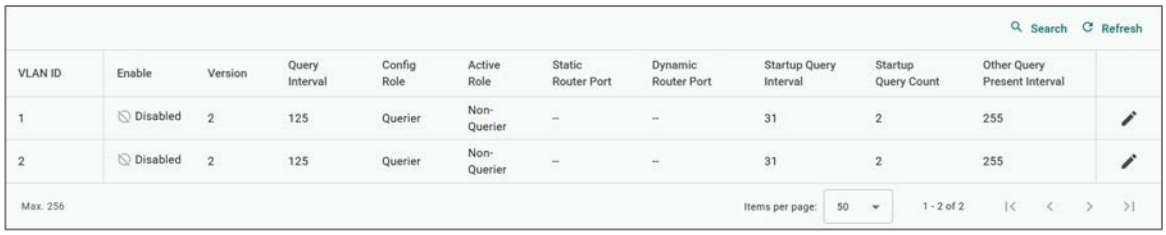


UI Setting	Description	Valid Range	Default Value
IGMP Snooping	Enable or disable IGMP snooping for the device. **Note** IGMP Snooping cannot be enabled when GMRP is enabled.	Enabled / Disabled	Disabled

IGMP Snooping - VLAN Settings

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

This page lets you configure IGMP snooping VLAN settings.



UI Setting	Description
VLAN ID	Shows the ID of the VLAN ID the entry is for.
Enable	Shows whether IGMP snooping is enabled for the VLAN.
Version	Shows the IGMP version of the packets the VLAN will listen to and send queries for.
Query Interval	Shows the query interval for the Querier function globally for the VLAN, if the Querier is enabled.
Config Role	Shows the config role of the VLAN.
Active Role	Shows the active role of the VLAN.
Static Router Port	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.
Dynamic Router Port	Shows the dynamic router port for the VLAN.
Startup Query Interval **(Only in Advanced Mode)**	Shows the amount of time in seconds to wait between sending IGMP queries after the VLAN interface starts up.
Startup Query Count **(Only in Advanced Mode)**	Shows how many IGMP queries will be sent after the VLAN interface starts up.

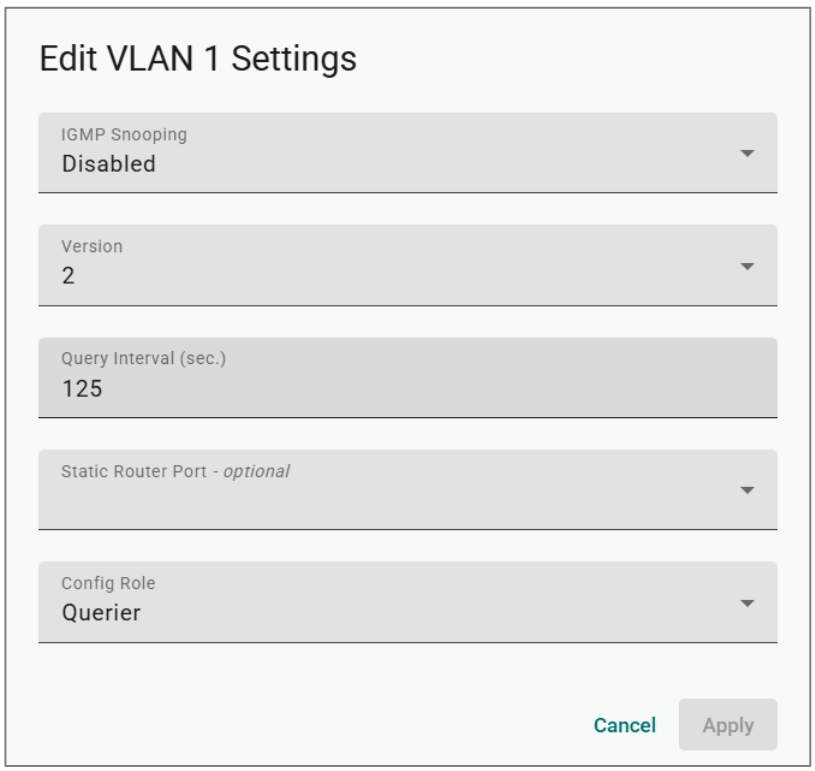
UI Setting	Description
Other Query Present Interval **(Only in Advanced Mode)**	Shows the amount of time in seconds the device waits after receiving an IGMP query from another querier before assuming the querier is no longer present. During this time, the device will not send out any queries. This interval is automatically determined based on the **Query Interval**.

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.



UI Setting	Description	Valid Range	Default Value
IGMP Snooping	Enable or disable IGMP snooping for the VLAN.	Enabled / Disabled	Disabled

UI Setting	Description	Valid Range	Default Value
Version	Specify the IGMP version of the packets to listen to and send queries for.	1 / 2 / 3	2
Query Interval	Specify the query interval for the VLAN, if the Querier is enabled.	20 to 600 sec.	125 sec.
Static Router Port	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
Config Role	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.

Limitations

There can be up to 1024 IGMP snooping group table entries.



Item	Description
VLAN	Shows the ID of the VLAN the entry is for.
Group Address	Shows the registered multicast group address for the VLAN.

Item	Description
Filter Mode	Shows the filter mode for the VLAN. This is only applicable for IGMPv3. • **Include**: Source-specific multicast address group • **Exclude**: Source-specific exclusive multicast address group
Port	Shows the forwarding port for the VLAN.
Source Address	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.

Limitations

There can be up to 1024 IGMP snooping forwarding table entries.



Item	Description
VLAN	Shows the ID of the VLAN the entry is for.
Group Address	Shows the associated multicast group address for streaming data for the VLAN.
Source Address	Shows the source address for streaming data for the VLAN.
Port	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.

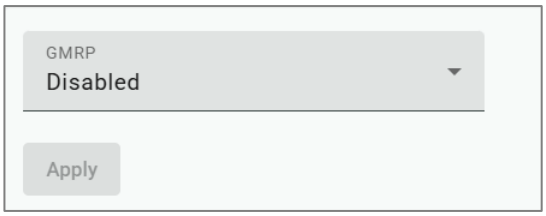
GMRP is now enabled.

GMRP

Menu Path: Layer 2 Switching > Multicast > GMRP

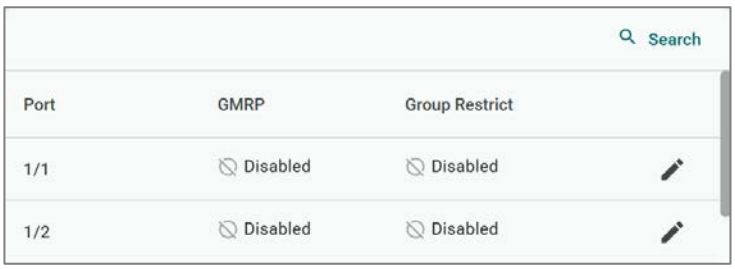
This page lets you configure the GMRP settings of your device.

GMRP Settings



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

GMRP Port List



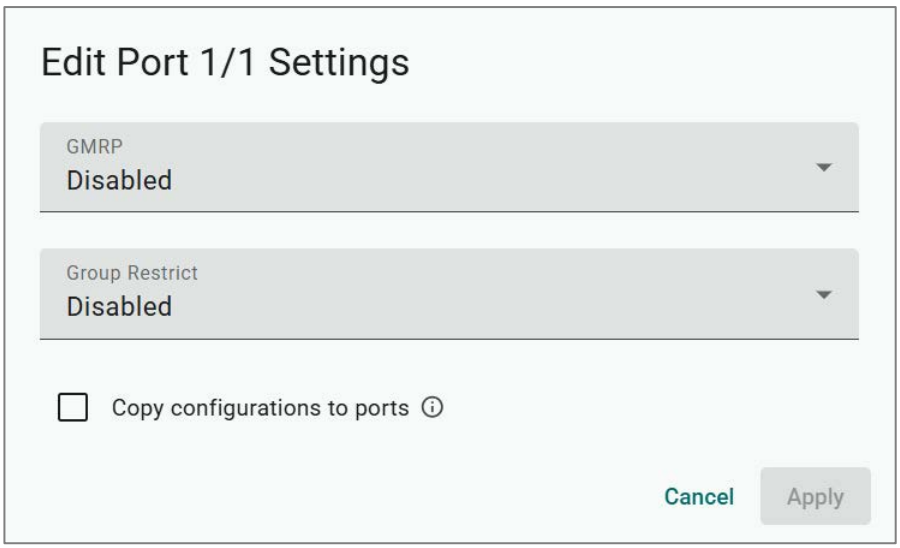
UI Setting	Description
Port	Shows the port number the entry is for.
GMRP	Shows whether GMRP is enabled for the port.
Group Restrict	Shows whether group restrict is enabled for the port.

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.



UI Setting	Description	Valid Range	Default Value
GMRP	Enable or disable GMRP for the port.	Enabled / Disabled	Disabled
Group Restrict	Enable or disable group restrict for the port.	Enabled / Disabled	Disabled
Copy configurations to ports	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.

Configuring Static Multicast Tables

1. Sign in to the device using administrator credentials.
2. Go to **Layer 2 Switching** > **Multicast** > **Static Multicast**
3. To add a static multicast entry, click the ***[Add]***.
4. Configure the following, and then click **Create**:

Option	Value
VLAN ID	Specify the VLAN ID

Option	Value
MAC Address	Specify the multicast MAC address. • IPv4 Multicast Range: 01:00:5E:00:00:00 to 01:00:5E:7F:FF (last 23 bits used for the multicast group address) • IPv6 Multicast Range: 33:33:00:00:00:00 to 33:33:FF:FF:FF (last 32 bits used for multicast group address)
Port	Choose one or more egress ports.

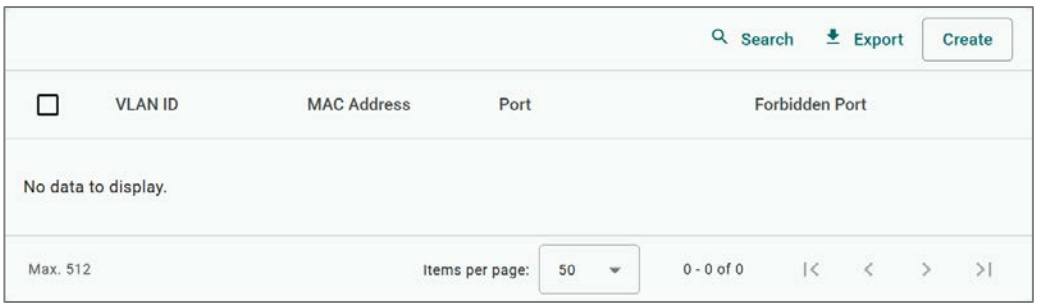
Static Multicast

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.



UI Setting	Description
VLAN ID	Shows the ID of the VLAN used for the multicast group entry.
MAC Address	Shows the MAC address for the multicast group entry.
Port	Shows the egress ports that multicast streams will forward to for the multicast group entry.

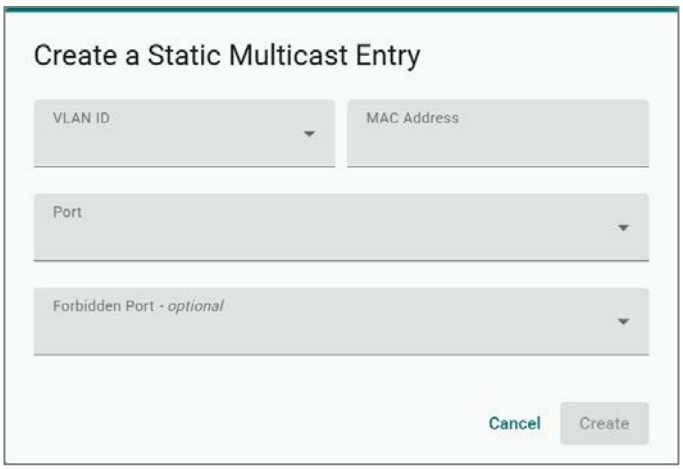
UI Setting	Description
Forbidden Port **(Only in Advanced Mode)**	Show the forbidden ports that packets will not be forwarded to for the multicast group entry.

Create a Static Multicast Entry

Menu Path: Layer 2 Switching > Multicast > Static Multicast

Clicking **Create** 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.



UI Setting	Description	Valid Range	Default Value
VLAN ID	Select a VLAN ID for the multicast entry.	Drop-down list of VLAN IDs	N/A
MAC Address	Specify the MAC address for the multicast entry.	Valid multicast MAC address	N/A
Port	Select the ports to use as egress ports for multicast streams to be forwarded to.	Drop-down list of ports	N/A
Forbidden Port **(Only in Advanced Mode)**	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 User Accounts for more information on user accounts.

Settings	Admin	Supervisor	User
Network Interface (for L3 models)	R/W	R/W	R

Network Interface - Settings

Menu Path: Network Interface - Settings

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

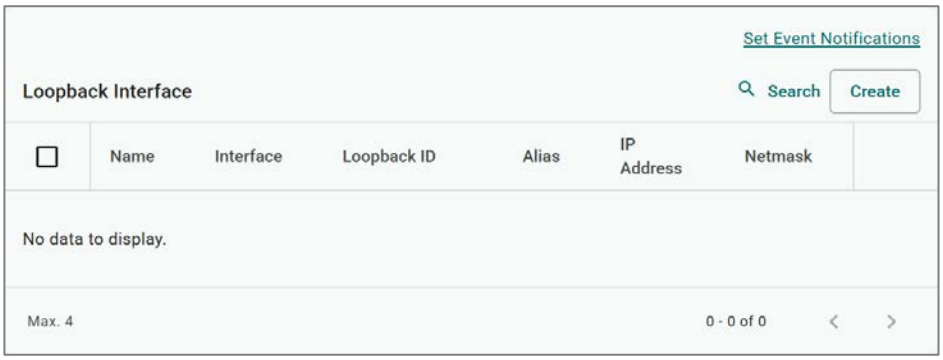
Limitations

You can create up to 4 loopback interfaces.

Limitations

You can create up to 256 VLAN interfaces.

Loopback Interface Table



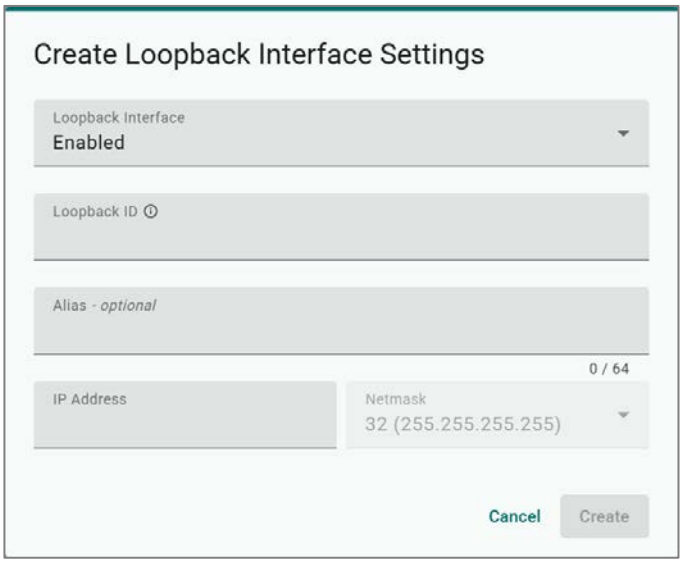
UI Setting	Description
Name	Shows the name of the loopback interface the entry is for.
Interface	Shows whether the loopback interface is enabled.
Loopback ID	Shows the ID for the loopback interface.
Alias	Shows the alias for the loopback interface.
IP Address	Shows the IP address for the loopback interface.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

Create Loopback Interface Settings

Menu Path: Network Interface - Settings

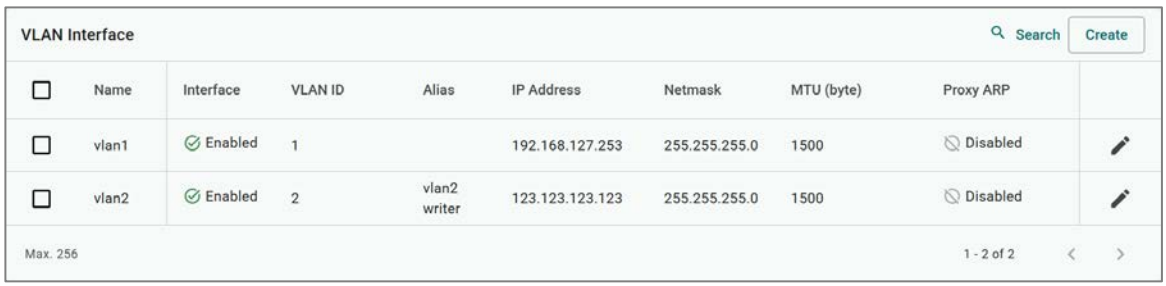
Clicking **Create** in the **Loopback Interface** table on the **Network Interface - Settings** page will open this dialog box. This dialog lets you create a loopback interface.

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



UI Setting	Description	Valid Range	Default Value
Loopback Interface	Enable or disable the loopback interface.	Enabled / Disabled	Enabled
Loopback ID	Specify the ID for the loopback interface.	1 to 10 characters	N/A
Alias	Specify an alias for the loopback interface.	0 to 64 characters	N/A
IP Address	Specify the IP address for the loopback interface.	Valid IP Address	N/A
Netmask	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



UI Setting	Description
Name	Shows the name of the VLAN interface the entry is for.
Interface	Shows whether the VLAN interface is enabled.
VLAN ID	Shows the ID for the VLAN interface.
Alias	Shows the alias for the VLAN interface.
IP Address	Shows the IP address for the VLAN interface.
Netmask	Shows the netmask for the VLAN interface.
MTU	Shows the MTU size in bytes for the VLAN interface.
Proxy ARP	Shows whether proxy ARP is enabled for the VLAN interface.

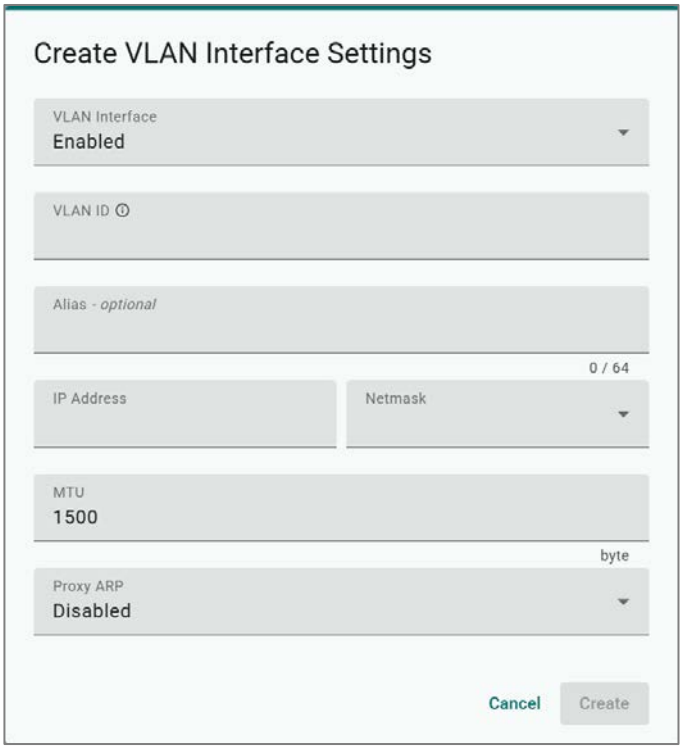
Create VLAN Interface Settings

Menu Path: Network Interface - Settings

Clicking **Create** 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



UI Setting	Description	Valid Range	Default Value
VLAN Interface	Enable or disable the VLAN interface.	Enabled / Disabled	Enabled
VLAN ID	Specify the ID for the VLAN interface.	1 to 4094	N/A
Alias	Specify an alias for the VLAN interface.	0 to 64	N/A
IP Address	Specify the IP address for the VLAN interface.	Valid IP Address	N/A
Netmask	Select a netmask for the VLAN interface.	Drop-down list of netmasks	N/A
MTU	Specify the MTU size in bytes to use for the VLAN interface.	1400 to 3000	1500
Proxy ARP	Enable or disable proxy ARP for the VLAN interface.	Enabled / Disabled	Disabled

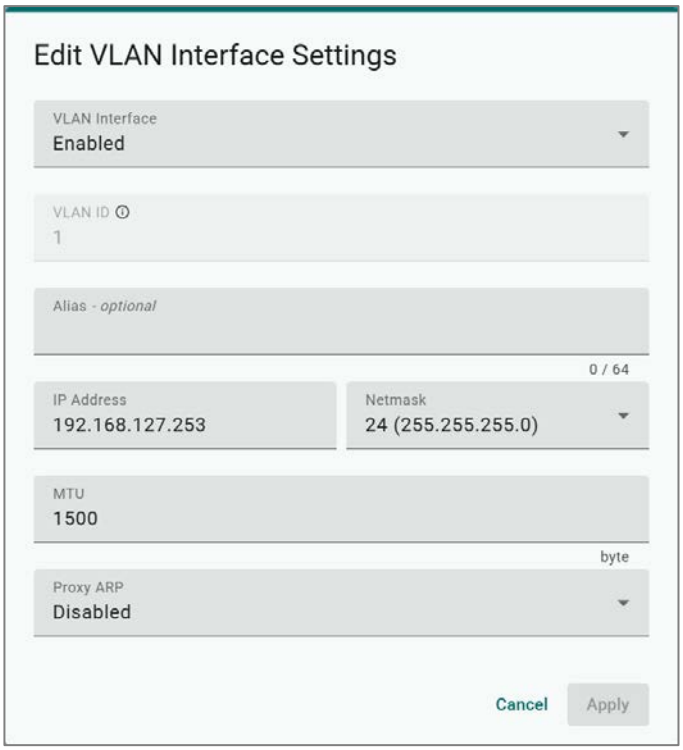
Edit VLAN Interface Settings

Menu Path: Network Interface - Settings

Clicking the **Edit (✎)** icon for an entry on the **Network Interface - Settings** page will open this dialog box. This dialog lets you edit the VLAN interface's settings.

Click **Apply** to save your changes.

Edit VLAN Interface Settings



UI Setting	Description	Valid Range	Default Value
VLAN Interface	Enable or disable the VLAN interface.	Enabled / Disabled	Enabled
VLAN ID	Shows the VLAN ID for the interface. This cannot be changed.	N/A	N/A
Alias	Specify an alias for the VLAN interface.	0 to 64 characters	N/A
IP Address	Specify the IP address for the VLAN interface.	Valid IP address	N/A

UI Setting	Description	Valid Range	Default Value
Netmask	Select a netmask for the VLAN interface.	Drop-down list of netmasks	N/A
MTU	Specify the MTU size in bytes to use for the VLAN interface.	1400 to 3000	1500
Proxy ARP	Enable or disable proxy ARP for the VLAN interface.	Enabled / Disabled	Disabled

Network Interface - Status

Menu Path: Network Interface - Status

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

Loopback Interface List



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

UI Setting	Description
Netmask	Shows the netmask for the loopback interface.

VLAN Interface List



UI Setting	Description
Name	Shows the name of the VLAN interface the entry is for.
Admin Status	Shows whether the VLAN interface is enabled.
Operation Status	Shows the operating status of the VLAN interface.
VLAN ID	Shows the ID for the VLAN interface.
IP Address	Shows the IP address for the VLAN interface.
Netmask	Shows the netmask for the VLAN interface.
MTU	Shows the MTU size in bytes for the VLAN interface.
Proxy ARP	Shows whether proxy ARP is enabled 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 User Accounts for more information on user accounts.

Settings	Admin	Supervisor	User
Layer 2 Redundancy			
Spanning Tree	R/W	R/W	R
Turbo Ring v2	R/W	R/W	R
Turbo Chain	R/W	R/W	R
MRP	R/W	R/W	R
Multiple Dual Homing	R/W	R/W	R
Multiple Network Coupling	R/W	R/W	R
IEC 62439-3 (for MDS-G4000-L2 models)			
PRP / HSR	R/W	R/W	R
Supervision Frame	R/W	R/W	R

Settings	Admin	Supervisor	User
Layer 3 Redundancy (for L3 models)			
VRRP	R/W	R/W	R
Tracking	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 Layer 2 Redundancy Protocols

Selecting the appropriate Layer 2 redundancy protocol for your network depends on several factors, including:

- The topology and size of your network
- The applications and services you are running
- Your availability and performance requirements

Here's a brief summary of each protocol to help you make an informed decision.

Category		RSTP	Turbo Ring v2	Turbo Chain	MRP
Specification Needs	Diameter	40 pcs	**V** 250 nodes per ring	**V** 250 nodes per chain	50 pcs
	Recovery Time		**V** Fast Ethernet: 20 ms Gigabit Ethernet: 50 ms	**V** Fast Ethernet: 20 ms Gigabit Ethernet: 50 ms	200 ms **Note** We recommend using fiber interfaces on 1G and 2.5G interfaces to ensure 200 ms recovery times; using copper for 1G and 2.5G interfaces may cause recovery times to exceed 200 ms due to cable limitations.
Application Needs	Multi-vendor Support	**V** Public Standard	Moxa proprietary	Moxa proprietary	Public standard
	Easy Deployment	Mesh	**V** Ring Topology	**V** Chain Topology	Ring topology
	Flexible Scalability		**O** Turbo Ring + Ring Coupling	**V** Directly connected to existing network without any changes.	MRP Ring + MRP Interconnection
Supported Versions		MX-NOS v1.x, v2.x, v3.x, v4.x, v5.x, v6.x	MX-NOS v1.x, v2.x, v3.x, v4.x, v5.x, v6.x	MX-NOS v1.x, v2.x, v3.x, v4.x, v5.x, v6.x	MX-NOS v4.x, v5.x, v6.x

V: Most appropriate

O: Partially applicable

About Scenarios for Turbo Ring

Large Semiconductor Network

A semiconductor factory plans to construct a new facility to increase chip production capacity for future electric vehicles. They require a large automated network (100+ switches) with redundant mechanisms to prevent unexpected downtime that could impact production lines. Additionally, their network must balance traffic across multiple links to prevent congestion and improve overall performance.

Analysis

1. This is a new project with no existing infrastructure.
2. A redundancy protocol is required and must support a network with at least 100 switches.
3. Link aggregation is needed to increase total throughput beyond what a single connection can sustain.

Solution: Turbo Ring v2

Turbo Ring v2 is suitable in situations where extremely fast failover times are required, such as in mission-critical industrial control systems. Turbo Ring v2 facilitates easy ring topology deployment. With Moxa Turbo Ring technology, networks can recover within 20 ms (Fast Ethernet/fiber) or 50ms (gigabit copper) on a network with up to 250 nodes.

Legacy Rapid Transit Network

A Phase II Metro project needs to build 15 new metro stations in an existing transit system, each requiring networking infrastructure. This project not only establishes its own system with a redundant topology but also ensures compatibility with the Phase I system. The Phase I system comprises a mesh topology with RSTP protocol, consisting of over 30 switches, with cabling that is outdated and no longer replaceable. Nevertheless, Phase II must be interconnected with Phase I without any modifications to the latter.

Analysis

1. This is a rebuilt project and it should be interconnected with RSTP topology.
2. Redundancy protocol is required and support 100+ switches network.

Solution: Turbo Chain

Turbo Chain is most suitable for this situation. One of the key advantages of Turbo Chain is its simplicity and ease of deployment. It can be directly interconnected to RSTP topology with any change on RSTP network.

Note:

The following two alternative solutions would also work in this scenario:

1. Turbo Ring v2 with Ring coupling to RSTP is also a alternate solution. This would depend on network physical deployment.
2. RSTP could be used to expand an existing RSTP network.

Inter-Consist Rail Network

A well-known railway vehicle manufacturer needs to plan a new on-board network, planning a ring network via Turbo Ring for multiple vehicles to form a consist. The consists also need to be interconnected with each other when connected as a train, and a redundant backup mechanism should be provided between consists.

Solution: Ring Coupling

Connection between Turbo Ring networks can be connected with ring coupling. This will allow consists with their own rings to be dynamically uncoupled and recoupled without reconfiguration.

About Spanning Tree

The Spanning Tree Protocol (STP) was designed to help construct a loop-free logical typology 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.

Note

This feature supports weaker authentication or encryption, and may not be secure over untrusted networks. Take appropriate security precautions.

About BPDU Guard

About BPDU Guard

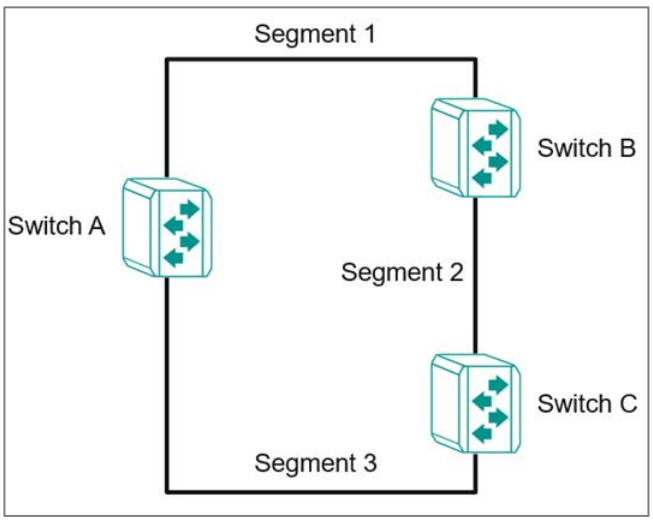
BDPUs (Bridge Protocol Data Units) are the network communication frames used in the STP (Spanning Tree Protocol). When two switches exchange messages, BDPUs are used to calculate the STP topology, and determine the network communication route. A BDPU filter is often used to screen sending or receiving BPDUs on a specific port of the switch.

BDPU 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.

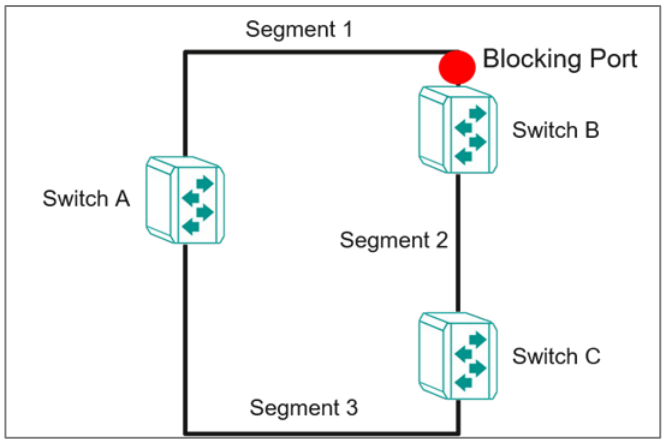
- **Root Guard:** Root Guard prevents a designated port role from changing to root port role on reception of superior information.
- **Loop Guard**: Loop Guard prevents temporary loops in a network caused by **non-designated ports** changing to the spanning-tree **forwarding** state due to a link failure 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

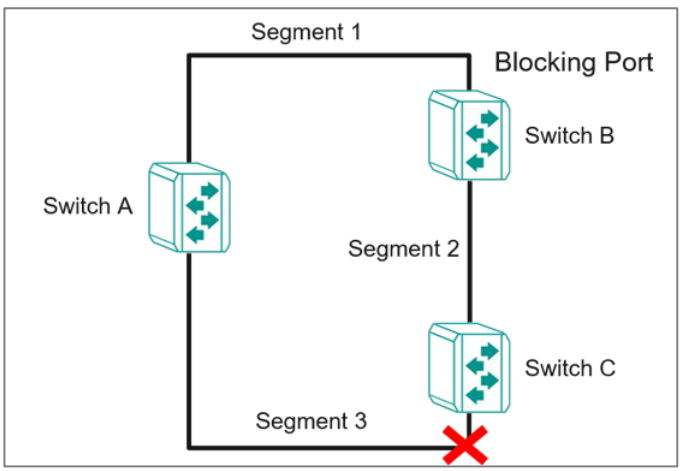
The figure below shows a network made up of three LANs separated by three bridges. Each segment uses at most two paths to communicate with the other segments. Since this configuration can give rise to loops, the network will overload if STP is not enabled.



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.

About SWIFT Mode

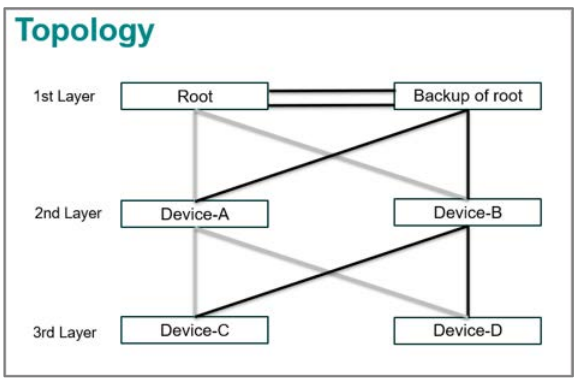
SWIFT Mode is a Moxa-proprietary feature that allows faster recovery times with standard RSTP protocols under certain circumstances. This is useful for scenarios requiring faster recovery times, but still needing standard protocols. Faster recovery times limit network impact during unexpected events.

SWIFT Mode supports two modes:

- Preempt Mode: Always restores the same RSTP root switch (fixed position) as soon as available.
- Non-Preempt Mode: Restores to any RSTP root switch is available, supporting sub-second recovery times.

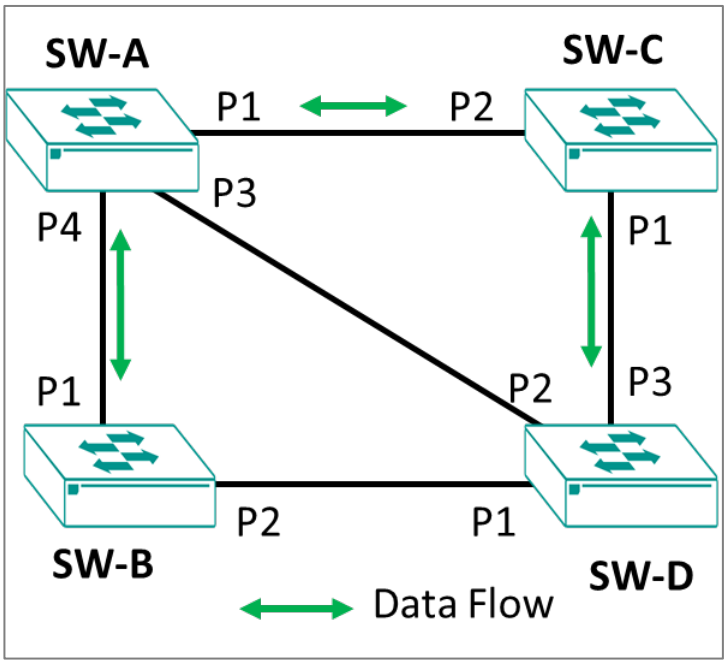
SWIFT Mode consistently supports sub-second recovery times if all of the following are true:

- **Preempt Mode** set to **Disabled**.
- Specific **Bridge Priority** settings:
    - Root/backup-root switches: 4096
    - Subsequent layers: consecutively lower priorities (higher numbers) at each layer (8092, 16184, etc.).
- Strict, hierarchical network topology:
    - Top layer:
        - Root and Backup switches must be connected to each other
    - In subsequent layers, each switch must have:
        - Exactly two connections to the preceding layer
        - No other connections to higher layers
        - No connections within thee same layer



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-D. 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 most 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

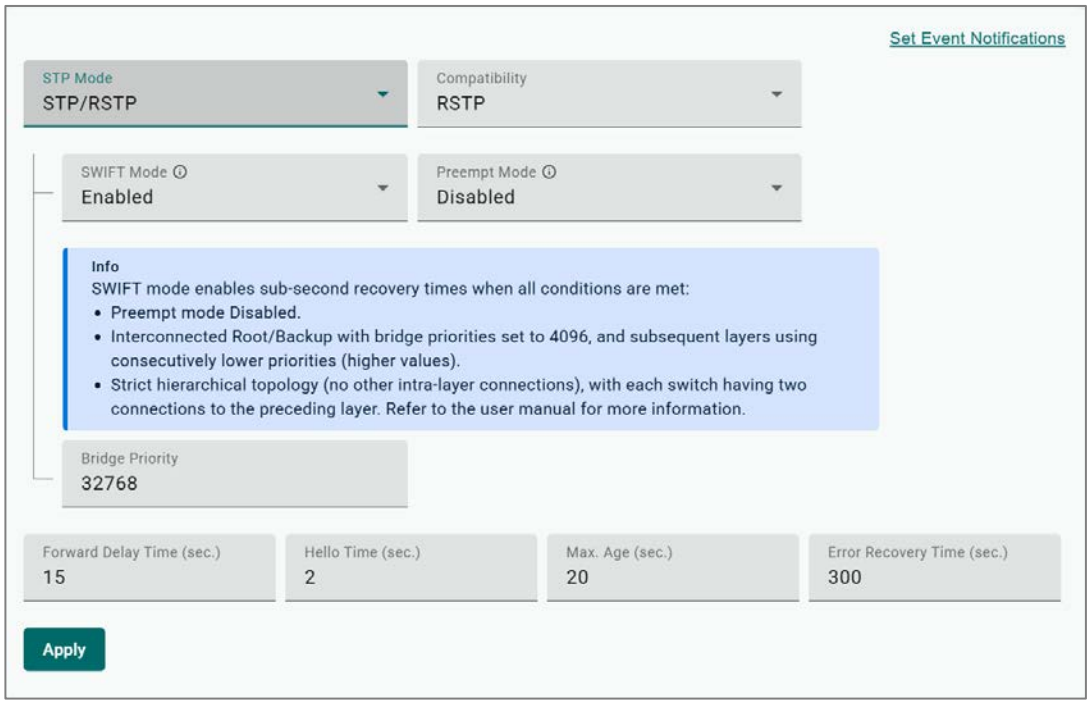
Spanning Tree - General

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.

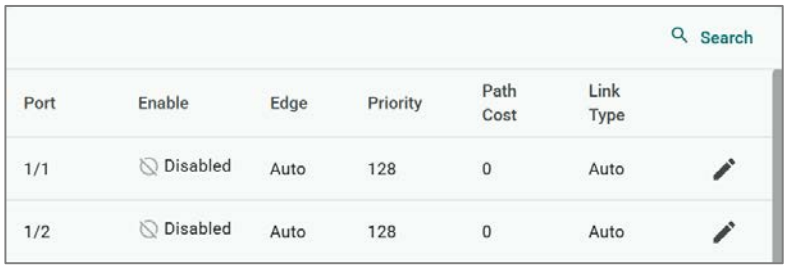


UI Setting	Description	Valid Range	Default Value
STP Mode	Specify the spanning tree protocol (STP) to use. **Note** MSTP and GVRP are both VLAN-related functions. When VLAN changes dynamically, MSTP needs to re-converge, which can make the system unstable due to running complex operations. When both 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.	Disabled / STP/RSTP/ MSTP	Disabled
Compatibility	Specify the compatibility mode to use.	STP / RSTP	RSTP

UI Setting	Description	Valid Range	Default Value
SWIFT Mode	Enable or disable SWIFT mode. **Note** These are the conditions required to use SWIFT mode: • Preempt Mode is Disabled • Interconnected Root/Backup with bridge priorities set to 4096, and subsequent layers using consecutively lower priorities (higher values) • Strict hierarchical topology (no other intra-layer connections), with each switch having two connections to the preceding layer	Enabled / Disabled	Enabled
Preempt Mode	Enable or disable preempt mode.	Disabled / Enabled	Disabled
Bridge Priority	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
Forward Delay Time	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
Hello Time	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
Max. Age	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
Error Recovery Time	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.



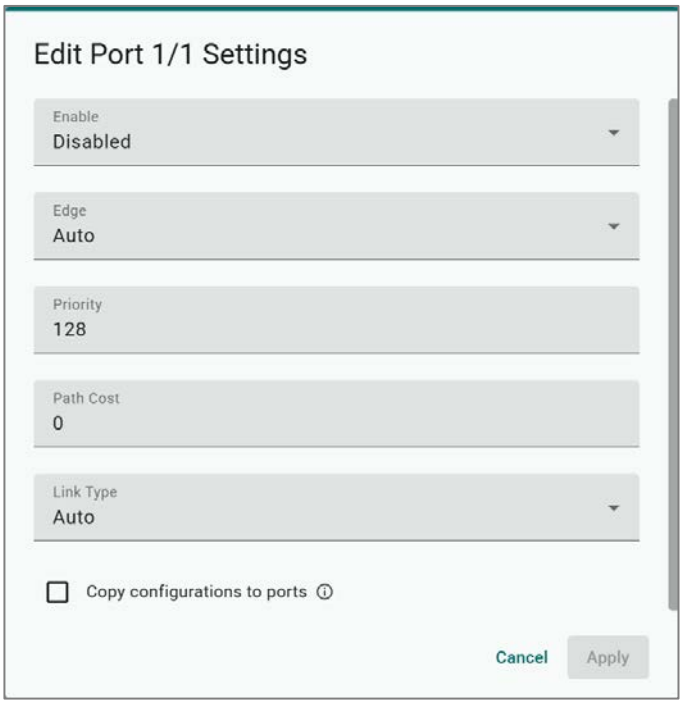
UI Setting	Description
Port	Shows the port number the entry is for.
Enable	Shows whether the spanning tree protocol is enabled for the port.
Edge	Shows the current edge port configuration for the port.
Priority	Show the bridge priority number for the port.
Path Cost	Show the path cost value for the port.
Link Type **(Only in Advanced Mode)**	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 a 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.

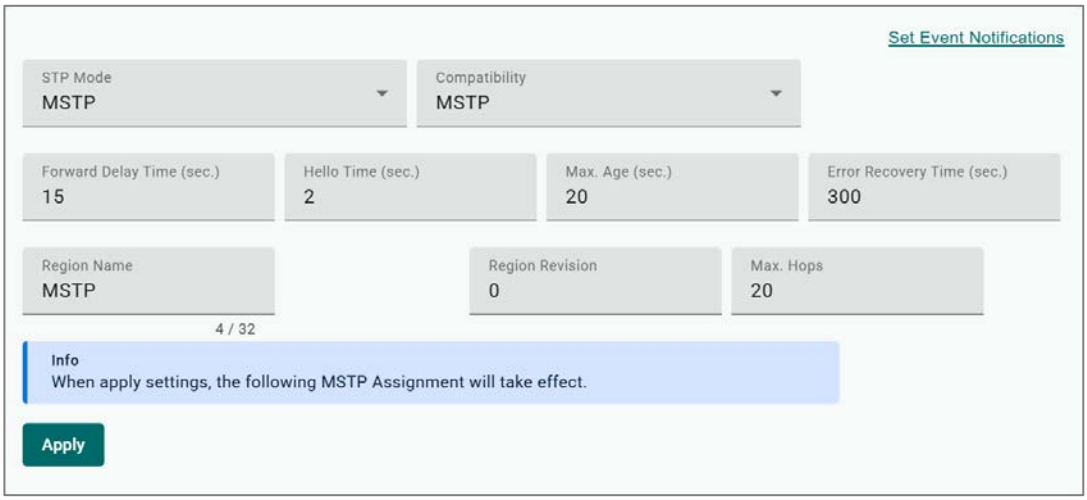


UI Setting	Description	Valid Range	Default Value
Enable	Enable or disable spanning tree protocol for the port.	Enabled / Disabled	Disabled
Edge	Select the edge port configuration for the port. • **Auto**: Auto-detect whether to configure the port as an edge port. • **Yes**: The port will be configured as an edge port. • **No**: The port will not be configured as an edge port.	Auto / Yes / No	Auto
Priority	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
Path Cost	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
Link Type **(Only in Advanced Mode)**	Select the link type for the port. • **Point-to-point**: Use this when the port is operating in full-duplex mode. • **Shared**: Use this when the port is operating in half-duplex mode. • **Auto**: Auto-detect which mode to use for the port.	Point-to-point / Shared / Auto	Auto

UI Setting	Description	Valid Range	Default Value
Copy configurations to ports	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.

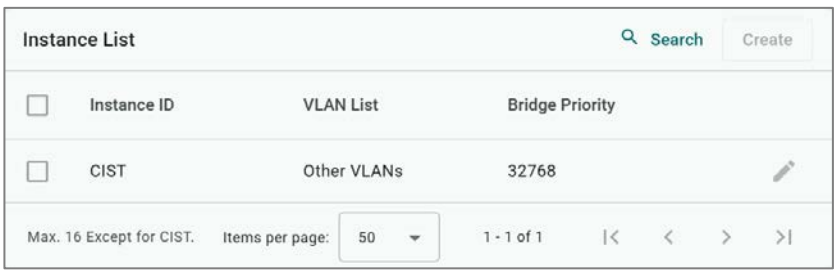


UI Setting	Description	Valid Range	Default Value
STP Mode	Specify the spanning tree protocol (STP) to use. **Note** MSTP and GVRP are both VLAN-related functions. When VLAN changes dynamically, MSTP needs to re-converge, which can make the system unstable due to running complex operations. When both 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.	Disabled / STP/RSTP/ MSTP	Disabled
Compatibility	Specify the compatibility mode to use.	RSTP / STP / MSTP	MSTP
Forward Delay Time	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

UI Setting	Description	Valid Range	Default Value
Hello Time	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
Max. Age	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
Error Recovery Time	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
Region Name	Specify the MSTP region name.	0 to 32 characters	MSTP
Region Revision	Specify the MSTP region revision.	0 to 65535	0
Max. Hops	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.



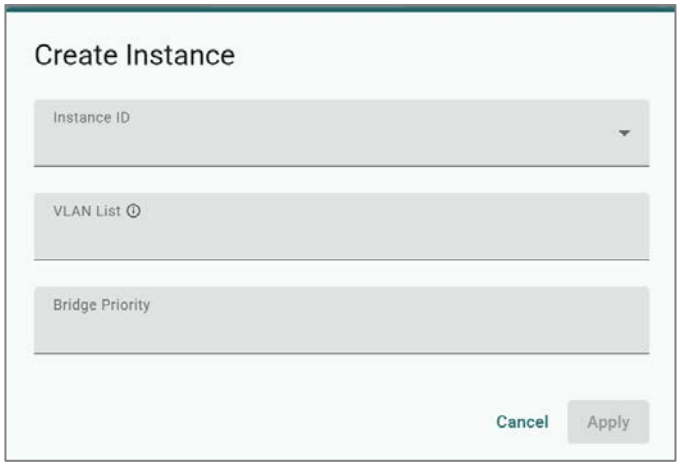
UI Setting	Description
Instance ID	Shows the of the instance the entry is for.
VLAN List	Show the VLAN list configured for the instance.
Bridge Priority	Show the bridge priority value for the instance.

Instance List - Create Instance

Menu Path: Redundancy > Spanning Tree - General

Clicking **Create** on the **Redundancy > Spanning Tree - General** page will open this dialog box. This dialog lets you create an MSTP instance.

Click **Create** to save your changes.



UI Setting	Description	Valid Range	Default Value
Instance ID	Select an ID for the instance.	Drop-down list of ID numbers.	N/A
VLAN List	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
Bridge Priority	Specify the bridge priority value for the instance as a multiple of 4096. Lower values have higher priority.	Multiples of 4096 from 0 to 61440	N/A

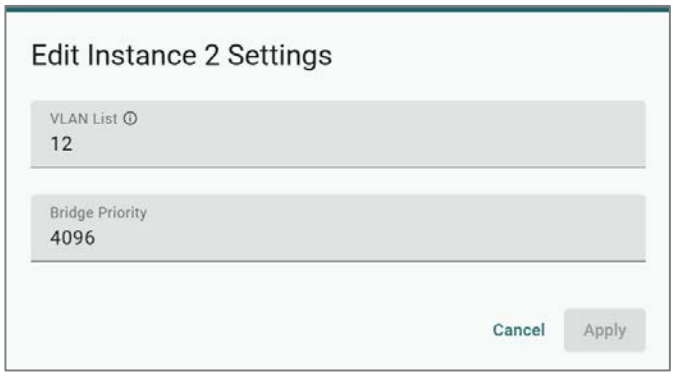
Instance List - Edit Settings

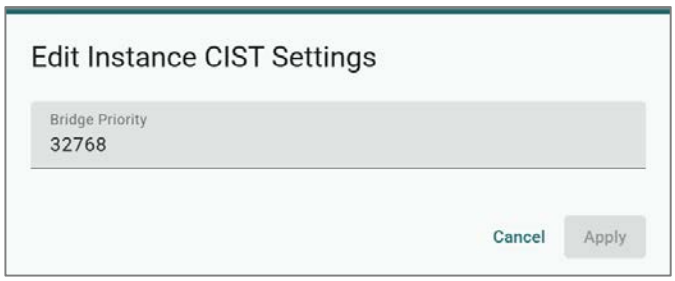
Menu Path: Redundancy > Spanning Tree - General

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.

The dialog shown will be different when editing the CIST instance.

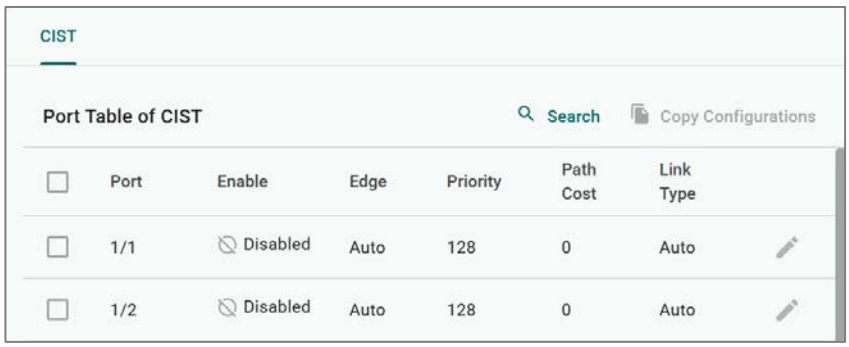




UI Setting	Description	Valid Range	Default Value
VLAN List	Specify the VLAN IDs to use for the instance. You can enter multiple VLAN IDs by separating them with commas or by using ranges (e.g., 2, 4-8, 10-13). **Note** This setting is not available for the CIST instance.	N/A	N/A
Bridge Priority	Specify the bridge priority value for the instance as a multiple of 4096. Lower values have higher priority.	Multiples of 4096 from 0 to 61440	32768 for CIST N/A for other instances

MSTP - 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.



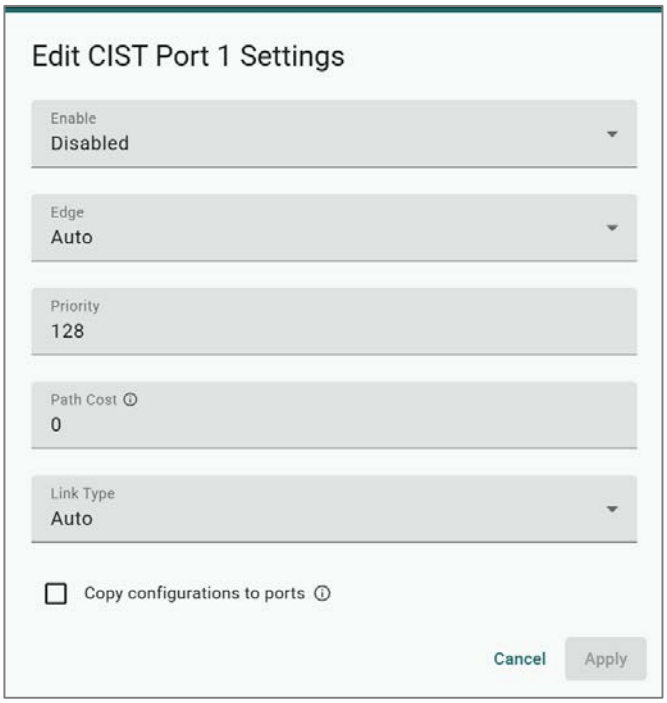
UI Setting	Description
Port	Shows the port number the entry is for.
Enable	Shows whether the spanning tree protocol is enabled for the port.
Edge	Shows the current edge port configuration for the port.
Priority	Show the bridge priority number for the port.
Path Cost	Show the path cost value for the port.
Link Type **(Only in Advanced Mode)**	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 a 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.



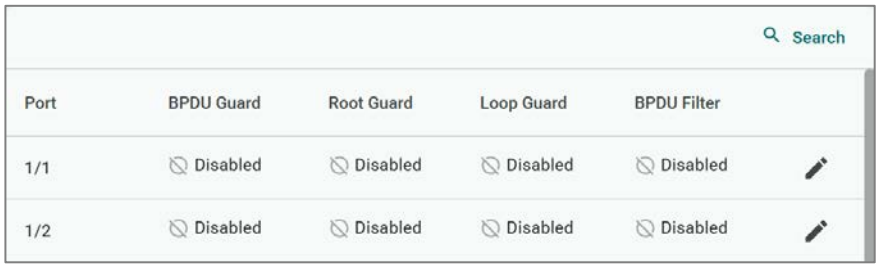
UI Setting	Description	Valid Range	Default Value
Enable	Enable or disable spanning tree protocol for the port.	Enabled / Disabled	Disabled
Edge	Select the edge port configuration for the port. • **Auto**: Auto-detect whether to configure the port as an edge port. • **Yes**: The port will be configured as an edge port. • **No**: The port will not be configured as an edge port.	Auto / Yes / No	Auto
Priority	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
Path Cost	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
Link Type **(Only in Advanced Mode)**	Select the link type for the port. • **Point-to-point**: Use this when the port is operating in full-duplex mode. • **Shared**: Use this when the port is operating in half-duplex mode. • **Auto**: Auto-detect which mode to use for the port.	Point-to-point / Shared / Auto	Auto

UI Setting	Description	Valid Range	Default Value
Copy configurations to ports	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.



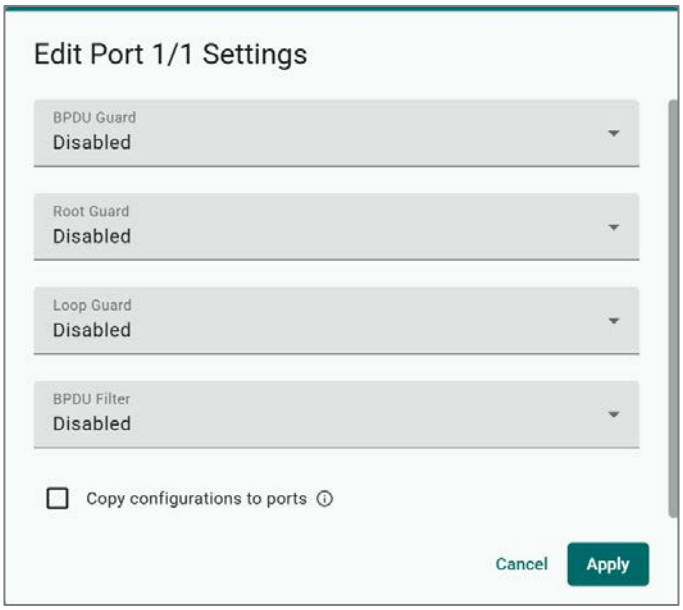
UI Setting	Description
Port	Shows the port number the entry is for.
BPDU Guard	Shows whether BPDU Guard is enabled for the port.
Root Guard (Only in Advanced Mode)	Shows whether Root Guard is enabled for the port.
Loop Guard (Only in Advanced Mode)	Shows whether Loop Guard is enabled for the port.
BPDU Filter	Shows whether the BPDU Filter is enabled for the port.

Spanning Tree 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.



UI Setting	Description	Valid Range	Default Value
BDPU Guard	Enable/disable BPDU Guard on the port.	Enabled / Disabled	Disabled
Root Guard **(Only in Advanced Mode)**	Enable/disable Root Guard on the port.	Enabled / Disabled	Disabled
Loop Guard **(Only in Advanced Mode)**	Enable/disable Loop Guard on the port.	Enabled / Disabled	Disabled
BDPU Filter	Enable/disable BPDU Filter on the port.	Enabled / Disabled	Disabled
Copy configurations to ports	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.



UI Setting	Description
Bridge ID	Shows the bridge ID.
Root Path Cost	Shows the root path cost.
Forward Delay Time	Shows the forward delay time in seconds.
Hello Time	Shows the hello time in seconds.
Max. Age	Shows the max. age time in seconds.

Bridge Information

If **STP Mode** is set to **STP/RSTP**, this display will appear.

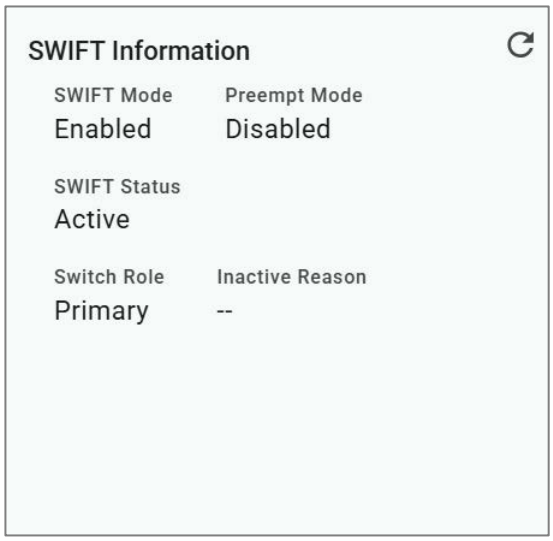


UI Setting	Description
Bridge ID	Shows the bridge ID.

UI Setting	Description
Running Protocol	Shows the current configured spanning tree protocol.
Forward Delay Time	Shows the forward delay time in seconds.
Hello Time	Shows the hello time in seconds.
Max. Age	Shows the max. age time in seconds.

SWIFT Information

If **STP Mode** is set to **STP/RSTP**, this display will appear.

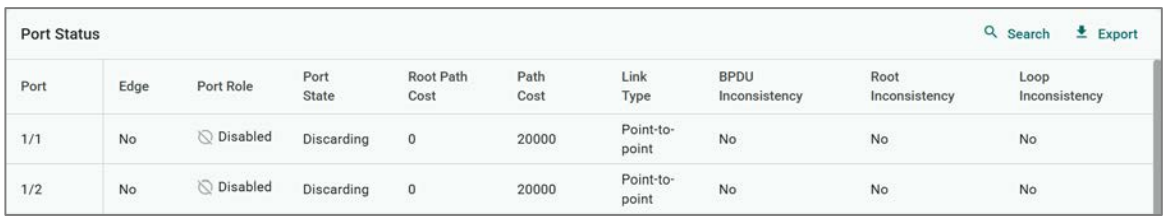


UI Setting	Description
SWIFT Mode	Shows whether SWIFT Mode is enabled or disabled.
Preempt Mode	Shows whether Preempt Mode is enabled or disabled.

UI Setting	Description
SWIFT Status	Shows whether all conditions for SWIFT mode are met for SWIFT mode to be active. **Note** These are the conditions required to use SWIFT mode: • Preempt Mode is Disabled • Interconnected Root/Backup with bridge priorities set to 4096, and subsequent layers using consecutively lower priorities (higher values) • Strict hierarchical topology (no other intra-layer connections), with each switch having two connections to the preceding layer
Switch Role	Shows the role of the switch in SWIFT Mode topology.
Inactive Reason	Shows the conditions not met for SWIFT mode to be active.

Spanning Tree - Port Status

If **STP Mode** is set to **STP/RSTP**, the following table will appear.



UI Setting	Description
Port	Shows the port number the entry is for.
Edge	Shows whether this port is connected to an edge device.

UI Setting	Description
Port Role	Shows the role for the port. • **Root**: The port is connected directly or indirectly to the root device. • **Designated**: The port is designated if it can send the best BPDU on the segment to which it is connected. • **Alternate**: The alternate port receives more useful BPDU from another bridge and is a blocked port. • **Backup**: The backup port receives more useful BPDU from the same bridge and is a blocked port. • **Disabled**: The port is disabled.
Port State	Show the port state. • **Forwarding**: Traffic can be forwarded through this port. • **Blocked**: Traffic will be blocked. • **Disabled**: The port is disabled.
Root Path Cost	Shows the total path cost to the root bridge for the port.
Path Cost	Shows the path cost for the port.
Link Type	Show the link type for the port. • **Edge Port**: The port is connected to an edge device. • **Point-to-point**: The port is connected to another bridge and is full duplex. • **Shared**: The port is connected to another bridge and is half duplex.
BPDU Inconsistency	Shows whether BPDU inconsistency was detected for the port.
Root Inconsistency **(Only in Advanced Mode)**	Shows whether root inconsistency was detected for the port.
Loop Inconsistency **(Only in Advanced Mode)**	Shows whether loop inconsistency was detected for the port.

General Information

If **STP Mode** is set to **MSTP**, this display will appear.

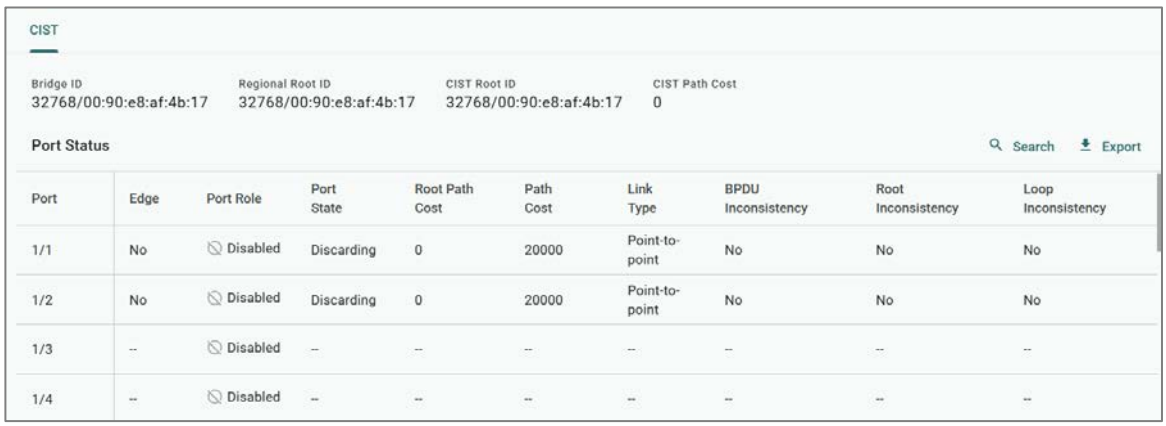


UI Setting	Description
Running Protocol	Shows the current configured spanning tree protocol.
Forward Delay Time	Shows the forward delay time in seconds.
Hello Time	Shows the hello time in seconds.
Max. Age	Shows the max. age time in seconds.

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 Instance

When viewing the CIST instance, this information will appear:

UI Setting	Description
Bridge ID	Shows the bridge ID for the CIST instance.
Regional Root ID	Shows the regional root ID for the CIST instance.
CIST Root ID	Shows the bridge ID for the CIST instance.
CIST Path Cost	Shows the bridge ID for the CIST instance.

When viewing an instance other than the CIST instance, this information will appear:

UI Setting	Description
Bridge ID	Shows the bridge ID for the instance.
VLAN List	Shows the VLAN IDs for the instance.
Designated Root ID	Shows the designated root ID for the instance.
Root Path Cost	Shows the root path cost for the instance.

Port Status

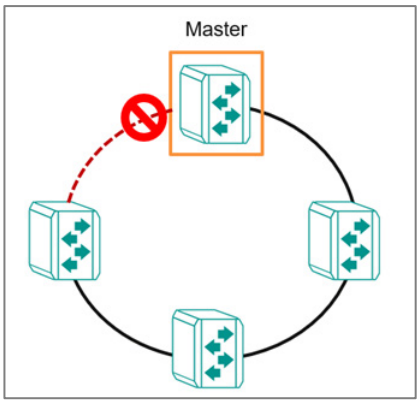
UI Setting	Description
Port	Shows the port number the entry is for.
Edge	Shows whether this port is connected to an edge device.
Port Role	Shows the role for the port. • **Root**: The port is connected directly or indirectly to the root device. • **Designated**: The port is designated if it can send the best BPDU on the segment to which it is connected. • **Alternate**: The alternate port receives more useful BPDU from another bridge and is a blocked port. • **Backup**: The backup port receives more useful BPDU from the same bridge and is a blocked port. • **Disabled**: MSTP is disabled for the port.
Port State	Show the port state. • **Forwarding**: Traffic can be forwarded through this port. • **Blocked**: Traffic will be blocked. • **Disabled**: The port is disabled.
Root Path Cost	Shows the total path cost to the root bridge for the port.
Path Cost	Shows the path cost for the port.
Link Type	Show the link type for the port. • **Edge Port**: The port is connected to an edge device. • **Point-to-point**: The port is connected to another bridge and is full duplex. • **Shared**: The port is connected to another bridge and is half duplex.
BPDU Inconsistency	Shows whether BPDU Guard detected the port receiving a BPDU.

UI Setting	Description
Root Inconsistency	Shows whether Root Guard detected the port changing to a root port.
Loop Inconsistency	Shows whether Loop Guard detected a loop for the port.

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.

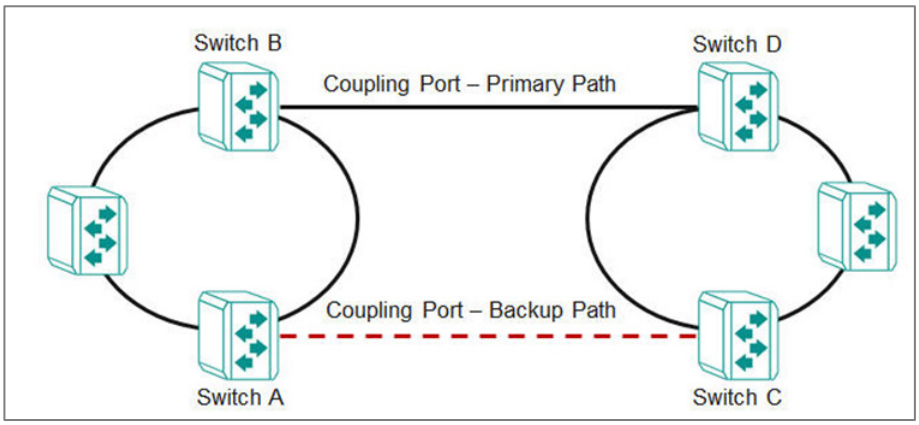
Note

This feature supports weaker authentication or encryption, and may not be secure over untrusted networks. Take appropriate security precautions.

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

There can be only one coupling (primary + backup) per ring pair.

Note

Ring coupling port support port channel.

Note

Please note check your network configuration after downgrading MX-NOS version from v6.0 to the version before as ring coupling port will be directly changed to port 5 or port 2/1(depends on product series). Make sure the conflict port configurations, for example port 5 or port 2/1 has been configured for other use.

About Ring Protection Actions

Ring Protection is a mechanism designed to protect a Turbo Ring network from being affected by incorrect redundant port configurations or physical miswiring.

Typical issues include:

- Redundant links accidentally connected to normal ports, causing Layer 2 loops in the network.
- Disturbance or flooding of control packets from misconfigured devices or malicious attackers.

This Moxa-proprietary mechanism provides the following protection actions:

- **No action**: Allow all redundant protocol packets to pass through normal ports.
- **Drop**: Drop unexpected or excessive redundant protocol packets on normal ports.
- **Disable port**: Disable ports that receive unexpected or excessive redundant protocol packets.

Note

This feature handles two types of redundant packets differently:

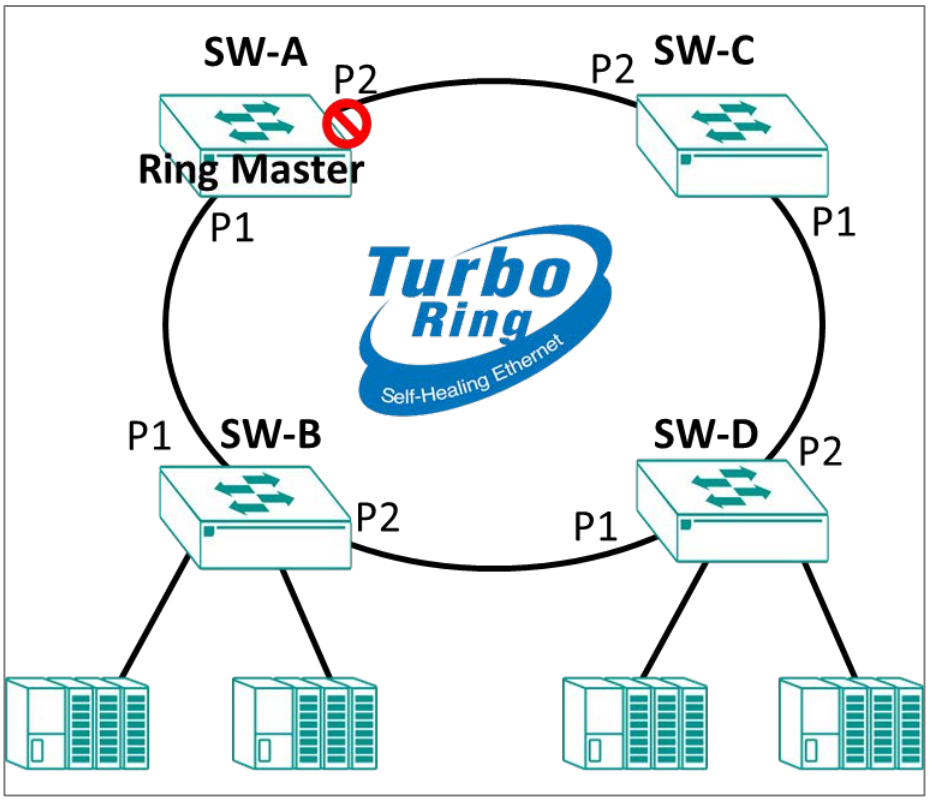
- Ordinary Redundant Protocol Packets
- Topology Change-related Redundant Protocol Packets

Ordinary Redundant Protocol Packets always trigger specified protection actions. Topology Change-related packets only trigger actions when deemed excessive. This ensures normal, short-lived topology changes do not trigger unnecessary protection events.

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 with administrator credentials.
2. Go to **Redundancy** > **Layer 2 Redundancy** > **Turbo Ring V2**, and then click **Settings**.
3. Set **Turbo Ring V2** to **Enabled**.

   Ring Protection Action appears.

4. Set **Ring Protection Action** to **Drop** to drop unexpected or excessive redundancy packets.
5. Select **Apply** to save your changes.
6. Under Ring Settings, next to **Ring 1**, select **[Edit]**.

   The Ring 1 Settings screen appears.

7. Configure all of the following:

Option	Value
Status	**Enabled**
Master	**Enabled**

Option	Value
Ring Port 1	**1 / 1**
Ring Port 2	**1 / 2**

Setting **Master** on multiple devices (or no devices) will have the following effects:

Master Setting	Result
Multiple devices set to Enabled	Ring election based on MAC addresses of **Enabled** devices
No devices set to Enabled	Ring election based on MAC addresses of all devices
Single device set to Enabled	**Enabled** device always master, failure of **Enabled** device results in ring election

8. Select **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 with administrator credentials.
2. Go to **Redundancy** > **Layer 2 Redundancy** > **Turbo Ring V2**, and then click **Settings**.
3. Set **Turbo Ring V2** to **Enabled**.

   Ring Protection Action appears.
4. Set **Ring Protection Action** to **Drop** to drop unexpected or excessive redundancy packets.
5. Select **Apply** to save your changes.
6. Under Ring Settings, next to **Ring 1**, select **[Edit]**.

The Ring 1 Settings screen appears.

7. Configure all of the following:

Option	Value
Status	**Enabled**
Master	**Disabled**
Ring Port 1	**1 / 1**
Ring Port 2	**1 / 2**

Setting **Master** on multiple devices (or no devices) will have the following effects:

Master Setting	Result
Multiple devices set to Enabled	Ring election based on MAC addresses of **Enabled** devices
No devices set to Enabled	Ring election based on MAC addresses of all devices
Single device set to Enabled	**Enabled** device always master, failure of **Enabled** device results in ring election

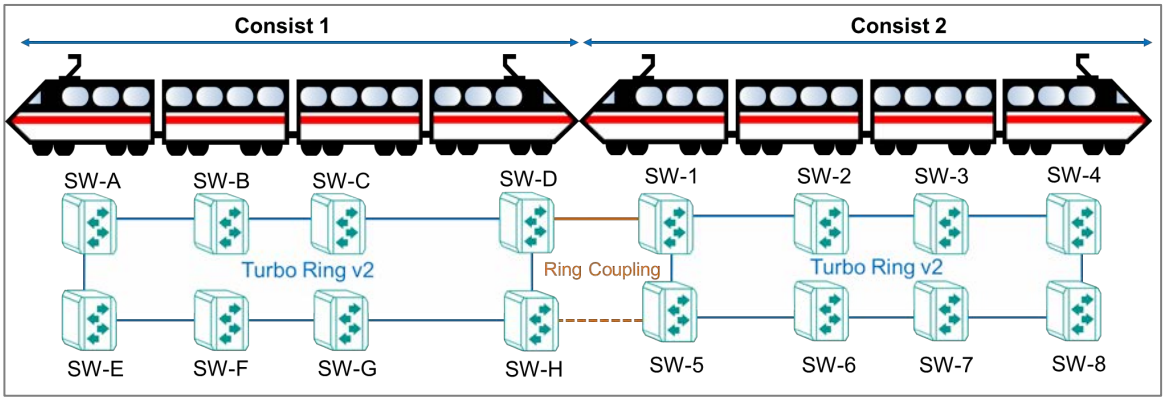
8. Select **Apply** to save your changes.

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 with administrator credentials.
2. Go to **Redundancy** > **Layer 2 Redundancy** > **Turbo Ring V2**, and then select **Settings**.
3. Set **Turbo Ring V2** to **Enabled**.

   Ring Protection Action appears.

4. Set **Ring Protection Action** to **Drop** to drop unexpected or excessive redundancy packets.
5. Select **Apply** to save your changes.
6. Under Ring Settings, next to **Ring 1**, select **[Edit]**.

The Ring 1 Settings screen appears.

7. Configure all of the following:

Option	Value
Status	**Enabled**
Master	**Enabled**
Ring Port 1	**1 / 1**
Ring Port 2	**1 / 2**

Setting **Master** on multiple devices (or no devices) will have the following effects:

Master Setting	Result
Multiple devices set to Enabled	Ring election based on MAC addresses of **Enabled** devices
No devices set to Enabled	Ring election based on MAC addresses of all devices
Single device set to Enabled	**Enabled** device always master, failure of **Enabled** device results in ring election

8. Select **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 with administrator credentials.
2. Go to **Redundancy** > **Layer 2 Redundancy** > **Turbo Ring V2**, and then click **Settings**.
3. Set **Turbo Ring V2** to **Enabled**.

Ring Protection Action appears.

4. Set **Ring Protection Action** to **Drop** to drop unexpected or excessive redundancy packets.
5. Select **Apply** to save your changes.
6. Under Ring Settings, next to **Ring 1**, select **[Edit]**.

The Ring 1 Settings screen appears.

7. Configure all of the following:

Option	Value
Status	**Enabled**
Master	**Disabled**
Ring Port 1	**1 / 1**
Ring Port 2	**1 / 2**

Setting **Master** on multiple devices (or no devices) will have the following effects:

Master Setting	Result
Multiple devices set to Enabled	Ring election based on MAC addresses of **Enabled** devices
No devices set to Enabled	Ring election based on MAC addresses of all devices
Single device set to Enabled	**Enabled** device always master, failure of **Enabled** device results in ring election

8. Select **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 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. 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:

1. Sign in to the device with administrator credentials.
2. Go to **Redundancy** > **Layer 2 Redundancy** > **Turbo Ring V2**, and then select **Settings**.
3. Under Ring Coupling Settings, select **[Edit]**.

   The Ring Coupling Settings screen appears.
4. Configure all of the following:

Option	Value
Status	**Enabled**
Coupling Mode	**Coupling Primary Path**
Coupling Port	**1/5**

5. Select **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. 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 with administrator credentials.
2. Go to **Redundancy** > **Layer 2 Redundancy** > **Turbo Ring V2**, and then select **Settings**.
3. Under Ring Coupling Settings, select **[Edit]**.

   The Ring Coupling Settings screen appears.
4. Configure all of the following:

Option	Value
Status	**Enabled**
Coupling Mode	**Coupling Backup Path**
Coupling Port	**1 / 5**

5. Select **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

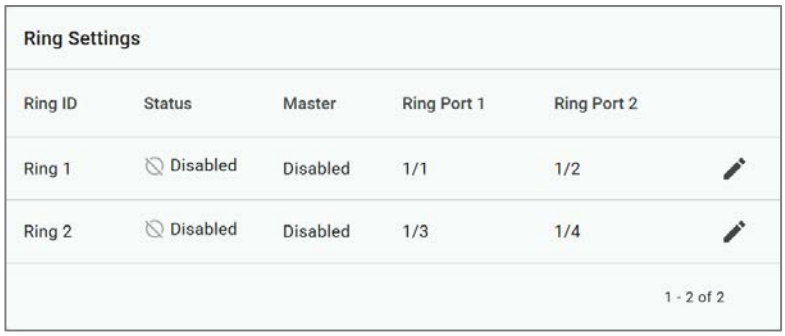
This page lets you configure the Turbo Ring V2 settings.

Turbo Ring V2 Settings



UI Setting	Description	Valid Range	Default Value
Turbo Ring V2	Enable or disable Turbo Ring V2 for the device.	Enabled / Disabled	Disabled
Ring Protection Action **(If Turbo Ring V2 is Enabled)**	Select the action to take when redundant protocol packets are detected on normal ports. • **No action:** Allow all redundant protocol packets pass through normal ports. • **Drop:** Drop redundant protocol packet on normal ports. • **Disable port:** Disable ports that received redundant protocol packets.	No action / Drop / Disable port	No action
Release Interval **(If Ring Protection Action is Disable port)**	Specify the release interval in minutes to wait after disabling a port before the port is re-enabled.	0 to 10800 min.	60

Ring Settings



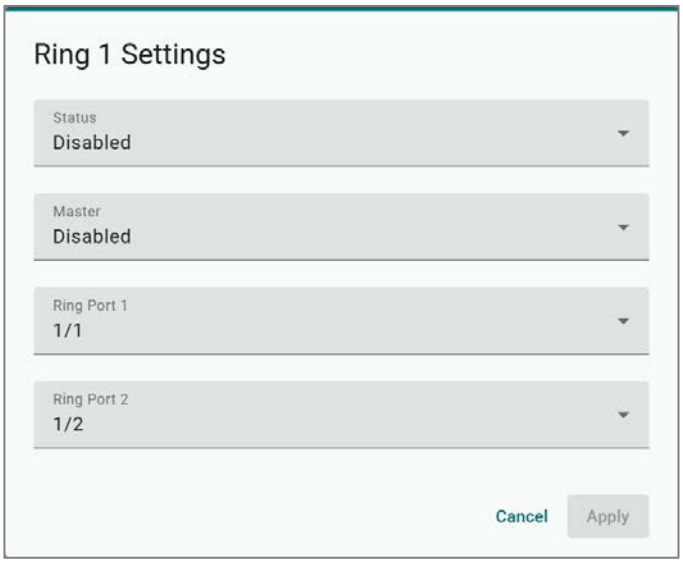
UI Setting	Description
Ring ID	Shows the ID of the ring the entry is for.
Status	Shows whether Turbo Ring V2 is enabled for the ring.
Master	Shows whether the device is designated as the master for the ring.
Ring Port 1	Shows which port will act as ring port 1. If this device is designated as the master for the ring, this will be the primary ring connection.
Ring Port 2	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

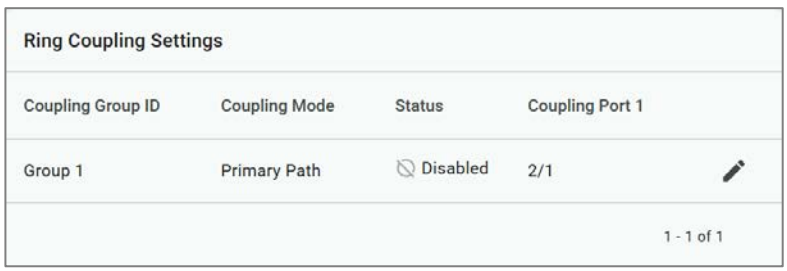
Clicking the **Edit (✎)** icon for a ring on the **Redundancy > Turbo Ring V2 - Settings** page will open this dialog box. This dialog lets you edit the Turbo Ring V2 settings for the ring.

Click **Apply** to save your changes.



UI Setting	Description	Valid Range	Default Value
Status	Enable or disable Turbo Ring V2 for the ring.	Enabled / Disabled	Disabled
Master	Enable or disable whether the device will be designated as the master for the ring.	Enabled / Disabled	Disabled
Ring Port 1	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
Ring Port 2	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



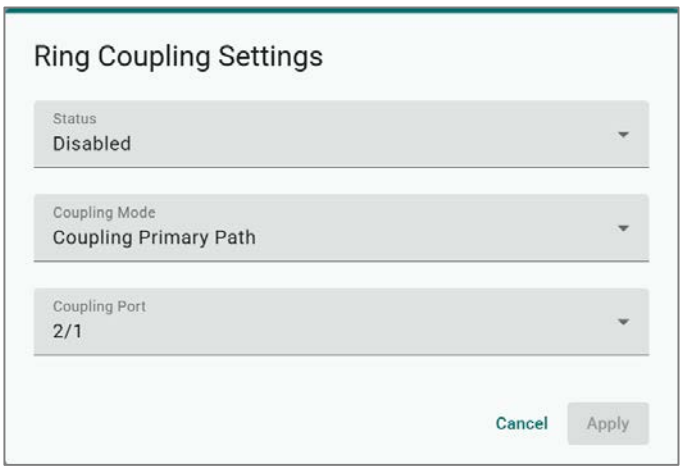
UI Setting	Description
Coupling Group ID	Shows the ID of the coupling group the entry is for.
Coupling Mode	Shows which coupling mode the entry is for.
Status	Shows whether ring coupling is enabled or disabled.
Coupling Port	Shows the port used for ring coupling.

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.



UI Setting	Description	Valid Range	Default Value
Status	Enable or disable ring coupling for the device.	Enabled / Disabled	Disabled
Coupling Mode	Specify whether this device will be designated as primary or backup path for ring coupling.	Coupling Primary Path / Coupling Backup Path	Coupling Primary Path
Coupling Port	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



UI Setting	Description
Ring ID	Shows the ID of the ring the entry is for.
Master ID	Shows the MAC address of the ring master.
Status	Shows the status of the ring. • **Healthy**: The ring and the ports are working properly. • **Break**: One or more rings are currently broken. • **Disabled**: The ring is disabled.
Role	Shows whether the device is configured as a master or slave for the ring.
Ring Port 1	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.
Ring Port 2	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

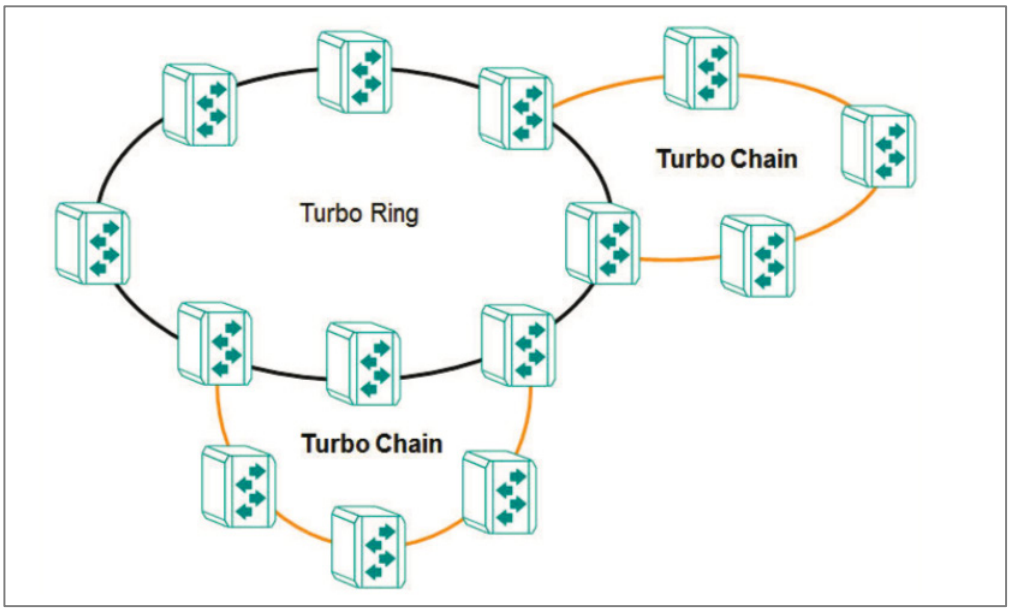


UI Setting	Description
Coupling Mode	Shows whether the device is the primary or backup path for ring coupling.
Coupling Port Status	Shows the status of the port used for ring coupling.

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.

Note

This feature supports weaker authentication or encryption, and may not be secure over untrusted networks. Take appropriate security precautions.

About Chain Protection Actions

Chain Protection is a mechanism designed to protect a Turbo Chain network from being affected by incorrect redundant port configurations or physical miswiring.

Typical issues include:

- Redundant links accidentally connected to normal ports, causing Layer 2 loops in the network.
- Disturbance or flooding of control packets from misconfigured devices or malicious attackers.

This Moxa-proprietary mechanism provides the following protection actions:

- **No action**: Allow all redundant protocol packets to pass through normal ports.
- **Drop**: Drop unexpected or excessive redundant protocol packets on normal ports.
- **Disable port**: Disable ports that receive unexpected or excessive redundant protocol packets.

Note

This feature handles two types of redundant packets differently:

- Ordinary Redundant Protocol Packets
- Topology Change-related Redundant Protocol Packets

Ordinary Redundant Protocol Packets always trigger specified protection actions. Topology Change-related packets only trigger actions when deemed excessive. This ensures normal, short-lived topology changes do not trigger unnecessary protection events.

Example: Configuring Turbo Chain

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 select **Settings**.
3. Set **Turbo Chain** to **Enabled**.
4. For **Chain Protection Action**, specify one of the following:

Option	Description
No action	Allows redundant packets protocol packets to pass through ordinary ports.
Drop	Drops unexpected or excessive redundant protocol packets on ordinary ports.
Disable port	Disables ports that receive unexpected or excessive redundant protocol packets.

5. 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.
6. Specify the following Ports based on the **Chain Role**:

Head Chain Role Option	Port Value
Tail Port	**2/1**
Member Port	**2/2**

Member Chain Role Option	
Member Port 1	**2 / 1**
Member Port 2	**2 / 2**

Tail Chain Role Option	
Member Port 1	**2 / 1**
Member Port 2	**2 / 2**

7. Select **Apply** to save changes.
8. 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 for your device.

Turbo Chain Settings



UI Setting	Description	Valid Range	Default Value
Turbo Chain	Enable/disable Turbo Chain for your device.	Enabled / Disabled	Disabled
Chain Protection Action	Select the action to take when redundant protocol packets are detected on normal ports.	No action / Drop / Disable port	No action
Release Interval **(If Chain Protection Action is Disable port)**	Specify the release interval in minutes to wait after disabling a port before the port is re-enabled.	0 to 10800	60
Chain Role	Specify the chain role for your device.	Head / Member / Tail	Member
Head Port **(If Chain Role is Head)**	Specify the port to use as the head port.	Drop-down list of ports	First port of the device
Tail Port **(If Chain Role is Tail)**	Specify the port to use as the tail port.	Drop-down list of ports	First port of the device
Member Port **(If Chain Role is Head or Tail)**	Specify the port to use as the member port.	Drop-down list of ports	Second port of the device

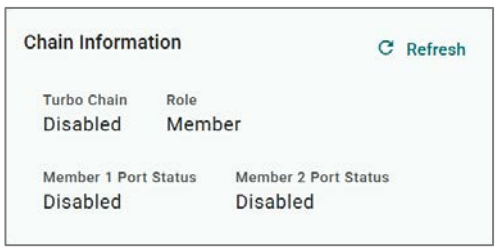
UI Setting	Description	Valid Range	Default Value
Member Port 1 **(If Chain Role is Member)**	Specify the port to use as member port 1.	Drop-down list of ports	First port of the device
Member Port 2 **(If Chain Role is Member)**	Specify the port to use as member port 2.	Drop-down list of ports	Second port of the device

Turbo Chain - Status

Menu Path: Redundancy > Turbo Chain - Status

This page lets you view the Turbo Chain status of your device.

Chain Information



UI Setting	Description
Turbo Chain	Shows whether Turbo Chain is enabled for your device.
Role	Shows the chain role of your device.
Member Port 1 Status	Shows the status of member port 1.
Member Port 2 Status	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 either:

- **LC-mode (Link check mode)**: The MRP interconnection manager can observe the interconnection topology by reacting directly on interconnection port link change notification messages
- **RC-mode (Ring check 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.

> **Note**
>
> This feature supports weaker authentication or encryption, and may not be secure over untrusted networks. Take appropriate security precautions.

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
Role	**Ring Manager**
VLAN ID	Specify the VLAN ID for the ring
Domain UUID	Choose either **Default** or **PROFITNET (Siemens)** according to your network configuration

Ring Manager Option	Ring Manager Value
React on Link Change	It is recommended to set this to **Enabled**. 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.
Ring Port 1	Specify the first redundant ring port
Ring Port 2	Specify the second redundant ring port

Ring Client Option	Ring Client Value
Role	**Ring Client**
VLAN ID	Specify the VLAN ID for the ring
Domain UUID	Choose either **Default** or **PROFITNET (Siemens)** according to your network configuration
Ring Port 1	Specify the first redundant ring port
Ring Port 2	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.

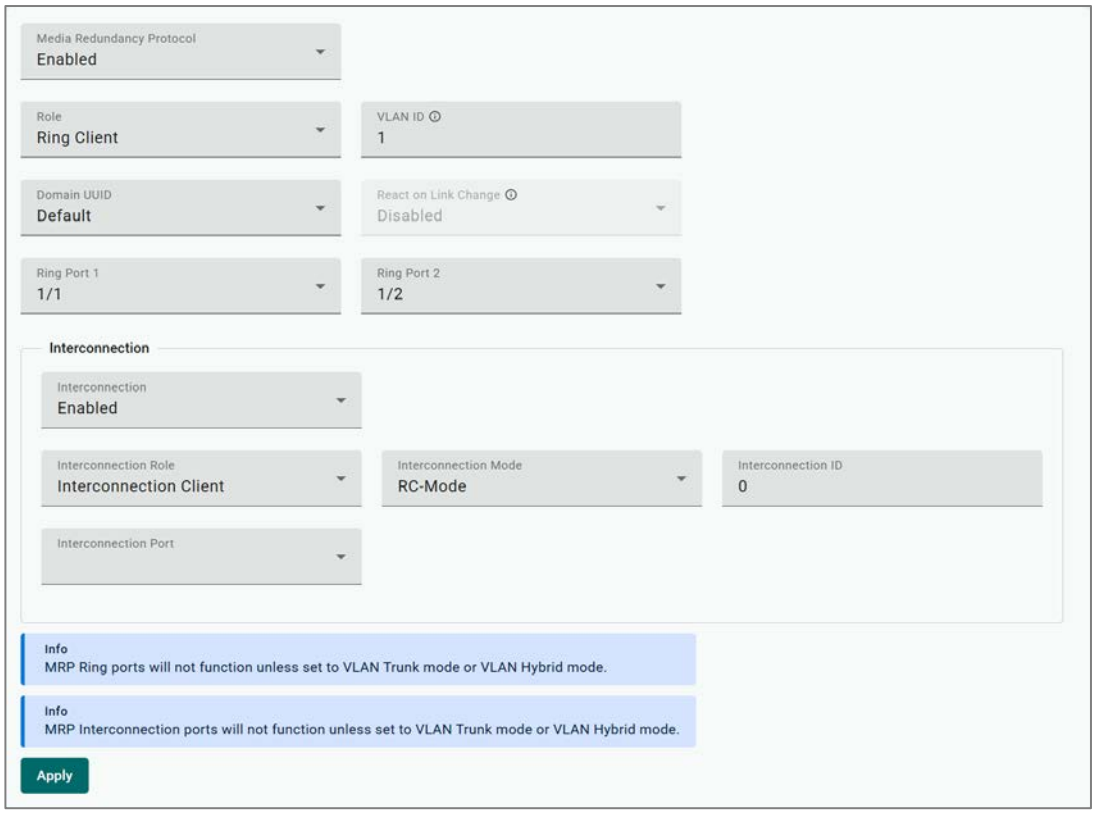
This page includes these tabs:

- Settings
- Status

MRP - Settings

Menu Path: Redundancy > MRP - Settings

This page lets you enable and configure MRP for your device.



UI Setting	Description	Valid Range	Default Value
Media Redundancy Protocol	Enable or disable Media Redundancy Protocol (MRP) for the device.	Enabled / Disabled	Disabled
Role	Specify the role for the device. • **Ring Client**: The device will act as a ring client. • **Ring Manager**: The device will act as a ring manager, and can manage and monitor the ring's health status.	Ring Client / Ring Manager	Ring Client
VLAN ID	Specify the VLAN ID to use for MRP. **Note** The VLAN ID should align with the ring port settings.	1 to 4094	1

UI Setting	Description	Valid Range	Default Value
Domain UUID	Select whether to use a default or PROFINET domain UUID.	Default / PROFINET	Default
React on Link Change **(If Role is Ring Manager)**	Enable or disable reacting on link change. Enable reaction on link change for faster recovery speeds.	Enabled / Disabled	Enabled
Ring Port 1	Specify the port to use as the 1st redundant port. **Note** Only select the port in VLAN Trunk/Hybrid mode.	Drop-down list of ports	N/A
Ring Port 2	Specify the port to use as the 2nd redundant port. **Note** Only select the port in VLAN Trunk/Hybrid mode.	Drop-down list of ports	N/A

Interconnection

UI Setting	Description	Valid Range	Default Value
Interconnection	Enable or disable MRP interconnection for the device.	Enabled / Disabled	Disabled
Interconnection Role	Select the interconnection role for the device.	Interconnection Manager / Interconnection Client	Interconnection Client
Interconnection Mode	Select the interconnection mode to use for the device. **Note** The Interconnection Manager and all Interconnection Clients in the same MRP interconnection topology must use the same interconnection mode.	LC-Mode / RC-Mode	RC-Mode
Interconnection ID	Specify an ID for the interconnection.	0 to 65535	0

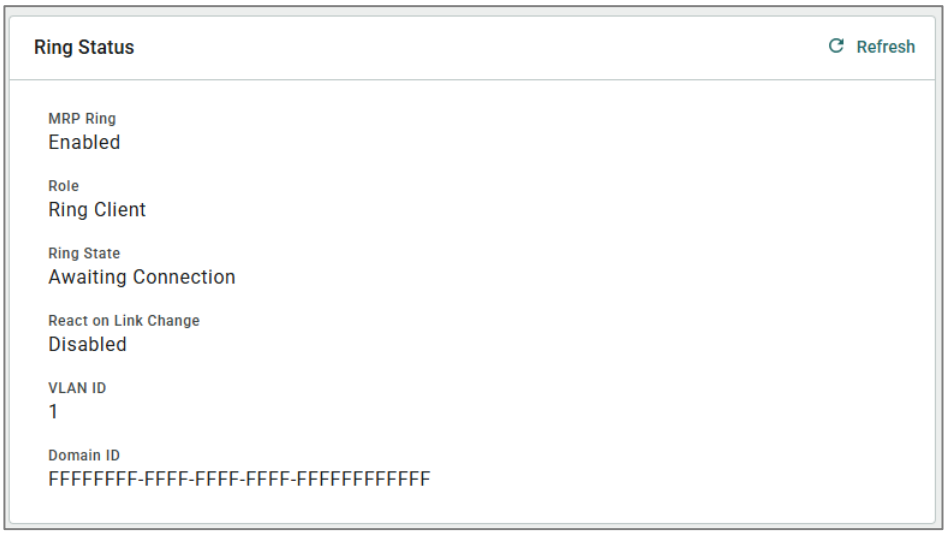
UI Setting	Description	Valid Range	Default Value
Interconnection Port	Select a port to use for the interconnection. **Note** For MRP Interconnection to perform properly, only select a port using VLAN Trunk/Hybrid mode.	Drop-down list of ports	N/A

MRP - Status

Menu Path: Redundancy > MRP - Status

This page lets you view the overall status of the MRP ring and ring ports.

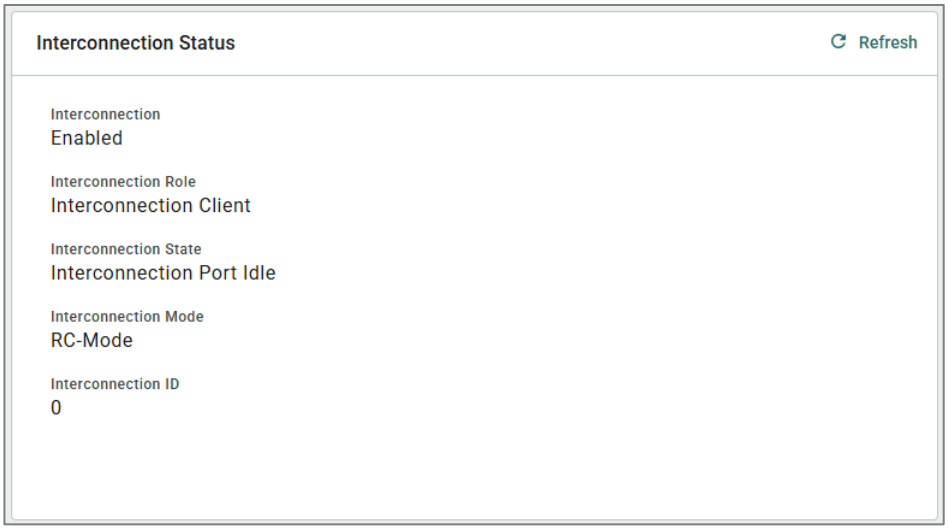
Ring Status



UI Setting	Description
MRP Ring	Shows whether the MRP ring is enabled.
Role	Shows the role of the device.
Ring State	Shows the current ring state.
React on Link Change	Shows whether reaction on link change is enabled.
VLAN ID	Shows the VLAN ID for the ring.

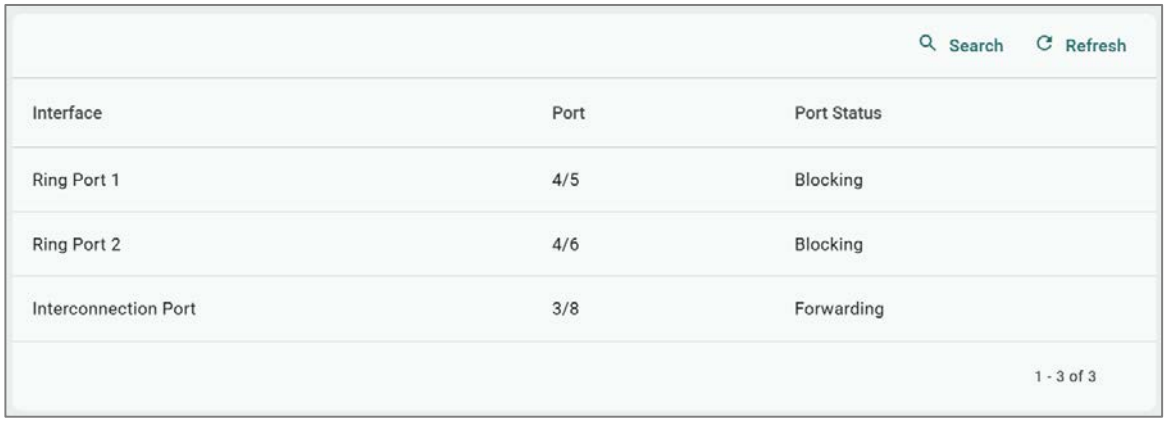
UI Setting	Description
Domain ID	Shows the domain UUID for the ring.

Interconnection Status



UI Setting	Description
Interconnection	Shows whether MRP Interconnection is enabled.
Interconnection Role	Shows the Interconnection role of the device.
Interconnection State	Shows the current Interconnection state.
Interconnection Mode	Shows the current Interconnection mode.
Interconnection ID	Shows the Interconnection ID for the ring.

MRP Port Status List



UI Setting	Description
Interface	Shows the interface the entry is for.
Port	Shows the port used for the interface.
Port Status	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.

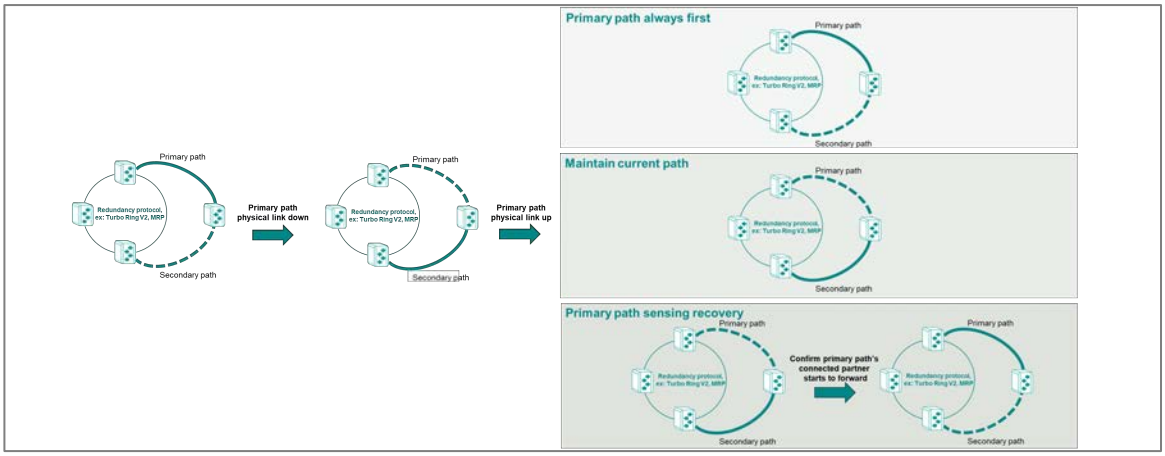
Multiple Dual Homing In Depth

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.



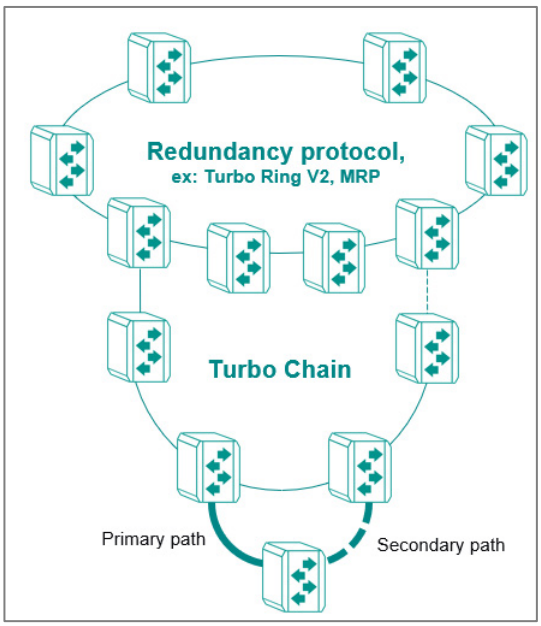
Note

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
Turbo Ring / Turbo Chain	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:

1. Port-Channel and member ports can not be deleted while set as a Primary or Secondary port.
2. 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
Primary path always first	Reconnects as soon as physical media is available, with recovery time determined by data link responsiveness.
Maintain current path	After switching paths, device will not switch back unless the secondary becomes unavailable, minimizing recovery time.
Primary path sensing recovery	Reconnects when primary path data link goes back up, reducing recovery time.

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

6. To edit a Session, under Dual Homing Table Settings, click **[Edit]** next to the corresponding **Session ID**.

The Edit Session Settings screen appears.

7. Specify all of the following, and click **Apply** to save your changes:

Option	Value
Status	**Enabled**
Primary Port	Specify the Port used as the primary path. This port will be the default link to the network.
Secondary Port	Specify the Port used as the secondary path. This port will be the backup link to the network.

The corresponding **Session ID** updates.

8. 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.

1. Sign in to the device with administrator credentials.
2. Go to **Port** > **Port Interface** > **Linkup Delay**.
3. Under **Linkup Delay**, select **Enable** from the drop down list, and then click **Apply**.
4. Configure Linkup Delay on each port by clicking **[Edit]** next to the corresponding **Port**, configuring the following, and then clicking **Apply**:

Linkup Delay	**Enabled**
Delay Time	2 seconds is the default and recommended setting.
Copy configurations to ports	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.

Limitations

You can create up to 4 multiple dual homing sessions.

Multiple Dual Homing Settings



UI Setting	Description	Valid Range	Default Value
Multiple Dual Homing	Enable or disable multiple dual homing for your device.	Enabled / Disabled	Disabled
Path Switching Mode	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:** 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.	Primary path always first / Maintain current path / Primary path sensing recovery	Primary path always first

Multiple Dual Homing Session List



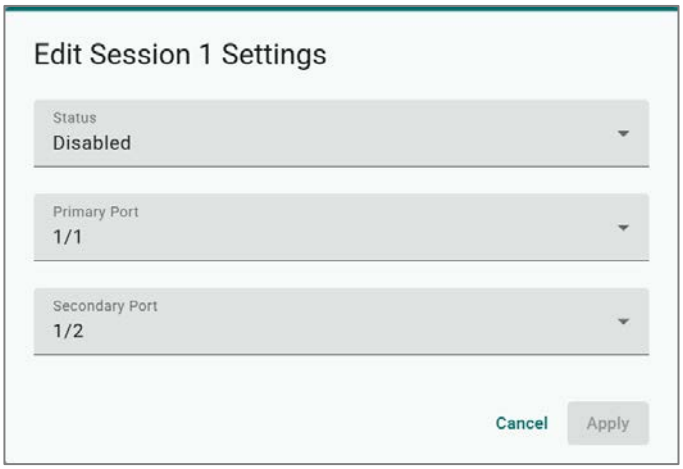
UI Setting	Description
Session ID	Shows the Multiple Dual Homing session ID the entry is for.
Status	Shows whether Multiple Dual Homing is enabled for the session.
Primary Port	Shows the primary port for the session.
Secondary Port	Shows the secondary port for the session.

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.



UI Setting	Description	Valid Range	Default Value
Status	Enable or disable Multiple Dual Homing for the session.	Enabled / Disabled	Disabled
Primary Port	Select the primary port to use for the session.	Drop-down list of ports	Depends on the product model
Secondary Port	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



UI Setting	Description
Session ID	Shows the session ID the entry is for.
Primary Port	Shows the primary port for the session.
Primary Link Status	Shows the current link status of the primary path for the session.
Primary Port Status	Shows the current status of the primary port for the session.
Secondary Port	Shows the secondary port for the session.
Secondary Link Status	Shows the current link status of the secondary path for the session.
Secondary Port Status	Shows the current status of the secondary port for the session.

About Multiple Network Coupling

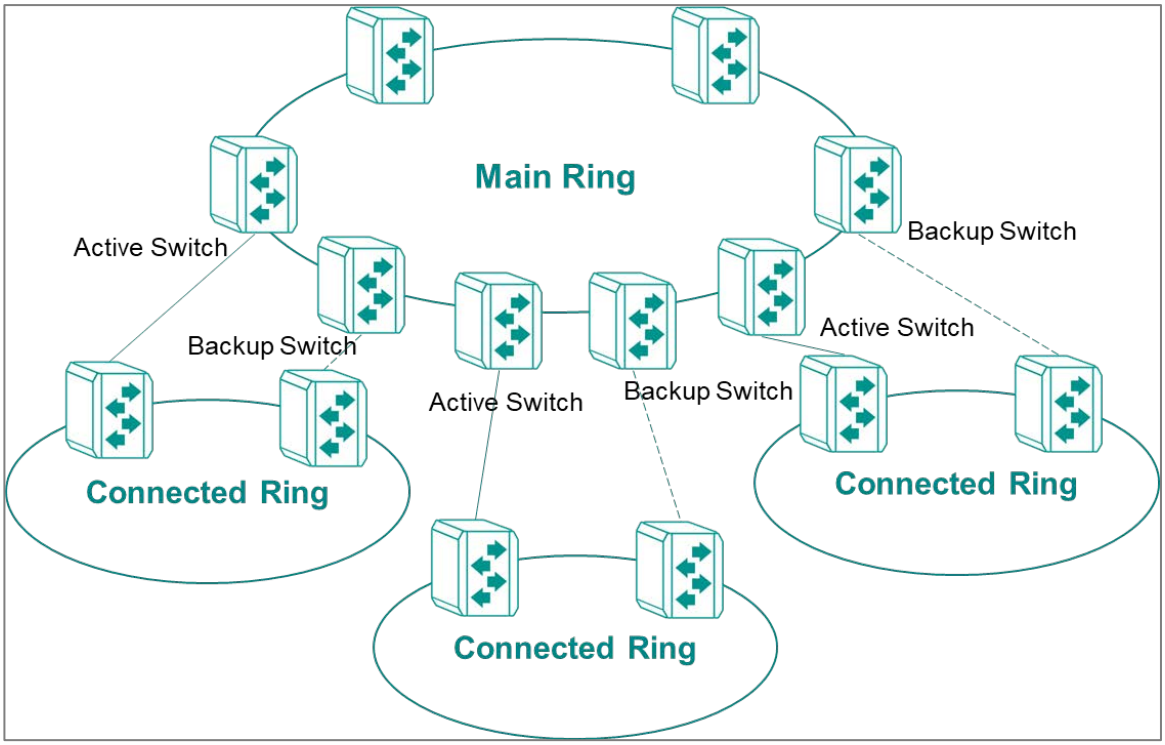
Multiple Network Coupling (MNC) is a proprietary Moxa feature designed to address various scenarios where heterogeneous redundant networks need to be connected to operate together.

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.



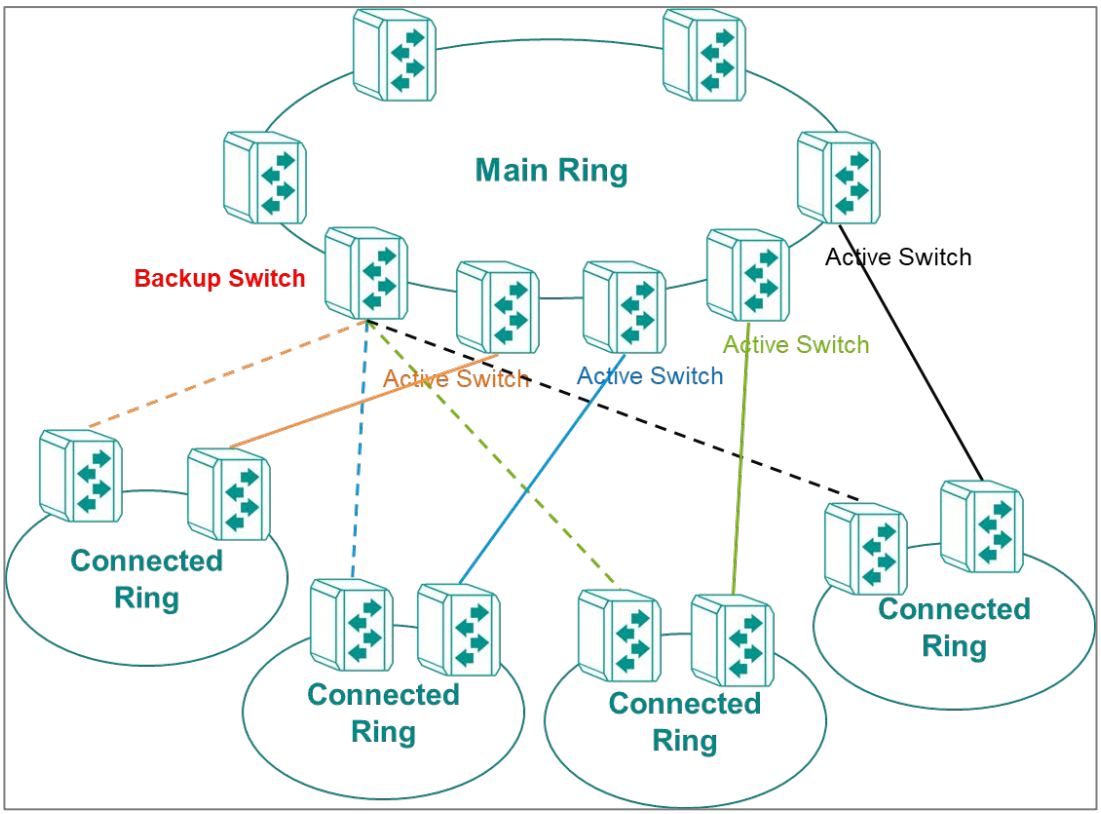
MX-NOS supports the following redundancy protocols for the Main Ring:

- 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

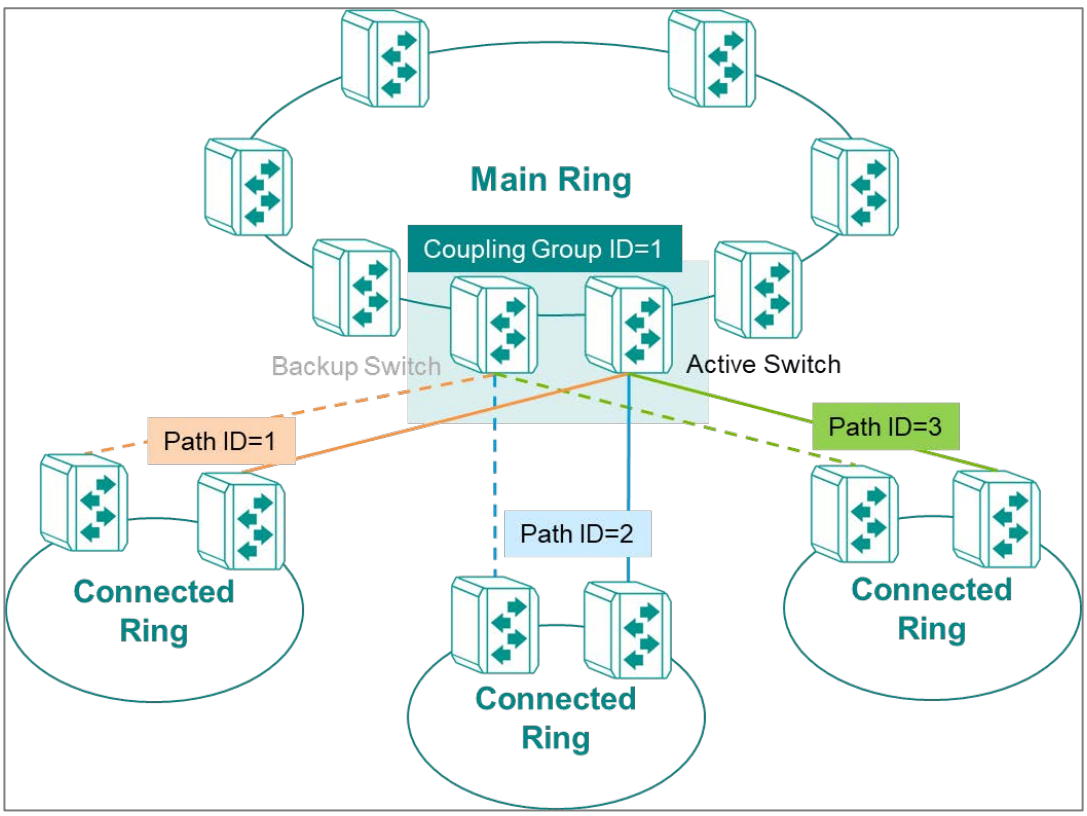
These are some examples of different Multiple Network Coupling deployments and guidelines for topology planning.

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.

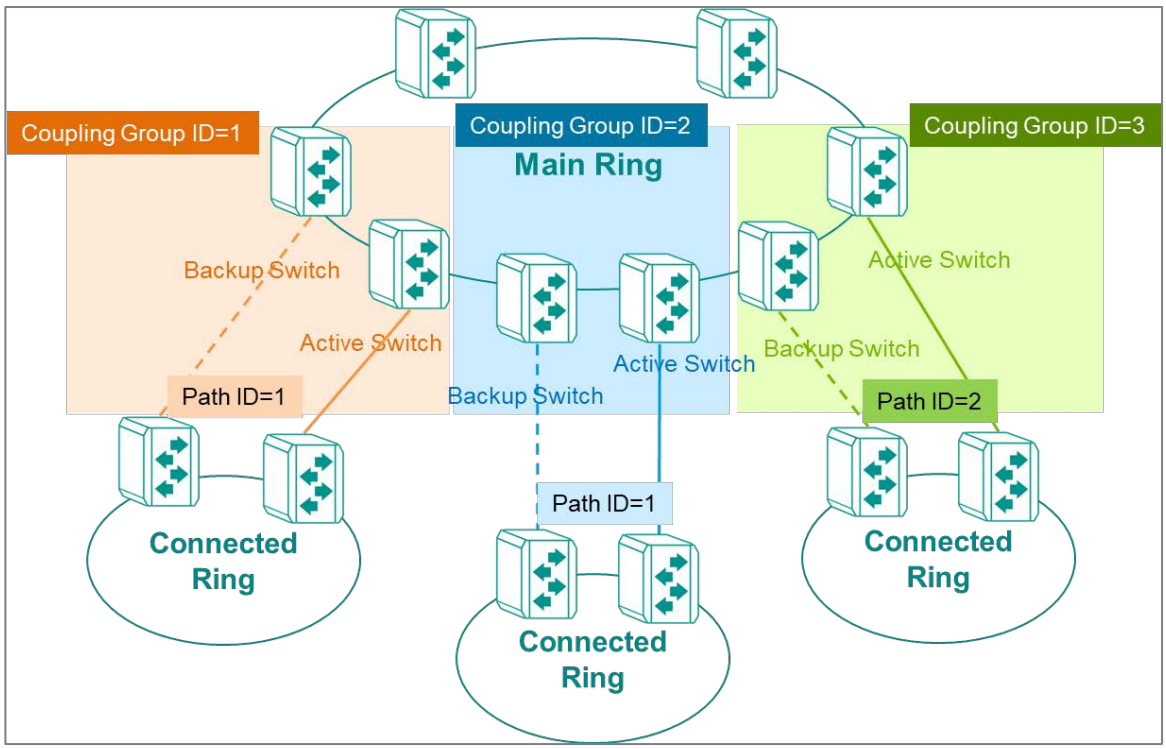
One Coupling Group, Shared Active and Backup Switches

This topology shares the same Main Ring switches for all Connected Rings. This is a simple, centralized configuration.



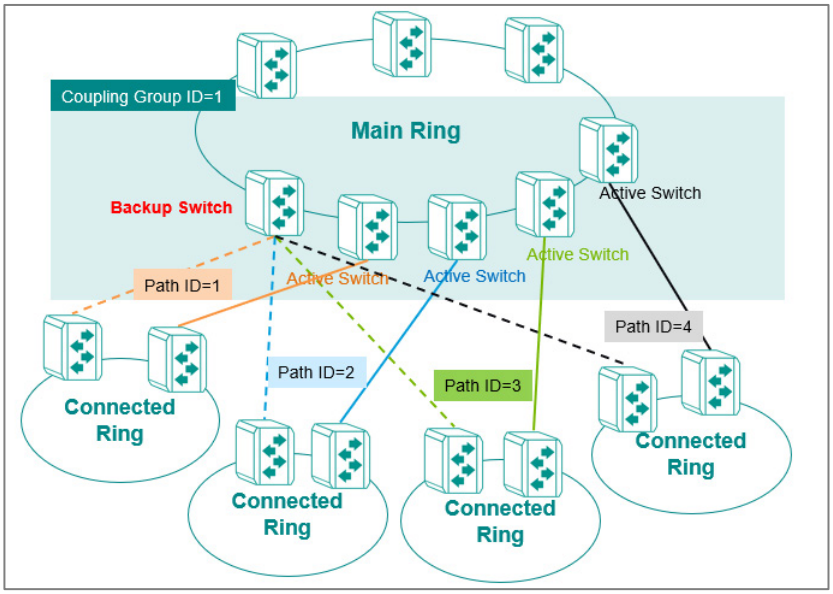
Three Coupling Groups, Separate Active and Backup Switches

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
Multiple Network Coupling	**Enabled**

Option	Value
Coupling switch role	• **Active**: device will serve as the active switch • **Backup**: device will serve as the backup switch Only one backup switch supported per connected ring.
Coupling group ID	Specify the coupling group ID from the dropdown list.
Coupling polling interval	• **80** ms: recommended for up to 16 path IDs. • **40** ms: recommended for up to 8 path IDs.

4. To configure Path IDs (corresponding to each Connected Ring), under Coupling Table Settings, click the corresponding ***[Edit]***.
   The Edit Path ID Settings screen appears.
5. Configure all of the following, and then click **Apply**:

Option	Value
Status	**Enabled**
Path ID	Specify the Path ID, corresponding to your Connected Ring
Coupling Port	Specify the port to which your Connected Ring will be connected.

6. 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

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:

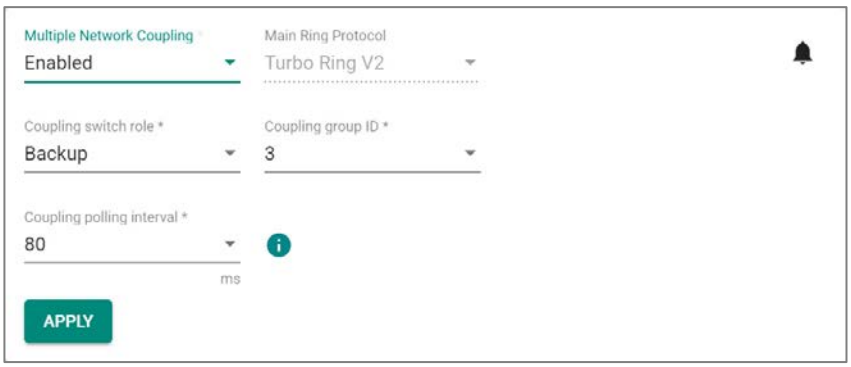
- Settings
- Status

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.

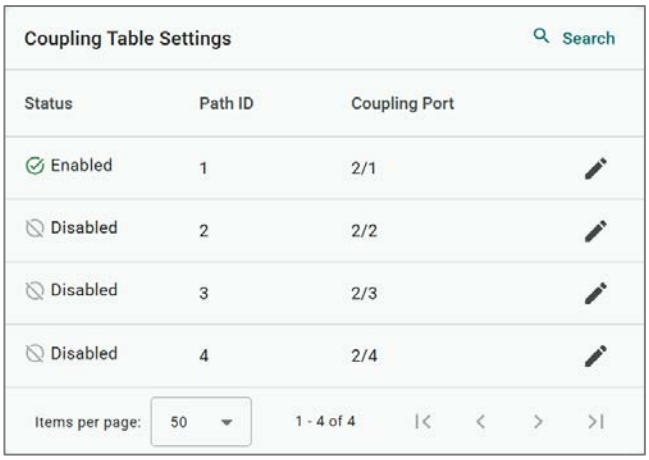
Multiple Network Coupling Settings



UI Setting	Description	Valid Range	Default Value
Multiple Network Coupling	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
Main Ring Protocol	Shows the redundant protocol being used for the Main Ring. This value cannot be changed here. **Note** The redundant protocol you want to enable in the Main Ring must be enabled before enabling Multiple Network Coupling. The redundant protocols supported in the Main Ring include: • Turbo Ring V2 • MRP • HSR	N/A	N/A

UI Setting	Description	Valid Range	Default Value
Coupling switch role	Specify the device's switch role in the Main Ring. • **Active:** The device will act as the active switch responsible for the primary path. • **Backup:** The device will act as the backup switch responsible for the backup path to the Connected Ring.	Active / Backup	Active
Coupling group ID	Specify the coupling group ID for the switch. **Note** The coupling group ID for the paired active switch and backup switch must be the same.	1 to 16	1
Coupling polling interval	Specify the coupling polling interval in milliseconds used to check if the coupling path is forwarding. **Note** The maximum number of active/backup switch pairs is 16. W e 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.	40, 80	80

Coupling Table Settings



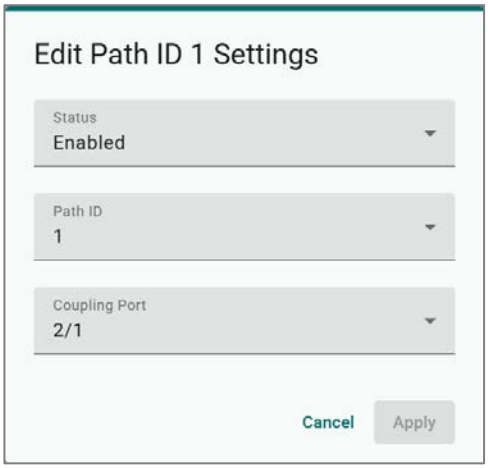
UI Setting	Description
Status	Shows whether Multiple Network Coupling is enabled for the entry.

UI Setting	Description
Path ID	Shows the path ID for the entry.
Coupling Port	Shows the coupling port for the entry.

Edit Path ID

Menu Path: Redundancy > Layer 2 Redundancy > Multiple Network Coupling - Settings

Clicking the **Edit (✎)** icon for an entry allows you to enable and configure the coupling port for the entry.



UI Setting	Description	Valid Range	Default Value
Status	Enable or disable the Path ID for the device.	Enabled / Disabled	Disabled
Path ID	Select the Path ID for the entry. ✎ **Note** • On an active or backup switch, you can configure a maximum of 4 Path ID/Coupling Port pairs. • Make sure each active/backup switch pair is using the same Path ID.	1 to 16	1
Coupling Port	Select the port to use as a coupling port for the Path ID.	Drop-down list of ports	Depends on the product model

Multiple Network Coupling - Status

Menu Path: Redundancy > Layer 2 Redundancy > Multiple Network Coupling - Status

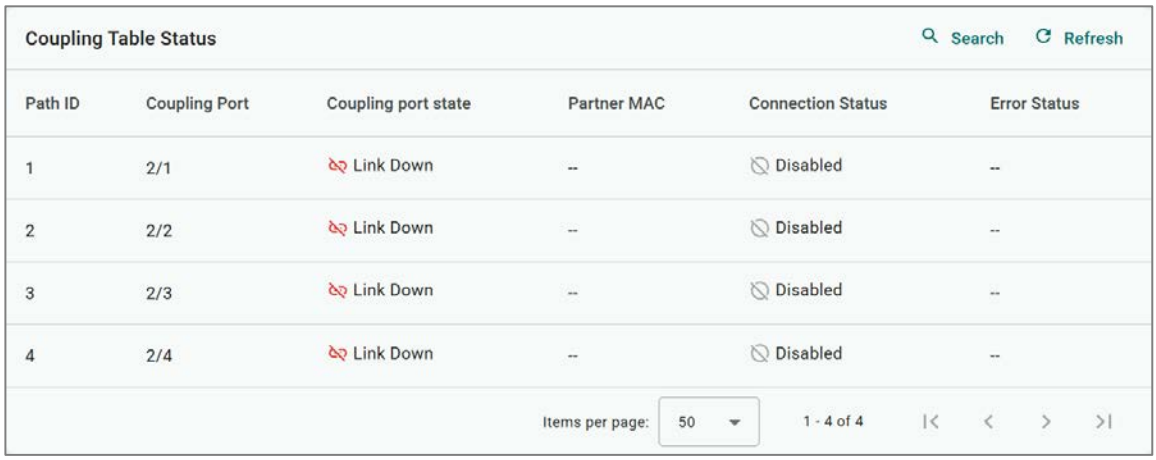
This page lets you view the status of Multiple Network Coupling for your device.

Role Information



UI Setting	Description
Coupling switch role	Shows the coupling switch role of the device.
Coupling group ID	Shows the coupling group ID of the device.

Coupling Table Status



UI Setting	Description
Path ID	Shows the Path ID for the entry.
Coupling Port	Shows the Coupling Port for the entry.

UI Setting	Description
Coupling Port State	Shows the current Coupling Port State for the entry.
Partner MAC	Shows the MAC address of the current partner for the entry, if there is one.
Connection Status	Shows the connection status of the current partner for the entry.
Error Status	Shows Error Status of the entry, if applicable. • **Multiple active switches**: There are duplicate active switches in same path ID and group ID • **Multiple backup switches**: There are duplicate backup switches in same path ID and group ID, or multiple backup switches for a single active switch. **Note** If there is an error, check the configurations for the device and partner device to ensure there are no duplicates.

About IEC 62439-3

IEC 62439-3 is an international standard defining protocols to achieve seamless, high-availability Ethernet networks for industrial automation and mission-critical applications.

It specifies two key redundancy protocols:

- **Parallel Redundancy Protocol (PRP)**: Enables devices to connect simultaneously to two independent LANs. Each frame is transmitted over both LANs in parallel, ensuring zero recovery time in case of a single network failure.
- **High-availability Seamless Redundancy (HSR)**: Uses a ring topology where each device forwards frames along the ring, sending duplicates in both directions. This also provides seamless failover without frame loss.

These protocols allow systems to tolerate failures in any single network without interrupting communication. PRP and HSR support deterministic redundancy, ensuring continuous data transmission without switchover delays, which is essential for real-time control systems, substation automation, and other applications requiring uninterrupted operation.

About RedBoxes

A Redundancy Box (RedBox) is a specialized network device defined in IEC 62439-3 for connecting nodes that do not natively support HSR or PRP, or for coupling PRP and HSR networks together. It allows standard Ethernet devices or different redundancy domains to communicate seamlessly within a high-availability network.

Key functions of a RedBox

- **Connects non-redundant devices**: RedBox lets standard single-port Ethernet devices join a redundant HSR ring or PRP network, providing them with seamless redundancy without modifying the end device itself.
- **Couples PRP and HSR domains**: RedBox can act as a bridge between a PRP dual-LAN network and an HSR ring, enabling traffic to flow between them while maintaining redundancy behavior and supervision mechanisms.

Primary roles of RedBoxes:

- **SAN-to-HSR**: Connects Singly Attached Nodes (SANs) to an HSR ring.
- **SAN-to-PRP**: Connects a SAN to both PRP LAN A and LAN B.
- **PRP-to-HSR**: Acts as a **coupling bridge** between a PRP domain and an HSR ring.

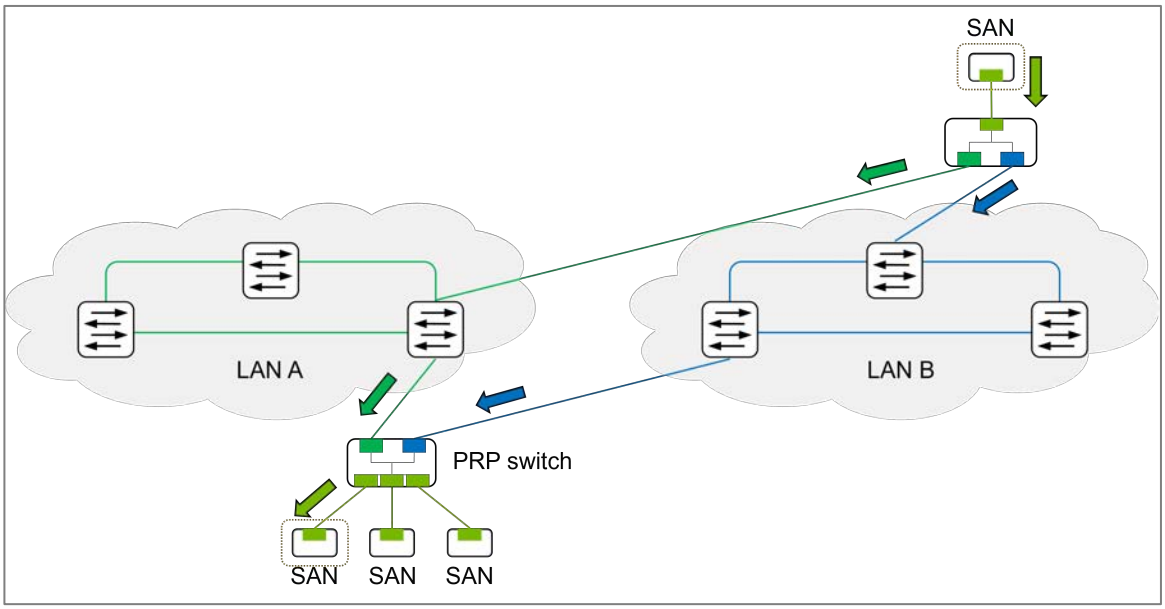
PRP in Depth

PRP allows a redundant connection across two independent LANs simultaneously. Because each frame is duplicated, there is no transition time in the event of a failure. PRP can be useful when you need redundancy with existing networks. As long as both PRP devices support the PRP protocol, Intermediate networks do not need to be PRP aware, and need only provide Layer 2 paths between PRP devices.

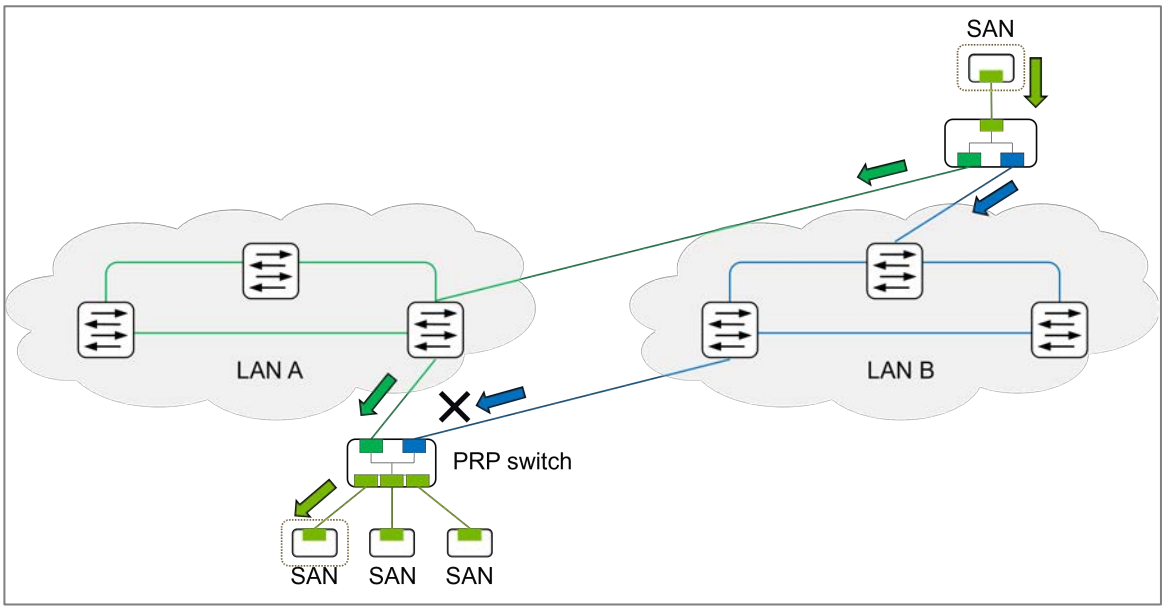
PRP devices use dedicated ports. Those ports should have the same MAC and IP address (unique within their respective networks, but duplicated on both ports A and B).

PRP network devices often host multiple Singly Attached Nodes (SANs)—conventional network devices that do not support PRP redundancy, such as end-user devices or industrial equipment with single network interfaces.

Because PRP connections use specialized devices with unique identifiers, risk of looping is minimized.



In this example, a PRP Switch connects to a RedBox by traversing two different ring networks, LAN A (Green) and LAN B (Blue). Note that LAN B does not connect through the same device; this is by design. The PRP link over LAN B will transparently benefit from redundancy protocols ordinarily operating over LAN B, without requiring additional configuration. Although this example employs ring topologies in LAN A and B, most topologies with clear L2 paths are supported.



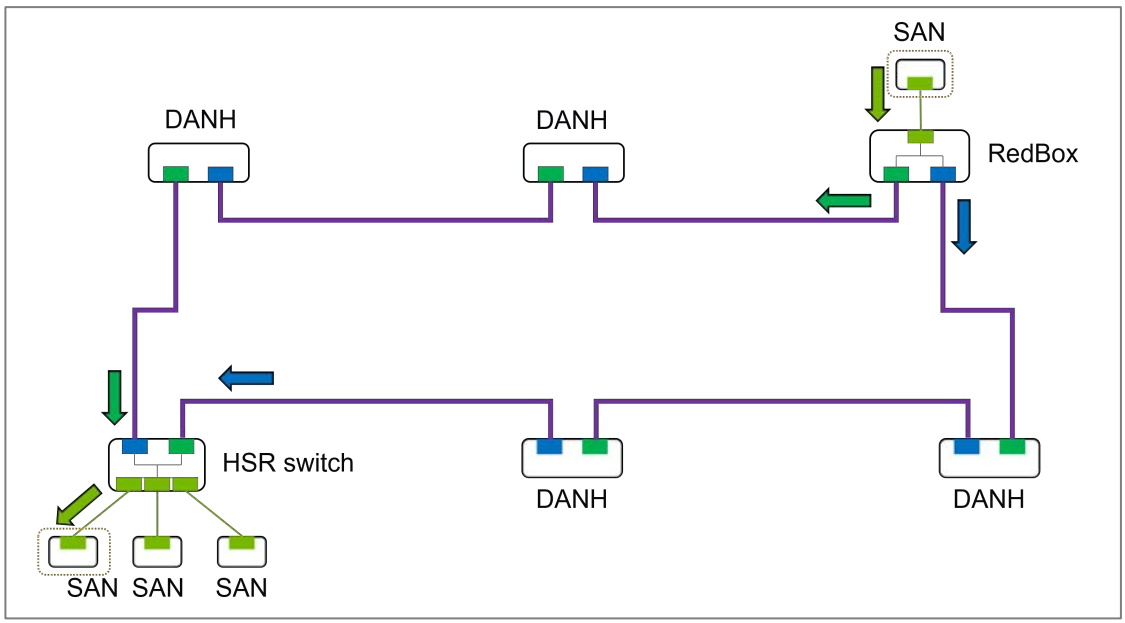
In the event of a block on LAN B, LAN A continues transmitting packets as normal—with zero transition time. The connection is automatically restored when the block is resolved.

HSR in Depth

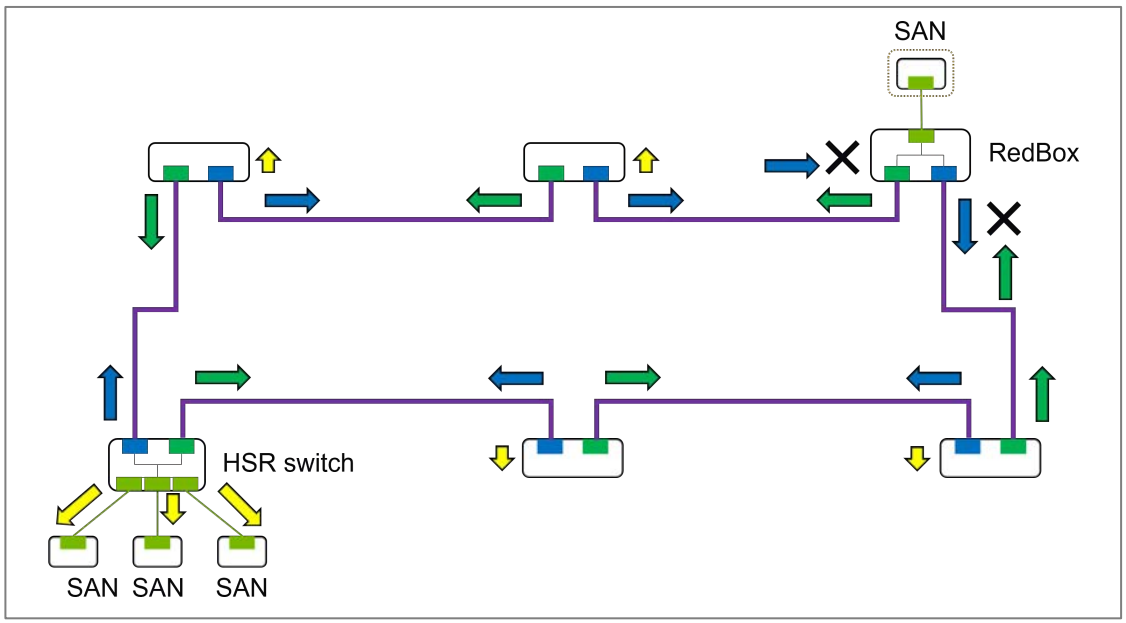
High-availability Seamless Redundancy (HSR) is a redundant ring topology. HSR duplicates frames along both paths of the ring to ensure zero transition time in the event of a failure.

Like PRP, HSR uses dedicated ports (Port A/ Port B) on each network device to form the ring.

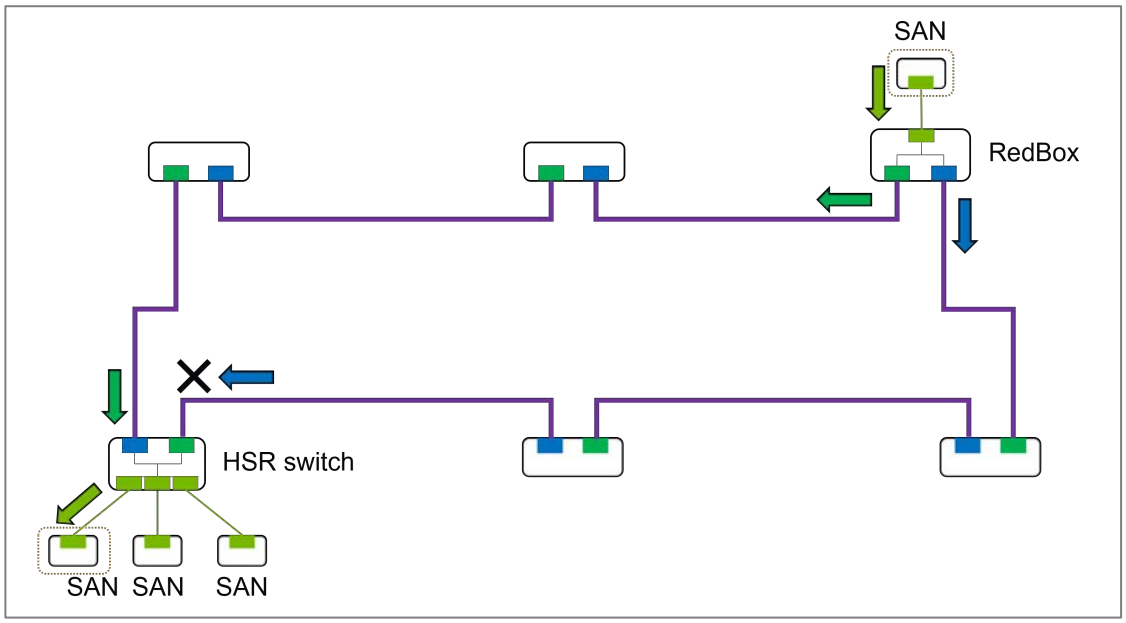
HSR network devices often host multiple Singly Attached Nodes (SANs)—conventional network devices that do not support HSR redundancy, such as end-user devices or industrial equipment with single network interfaces.



An HSR switch connects to the ring by connecting to dedicated HSR ports (Port A/B). Frames are duplicated and sent through both directions of the ring. Frames sent from the RedBox to the HSR switch traverse the network in both directions, with each device retransmitting frames until they arrive. The HSR switch recognizes the frames have converged on their destination, and does not transmit them further. The frames are then passed to destination SANs.



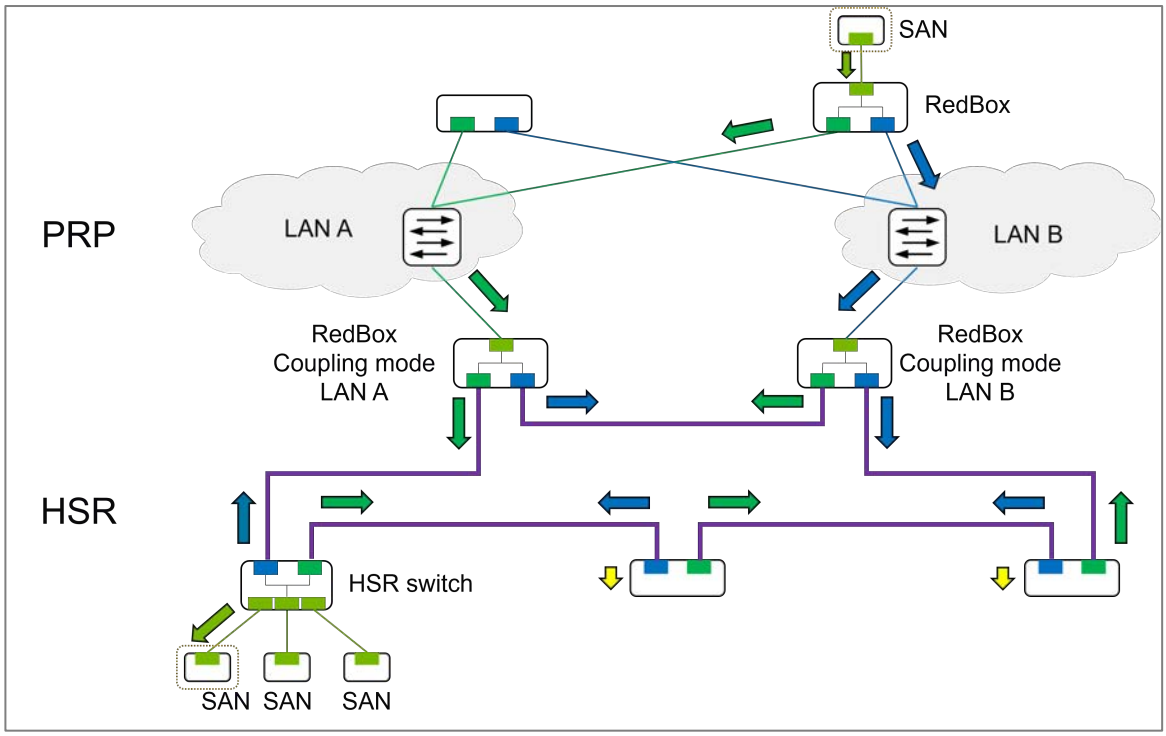
Broadcast frames are relayed to the entire ring. Frames are not re-forwarded by their originator to avoid looping.



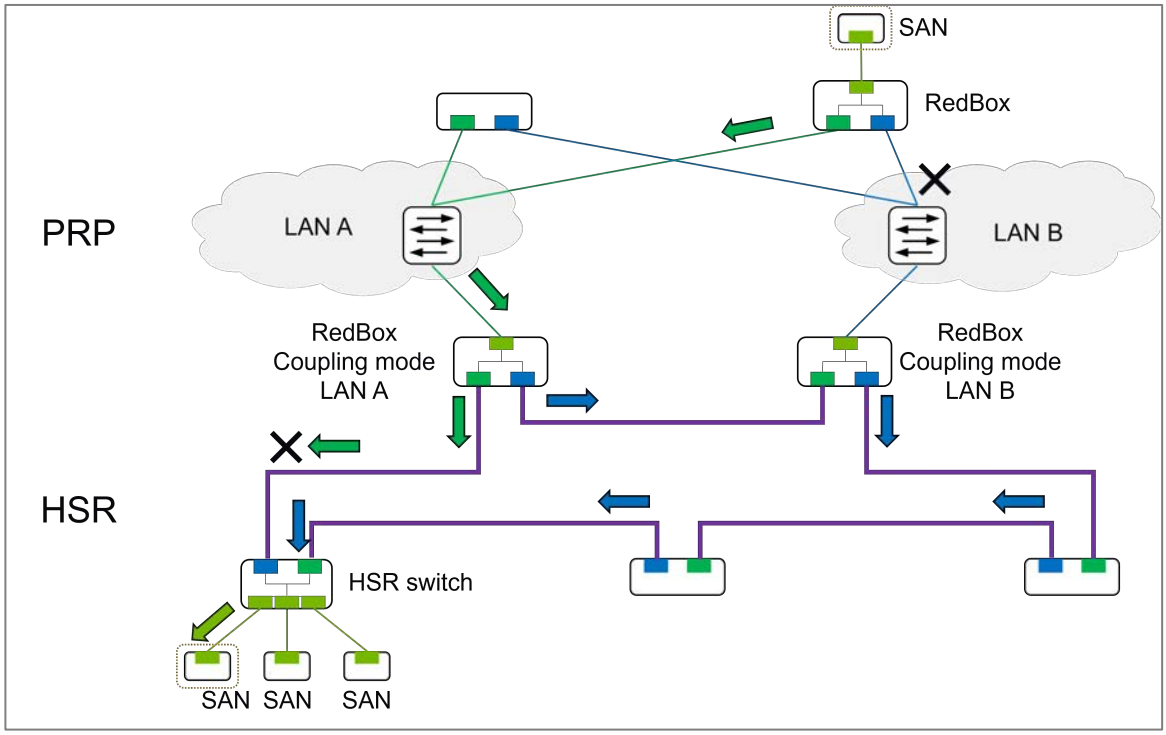
In the event of a failure in one segment of the ring, packets continue to flow over the active segment. Unicast frames are forwarded across the ring until they reach their intended destination.

About PRP-HSR Single Coupling

Different kinds of networks can be coupled together to leverage maximum redundancy without replacing existing equipment.



In this example, an HSR ring is bridged over two different, non-HSR-aware and non-PRP-aware LANs. Frames from the RedBox SAN first traverse the PRP network, then through the HSR couplings, and are then relayed along the ring until they reach the destination HSR switch.



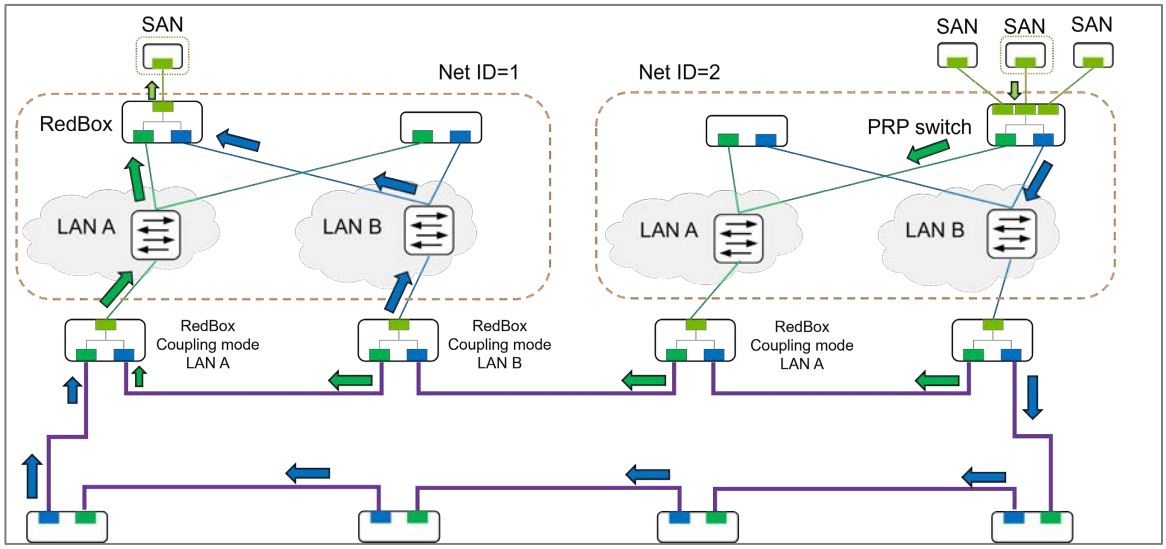
In the event of one or more failures, frames are routed along available routes and networks until they reach their destination without failover time.

Note

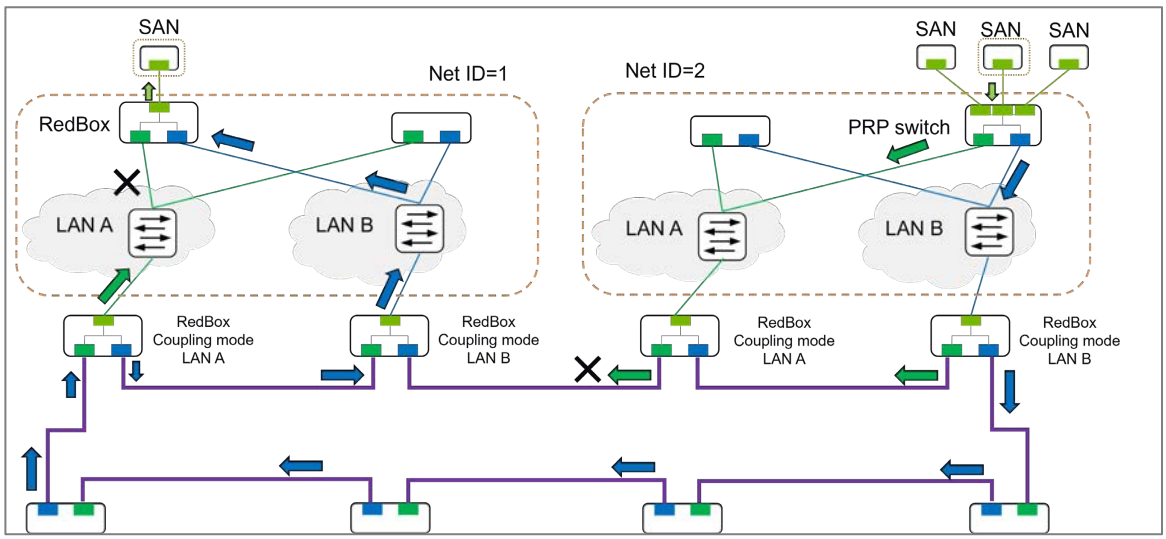
Important: Coupling mode must be enabled on links between PRP and HSR to avoid looping of the PRP (LAN A/B) networks.

About PRP-HSR Multiple Coupling

HSR and PRP can be further combined to link multiple networks with high resiliency and zero failover time.



In this example, two PRP networks are connected by an HSR ring. Outbound frames from the SAN on the PRP Network ID 2 are duplicated across the PRP network, and passed to the HSR network where they are passed over the HSR ring over the HSR ring until reaching the PRP Network ID 1, where they are duplicated across the PRP network before converging on the destination RedBox, which forwards them to the SAN.



In the event of multiple failures in the network (in this case, a gap in the ring and a gap in the PRP network), frames continue to be sent over the remaining redundant links. Because no rerouting is required, there is no failover time, despite network complexity.

Note

Important: Coupling mode must be enabled on links between PRP and HSR to avoid looping of the PRP (LAN A/B) networks.

Note

Important: Because there are multiple PRP networks, it is vital that all PRP-aware devices on each net be configured with the correct Net IDs to avoid looping.

Considerations for PRP/HSR Network Planning

Here are some design tips when planning a PRP and HSR deployment.

For PRP and HSR networks:

- Configure Supervision Frame on all PRP/HSR devices. They are a mandatory part of IEC 62439-3, and the networks will not function correctly without configuration.
- Avoid single points of failure. Leverage redundancy in each part of the network, including redundant power supplies, and network redundancy in any intermediate networks.
- PRP/HSR are interoperable, but other redundancy protocols such as Turbo Chain, Turbo Ring, and MRP cannot be enabled on the same ports at the same time.
- Port mirroring and SPAN are supported (1-to-1 or N-to-1) with the following caveats:
    - Ports A and B cannot be set as mirror destination ports.
    - Ports A and B cannot be set as RSPAN source ports.
- Supports QoS, DHCP Relay Agent, and Access Control Lists.

For PRP networks:

- Use similar topologies in both networks to keep latencies similar.
- Limit SANs to a single network.
- Do not connect non-PRP devices to both intermediate LANs to avoid looping. Only PRP-aware devices should be used.

- Do not connect RedBoxes with Layer 2 paths that use bridges to PRP intermediate networks.
- Make sure that LAN A and B are fully separated.

For HSR Networks:

- Ensure that all devices directly on the HSR ring are HSR aware.

About Supervision Frames

Supervision frames are specialized Ethernet frames defined by IEC 62439-3 to monitor network health in PRP and HSR systems. Each node periodically sends supervision frames to announce its presence and unique identifier to other nodes. Devices maintain a table of known nodes based on received supervision frames.

The supervision mechanism serves multiple purposes:

- **Presence detection**: Verifies that nodes are online and reachable.
- **Failure detection**: Absence of supervision frames beyond a configured time threshold indicates possible node or network failure.

Supervision frames use reserved multicast destination addresses, enabling all PRP/HSR-capable devices to receive them without broadcasting to every device on the network.

Enabling PRP/HSR

PRP/HSR must be enabled to function.

- Ensure that Turbo Chain, Turbo Ring, and MRP are disabled on this device.

1. Sign in to the device with administrator credentials.
2. Go to **Redundancy** > **IEC 62439** > **PRP/HSR**.
3. Configure the following:

Option	Value
PRP/HSR Protocol	Choose • **PRP** for devices in a PRP network. • **HSR** for devices in an HSR ring. • **Coupling** for devices that are coupled between HSR rings and PRP networks.

Option	Value
Entry Forget Time	Choose: • **100** ms for Fast Ethernet • **10** ms for Gigabit Ethernet Since PRP and HSR use duplicate frames in loop-like topologies, frames are briefly stored in a duplicate table to make sure the device does not forward a frame more than once. This value specifies how long those entries are maintained.
Net ID	For **PRP/HSR Protocol**: **Coupling**, choose a Net ID from **1** to **7**, which corresponds to the PRP network to which the device attaches.
LAN ID	For **PRP/HSR Protocol**: **Coupling**, choose **LAN A** or **LAN B** which corresponds to the PRP network to which the device attaches.

4. Select **Apply** to save your changes.

Configuring Supervision Frames

Supervision Frames must be configured for PRP/HSR to function.

1. Sign in to the device using administrator credentials.
2. Go to **Redundancy** > **IEC 62439** > **Supervision Frame**, and then selecting **General**.
3. Configure the following:

Option	Value
Supervision Frame	Choose **Enabled**. Supervision frames must be enabled for PRP/HSR to function.
Life Check Interval	Specify the interval between two successive supervision frames between 1 to 60 seconds, default 2.
Destination Address	Specify the Bridge Multicast Address used by your PRP/HSR networks in hex. This might be used when multiple PRP/HSR networks are visible at Layer 2 but not logically part of the same redundant domain. Ordinarily, all network devices in the same redundant domain should use the same multicast address.

Option	Value
Supervision Forward To Interlink	Choosing **Enabled** sends Supervision Frames over interlinks (ie LAN A, LAN B in PRP).

4. Click **Apply** to save changes.

Supervision frames can be monitored from **Redundancy** > **IEC 62439** > **Supervision Frame**, and then selecting **Nodes Table**.

IEC 62439-3

Menu Path: Redundancy > IEC 62439-3

This section lets you configure IEC 62439-3 redundancy features.

This section includes these pages:

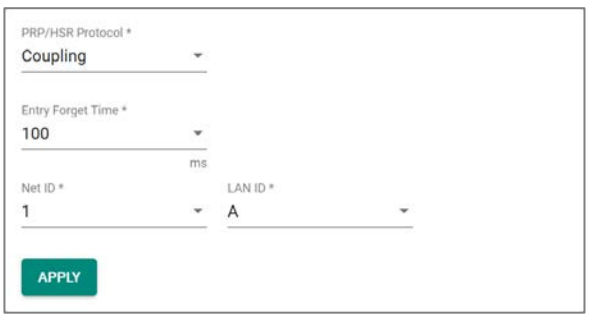
- PRP/HSR
- Supervision Frame

PRP / HSR

Menu Path: Redundancy > IEC 62439-3 > PRP / HSR

This page lets you enable and configure PRP/HSR protocol use for your device.

PRP / HSR Settings



UI Setting	Description	Valid Range	Default Value
PRP/HSR Protocol	Enable or disable PRP, HSR, or Coupling mode for the device. • **Disabled:** PRP and HSR will be disabled. • **PRP:** The device will use PRP. • **HSR:** The device will use HSR. • **Coupling:** The device will use PRP-HSR Coupling.	Disabled / PRP / HSR / Coupling	Disabled
Entry Forget Time	Select the entry forget time in ms. This determines the maximum amount of time in ms an entry may reside in the duplicate table. Select 100 ms for 100M, and 10 ms for 1000M.	10 / 100	10
NET ID **(If PRP/HSR Protocol is Coupling)**	Specify a NET ID to use for Coupling mode.	1 to 7	1
LAN ID **(If PRP/HSR Protocol is Coupling)**	Specify a LAN ID to use for Coupling mode.	A / B	A

Supervision Frame

Menu Path: Redundancy > IEC 62439-3 > Supervision Frame

This page lets you manage the supervision frame feature for your device.

This page includes these tabs:

- General
- Nodes Table

Supervision Frame - General

Menu Path: Redundancy > IEC 62439-3 > Supervision Frame - General

This page lets you enable and configure supervision frames for your device.

Supervision Frame Settings



UI Setting	Description	Valid Range	Default Value
Supervision Frame	Enable or disable the supervision frame feature globally. When enabled, supervision frames will be sent out to detect nodes and add them to the Nodes Table. Refer to Nodes Table for more information.	Enabled / Disabled	Disabled
Life Check Interval	Specify a life check interval in sec, which determines the interval between supervision frames.	1 to 60	2
Destination Address	Specify the multicast MAC address to use when sending supervision frames. **Note** Devices should use the default (00) unless there is a conflict with another multicast listener. Any changes to the destination address must be consistent across all PRP/HSR nodes in the same network to correctly send and receive supervision frames.	Hex value from 00 to FF	00
Supervision Forward To Interlink	Enable or disable forwarding supervision frames through the interlink port. **Note** For RedBoxes using PRP or HSR protocol: • SAN devices connected to the interlink port will receive supervision frames. For RedBoxes using PRP/HSR coupling disabled: • The RedBox listens for HSR supervision frames on LAN A/B ports and forwards them to the interlink port.	Enabled / Disabled	

Nodes Table

Menu Path: Redundancy > IEC 62439-3 > Supervision Frame - Nodes Table

This page lets you view and manage the nodes table. The nodes table shows nodes detected through supervision frames.

Limitations

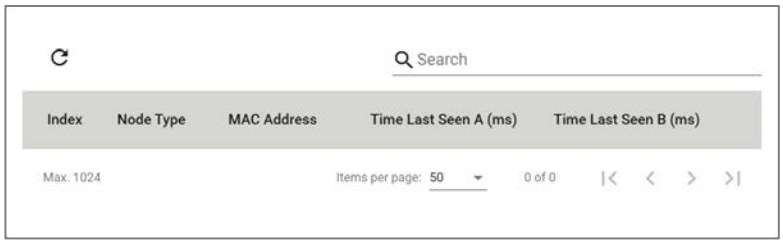
The nodes table can hold up to 1024 entries.

Nodes Table Settings



UI Setting	Description	Valid Range	Default Value
Node Forget Time	Specify the node forget time in seconds, which is how long a node entry will stay in the Nodes Table after the device stops receiving frames from the node. **Note** The Node Forget Time works as follows: • A timer starts/resets when the device receives any frame from a specific node. • If the Node Forget Time expires without new frames from that node, the local device considers that node offline and removes it from the Nodes Table. The Node Forget Time helps detect: • Node failures (e.g., a node powered off) • Network issues (e.g., link failure on both LAN A and LAN B to that node)	60 to 120	60

Nodes Table



UI Setting	Description
Index	Shows the index of the node entry.
Node Type	Shows the node type according to IEC 62439-3 (DANP/RedboxP/VDANP/DANH/RedboxH/VDANH).
MAC Address	Shows the MAC address of the node.
Time Last Seen A (ms)	Shows the last time the device received packets from the node on LAN A.
Time Last Seen B (ms)	Shows the last time the device received packets from the node on LAN B.

Note

The time between Time Last Seen A (ms) and Time Last Seen B (ms) should be the same or very close in a normally functioning network.

An increasing difference between the two times may be due to packets being dropped in one of the LANs, and may require further troubleshooting.

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.

> **Note**
>
> This feature supports weaker authentication or encryption, and may not be secure over untrusted networks. Take appropriate security precautions.

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.

Limitations

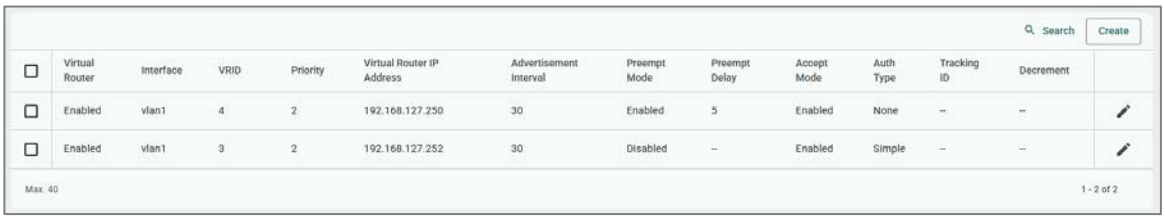
You can create up to 40 virtual routers.

VRRP Settings



UI Setting	Description	Valid Range	Default Value
VRRP	Enable or disable VRRP for the device.	Enabled / Disabled	Disabled
Version	Select the VRRP version to use.	V2 / V3	V2

VRRP List



UI Setting	Description
Virtual Router	Shows whether the VRRP interface is enabled.
Interface	Shows which network interface is used for the VRRP interface.
VRID	Shows the virtual router ID for the VRRP interface, which is used to assign the virtual router to a VRRP group.
Priority	Shows the priority of the VRRP interface. Higher numbers indicate higher priority, with 254 being the highest.

UI Setting	Description
Virtual Router IP Address	Shows the IP address of the VRRP interface.
Advertisement Interval (ms)	Shows the advertisement interval for the VRRP interface in milliseconds.
Preempt Mode	Shows the preemption status of the VRRP interface.
Preempt Delay	Shows the preempt delay value of the VRRP interface.
Accept Mode	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.
Auth Type	Shows the auth type of the VRRP interface, if VRRP V2 is being used.
Tracking ID	Shows the tracking ID of the VRRP interface.
Decrement	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 **Create** 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.



UI Setting	Description	Valid Range	Default Value
Virtual Router	Enable or disable the VRRP interface.	Enabled / Disabled	N/A
Interface	Specify which network interface to use for the VRRP interface.	Drop-down list of interfaces	N/A
VRID	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. **Note** Devices that operate as master/backup should have the same ID. Each interface supports one virtual router ID.	1 to 255	N/A
Priority	Specify the priority of the VRRP interface. Higher numbers indicate higher priority, with 254 being the highest. **Note** If multiple devices have the same priority, the device with the highest IP address will have priority.	1 to 254	N/A

UI Setting	Description	Valid Range	Default Value
Virtual Router IP Address	Specify the virtual router IP address for the VRRP interface. **Note** Devices in the same VRRP group must be in the same subnet.	Valid IP address	N/A
Advertisement Interval	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
Preempt Mode	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
Preempt Delay **(If Preempt Mode is Enabled)**	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
Auth Type	Select the authentication type to use for the VRRP interface. • **None:** No authentication will be used. • **Simple:** Simple authentication will be used.	None / Simple	N/A
Authentication Key **(If Auth Type is Simple)**	Specify the authentication key to use for the VRRP interface.	0 to 8 characters	N/A
Accept Mode	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
Tracking ID	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.



UI Setting	Description	Valid Range	Default Value
Virtual Router	Enable or disable the VRRP interface.	Enabled / Disabled	N/A
Interface	Specify which network interface to use for the VRRP interface.	Drop-down list of interfaces	N/A
VRID	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. **Note** Devices that operate as master/backup should have the same ID. Each interface supports one virtual router ID.	1 to 255	N/A
Priority	Specify the priority of the VRRP interface. Higher numbers indicate higher priority, with 254 being the highest. **Note** If multiple devices have the same priority, the device with the highest IP address will have priority.	1 to 254	N/A

UI Setting	Description	Valid Range	Default Value
Virtual Router IP Address	Specify the virtual router IP address for the VRRP interface. **Note** Devices in the same VRRP group must be in the same subnet.	Valid IP address	N/A
Advertisement Interval	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
Preempt Mode	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
Preempt Delay **(If Preempt Mode is Enabled)**	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
Auth Type	Select the authentication type to use for the VRRP interface. • **None:** No authentication will be used. • **Simple:** Simple authentication will be used.	None / Simple	N/A
Authentication Key **(If Auth Type is Simple)**	Specify the authentication key to use for the VRRP interface.	0 to 8 characters	N/A
Accept Mode	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
Tracking ID	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.



UI Setting	Description
Interface	Shows which network interface is used for the VRRP interface.
VRID	Shows the virtual router ID for the VRRP interface, which is used to assign the virtual router to a VRRP group.
Priority	Shows the priority of the VRRP interface. Higher numbers indicate higher priority.
State	Shows the state of the VRRP interface. • **Init State**: This is the initial state when a virtual router starts up. • **Master State**: 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. • **Backup State**: The virtual router is in the backup state, and waiting to take over the master role if the current master fails.
Master Address	Shows the IP address of the current master for the VRRP interface.

About Tracking

Tracking monitors connectivity status, and is leveraged by multiple redundancy protocols to trigger fallback actions. For example, when using the Virtual Router Redundancy Protocol (VRRP), tracking features can detect when the primary router becomes unavailable, triggering the backup router.

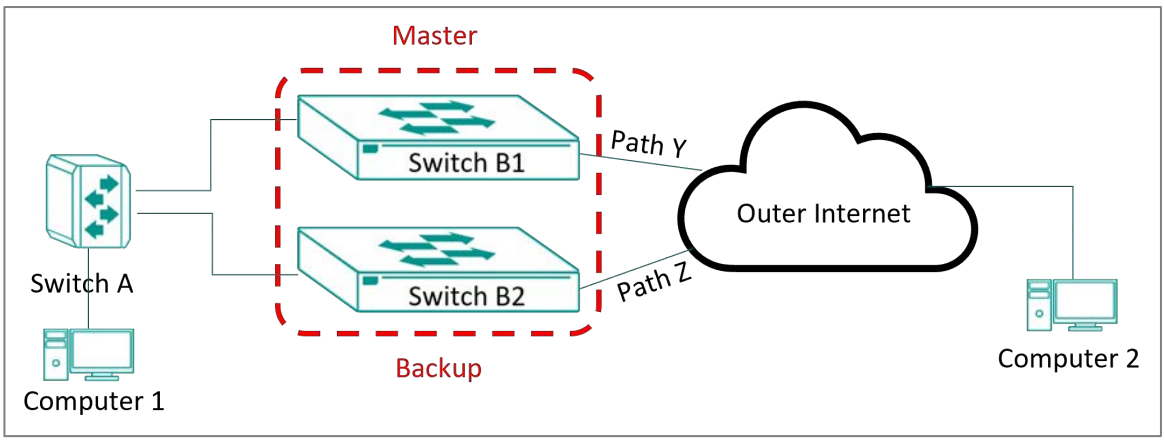
Tracking entries determine how tracking actions are triggered. The device supports three kinds of entries:

- **Interface tracking**: Monitors whether an interface or port is up or down.
- **Ping tracking**: Monitors whether a specified IP address responds to ping packets.
- **Logical tracking**: Compares the status of other tracking entries using AND, OR, NAND, or NOR operators.

Tracking operates at both Layer 2 and Layer 3.

Layer 3 Tracking: VRRP

VRRP is commonly used in conjunction with tracking for L3 switch redundancy. However, VRRP's tracking ability is limited to protecting traffic from L3 to L2, and cannot not track traffic from L3 to outside networks like the internet.



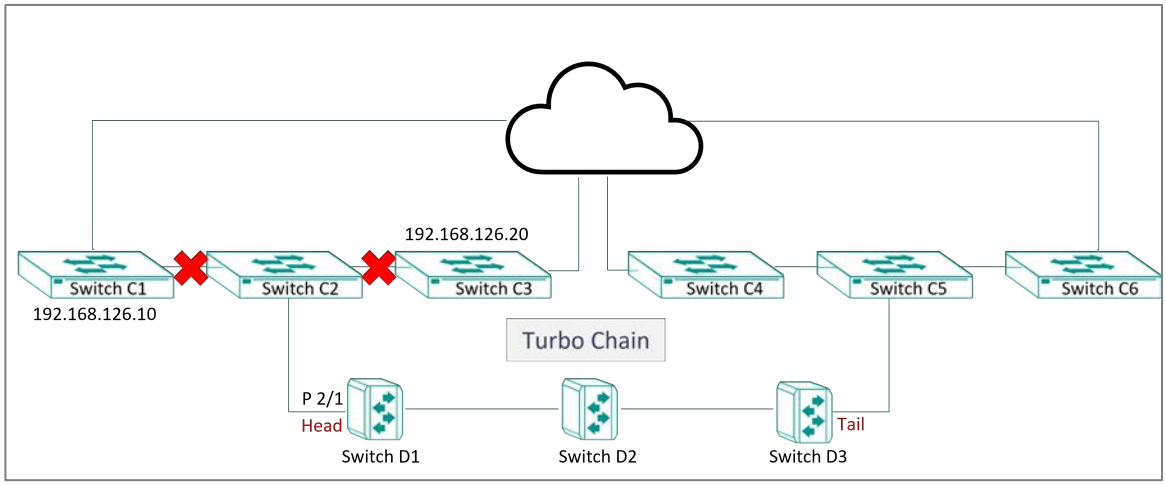
VRRP can protect traffic between L2 switches (Switch A) and L3 switches (Switches B1 and B2), but it cannot safeguard traffic from the L3 switches to the cloud. We can use a tracking to monitor **Path Y**, and if it fails, change the priority of the Master switch, rerouting through the backup switch and preventing disruption.

Layer 3 Tracking: Static Route

Static routes rely on manually configuring the next hop in the route. However, the state of the next hop may not always be known. To address this, ping tracking can monitor the IP address of the next hop, allowing the device to automatically disable the primary static route and move to a backup, ensuring that routes and subnets remain intact.

Layer 2 Tracking: Port Tracking

In Turbo Chain deployments, it can be hard to determine when pathways further than one level beyond the tail/head of the chain are down.



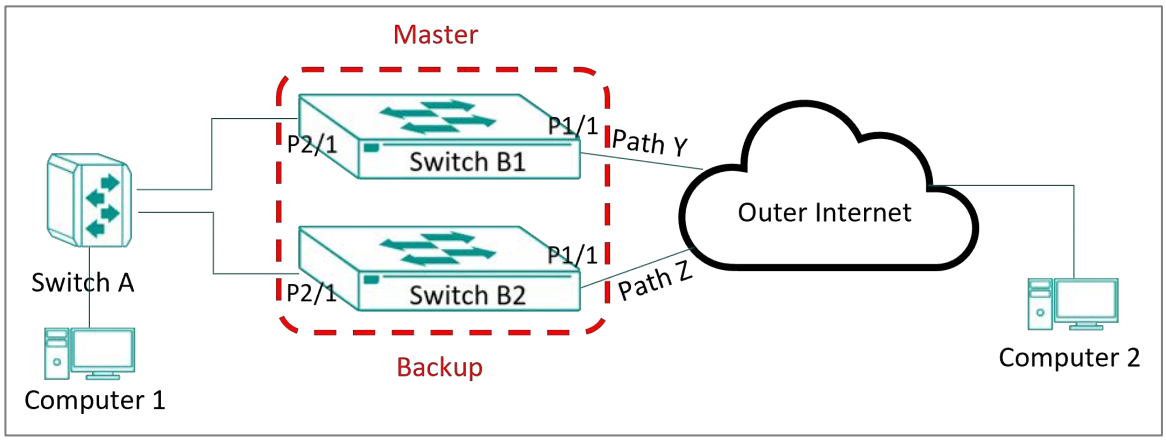
Turbo Chain only detects breaks in paths directly connected to the chain. With Tracking, we can expand this fault detection to monitor traffic from Switch C2 to Switches C1 and C3. If both paths are broken, Tracking can disable the port of Switch D1, triggering Turbo Chain to:

1. Change the head port of Switch D1 from forwarding to blocking
2. Change the tail port of Switch D3 from blocking to forwarding

This ensures that Turbo Chain doesn't maintain connections to switches that lack upstream connectivity.

Scenario: Configuring Interface Tracking for VRRP

Monitor connectivity to the outside internet to trigger VRRP (Virtual Router Redundancy Protocol).



1. On both switches, configure VRRP

At this stage, we set **Priority** values for the virtual routers: 250 for Switch B1 and 200 for Switch B2. The B1 **Priority** value will be decremented by the Tracking Entry

2. On Switch B1, Enable Tracking.
3. On Switch B1, create an interface tracking entry.

This entry will monitor Path Y connectivity to the internet.

4. On Switch B1, assign the **Tracking ID** to the Virtual Router.

This step will assign **Decrement** values to the tracking entry, which change the **Priority** values from Step 1. The reduced priority will cause Switch B2 to take priority over switch B1, routing all traffic over Path Z until Path Y is restored.

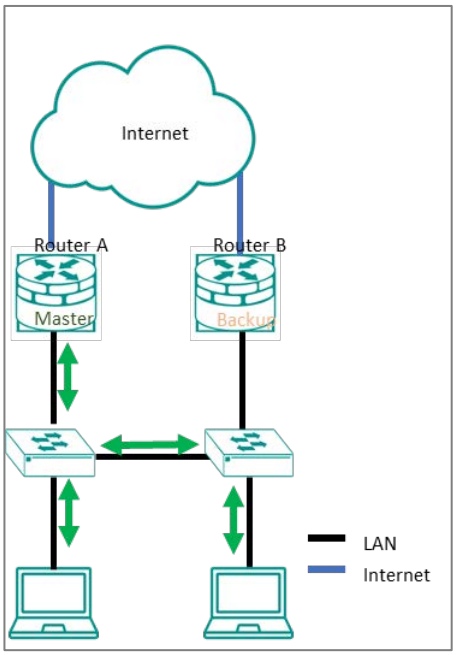
See the subsequent sections for examples and detailed instructions to configure this scenario.

Scenario: VRRP on Two Devices

In this scenario, we'll configure two devices connected to the same LAN (Local Area Network). We will configure VRRP to ensure that if one of the devices fails, the other device will continue to forward traffic to the LAN.

For example, suppose Device A (LAN interface IP: 192.168.127.1) is initially configured as the master and Device B (LAN interface IP: 192.168.127.2) as the backup in the VRRP group. Device A is responsible for forwarding packets to the LAN. The master should keep tracking the interface by pinging the device (IP 192.168.127.100) in order to make sure of the LAN communication.

If Device A were to fail by ping lost or any link down event, Device B would detect this and assume the role of the master. It would then begin forwarding packets to the LAN, ensuring that there is no disruption in network connectivity. Once Device A becomes available, it can take over as the master, and Device B reverts to its backup role.



Example: Configuring VRRP on Device A

This task assumes that each device has already configured an interface called LAN1 with the following IP addresses:

- Device A: 192.168.127.1
- Device B: 192.168.127.2

To configure Device A, do the following:

1. Sign in to the device with administrator credentials.
2. Go to **Redundancy** > **Layer 3 Redundancy** > **VRRP**, and then click **Settings**.
3. On the lower table of the screen, click **Add**.

   The Create Virtual Router screen appears.
4. Configure the following, and then click **Create**.

Option	Value
Interface	LAN1
Virtual IP	192.168.127.3
Priority	200

Option	Value
Preemption	**Enabled**
Preemption Delay	120
Target IP	192.168.127.100

The **Virtual Router** settings appear in the list.

5. Under the Virtual Router list, click **Apply**.
6. At the top of the page, under **VRRP**, select **Enabled** from the dropdown list, and then click **Apply**.

Device A is now configured for VRRP.

Continue to configure Device B.

Example: Configuring VRRP on Device B

This task assumes that each device has already configured an interface called LAN1 with the following IP addresses:

- Device A: 192.168.127.1
- Device B: 192.168.127.2

To configure Device B, do the following:

1. Sign in to the device with administrator credentials.
2. Go to **Redundancy** > **Layer 3 Redundancy** > **VRRP**, and then click **Settings**.
3. On the lower table of the screen, click **Add**.

The Create Virtual Router screen appears.

4. Configure the following, and then click **Create**.

Option	Value
Interface	LAN1
Virtual IP	192.168.127.3
Priority	100

Option	Value
Preemption	**Enabled**
Preemption Delay	120
Target IP	192.168.127.100

The **Virtual Router** settings appear in the list.

5. Under the Virtual Router list, click **Apply**.
6. At the top of the page, under **VRRP**, select **Enabled** from the dropdown list, and then click **Apply**.

Both devices are now configured for VRRP. In the event of a failure of one device, the other can take over using the same virtual IP address, ensuring continued function without reconfiguration.

Example: Creating an Interface Tracking Entry

Create an interface tracking entry to monitor port status and enable failover actions. You can select tracking entries from redundancy protocols to trigger backup or prioritization actions.

Make sure you assigned a **Tracking ID** in the previous task.

1. Sign in to the device with administrator credentials.
2. Go to **Redundancy** > **Tracking**.
3. Next to **Tracking of...**, click **Select**, choose **Interface**, and then click **Add**.
4. Configure all of the following, and then click **Create**:

Option	Value
Interface Tracking	**Enabled**
Tracking ID	1
Interface Type	**Port**
Port	**1/1**

The Interface Tracking Entry appears on the list.

Continue to add the interface tracking entry to the virtual router.

Example: Enabling Tracking

Turn on tracking to allow the system to monitor interfaces and trigger redundancy actions.

1. Sign in to the device with administrator credentials.
2. Go to **Redundancy** > **Tracking**.
3. Set **Tracking** to **Enabled**, and then click **Apply**.

Example: Adding an Interface Tracking Entry to a Virtual Router

Add the tracking entry to a virtual router to enable automatic failover when connectivity is lost.

Make sure you assigned a **Tracking ID**in the previous task.

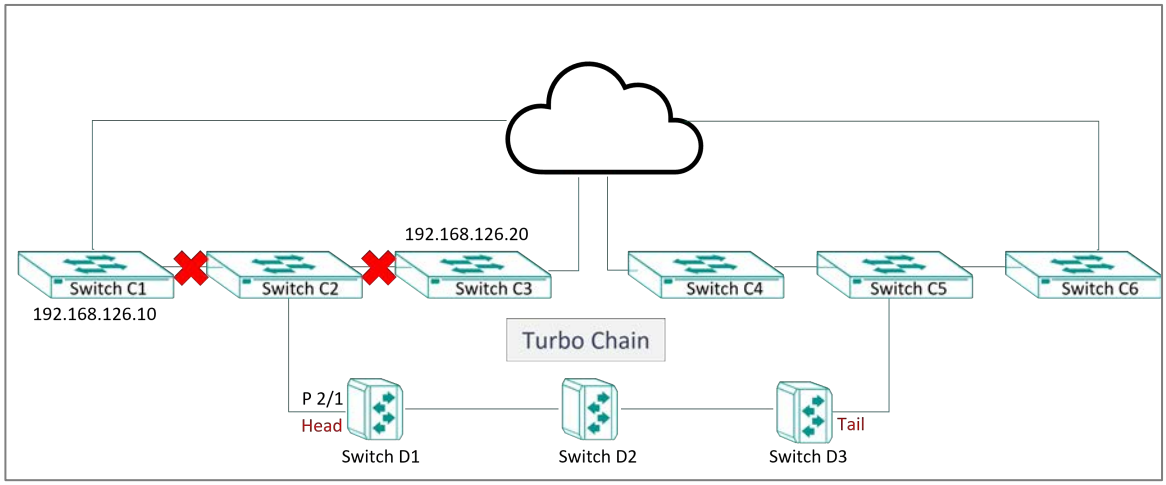
On Switch B1, do the following:

1. Sign in to the device with administrator credentials.
2. Go to **Redundancy** > **Layer 3 Redundancy** > **VRRP**, and then click **Settings**.
3. Click **Edit** next to the corresponding **Virtual Router**.
4. Click **Tracking ID**, and then choose the **Tracking ID** created in the preceding task, and then click **Select**.
5. Specify a **Decrement** of 100, and then click **Apply**.

The tracking entry allows changing to the backup virtual router. If an internet connection is no longer detecting, the **Decrement** value is subtracted from the **Priority** value of the virtual router, causing the backup to take over and restoring the network connection.

Scenario: Configuring Logical Tracking for Turbo Chain

In this example, we will create ping tracking entries on Switch D1 to monitor traffic by pinging two different target IP addresses. We will then combine these tracking entries by using a logical tracking entry, and use the logical tracking entry to control a port.



This task presumes that Turbo Chain has already been configured inline with the above scenario. Refer to About Turbo Chain for information about configuring Turbo Chain.

Configure all of the following on Switch D1:

1. Enable Tracking.
2. Create the Ping Tracking Entries targeting Switches C1 and C3.
3. Create Logical Tracking Entries using the Ping Tracking Entries.
4. Assign the Tracking ID to the Port from **Port Interface**.

Example: Enabling Tracking

Turn on tracking to allow the system to monitor interfaces and trigger redundancy actions.

1. Sign in to the device with administrator credentials.
2. Go to **Redundancy** > **Tracking**.
3. Set **Tracking** to **Enabled**, and then click **Apply**.

Example: Creating Ping Tracking Entries

Create ping tracking entries to monitor IP reachability and support logical tracking for redundancy decisions.

1. Sign in to the device with administrator credentials.
2. Go to **Redundancy** > **Tracking**.

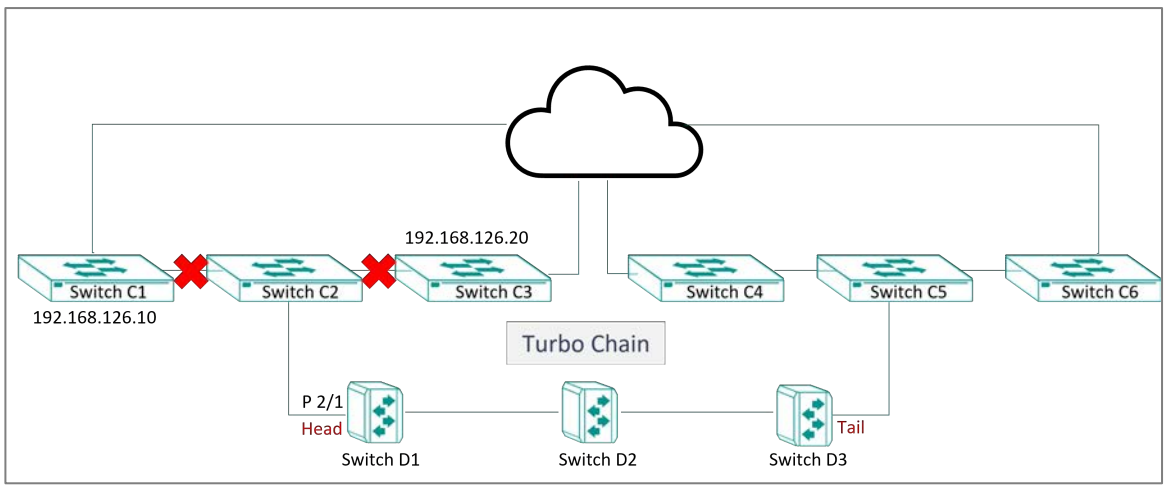
3. Next to **Tracking of...**, click **Select**, choose **Ping**, and then click **Add**.
4. Configure all of the following, and then click **Create**:

Option	Value
Ping Tracking	**Enabled**
Tracking ID	2
IP Address	192.168.126.10

5. Add a second entry by clicking click **Add**, specifying all of the following, and then clicking **Create**:

Option	Value
Ping Tracking	**Enabled**
Tracking ID	3
IP Address	192.168.126.20

These ping tracking entries separately monitor connectivity to C1 and C3.



Continue to create a logical tracking entry, which will combine the two ping tracking entries to determine when switch C2 is completely disconnected. The logical entry can then switch the Turbo Ring tail from blocking to forwarding, rerouting traffic over switch C5.

Example: Creating Logical Tracking Entries for Turbo Chain

Logical Entries are made up of one or more other kinds of tracking entries. These rules can accommodate more complex situations encompassing multiple tracking entries.

To combine the ping tracking entries 2 and 3 you just created:

1. Sign in to the device with administrator credentials.
2. Go to **Redundancy** > **Tracking**.
3. Next to **Tracking of...**, click **Select**, choose **Logical**, and then click **Add**.
4. Configure all of the following, and then click **Create**:

Interface Tracking	**Enabled**
Tracking ID	4
Logical List	Choose **2** and **3**
Logical Operator	**AND**

Continue to assign tracking entries to ports.

Example: Adding Tracking Entries to Ports

Assign the logical tracking entry to a port to enable automatic failover if both routes fail.

Make sure you assigned a **Tracking ID** in the previous task.

On Switch B1, do the following:

1. Sign in to the device with administrator credentials.
2. Go to **Port** > **Port Interface** > **Port Settings**.
3. Next to **Port 2/1**, click **Edit**.
4. Click **Tracking ID**, and then choose the **Tracking ID** created in the preceding task, and then click **Select**.
5. Click **Apply**.

Now that the logical tracking entry has been assigned, if both routes fail, the Turbo Chain tail can be triggered to allow traffic.

Scenario: Configuring Tracking for Static Route

Create an interface tracking entry to monitor an interface, then use that tracking entry to control a static route. Static routes offer fine control over traffic flows, but often suffer from a single point of failure. When coupled with Interface Tracking, static routes can be reconfigured based on network changes, without the complexity or unpredictability of dynamic routing.

This scenario requires a working static route. Refer to Static Routes for details about configuring static routes.

To configure this scenario:

1. Enable tracking.
2. Create an Interface Tracking Entry
3. Assign the Tracking Entry to the Static Route.

Example: Enabling Tracking

Turn on tracking to allow the system to monitor interfaces and trigger redundancy actions.

1. Sign in to the device with administrator credentials.
2. Go to **Redundancy** > **Tracking**.
3. Set **Tracking** to **Enabled**, and then click **Apply**.

Example: Creating an Interface Tracking Entry for a Static Route

Create an interface tracking entry to monitor port status and enable failover actions.

1. Sign in to the device with administrator credentials.
2. Go to **Redundancy** > **Tracking**.
3. Next to **Tracking of...**, click **Select,** choose **Interface**, and then click **Add**.
4. Configure all of the following, and then click **Create**:

Option	Value
Interface Tracking	**Enabled**

Option	Value
Tracking ID	5
Interface Type	**Network Interface**
Network Interface	Select the interface to which the static route is bound

The Interface Tracking Entry appears on the list.

Continue to add the interface tracking entry to the Static Route.

Example: Adding Interface Tracking Entry to a Static Route

Add the tracking entry to a static route to disable the route automatically when connectivity is lost.

Make sure you assigned a **Tracking ID** in the previous task.

1. Sign in to the device with administrator credentials.
2. Go to **Routing** > **Unicast Route** > **Static Routing**.
3. Locate the Static Route to track, and then click **Edit**.
4. Click **Tracking ID**, and then choose the **Tracking ID** created in the preceding task, and then click **Select**.
5. Click **Apply**.

The tracking entry will disable the static route when not available.

Tracking

Menu Path: Redundancy > Tracking

This page lets you manage the status tracking feature of your device.

This page includes these tabs:

- Settings
- Status

Note

This feature supports weaker authentication or encryption, and may not be secure over untrusted networks. Take appropriate security precautions.

Tracking - Settings

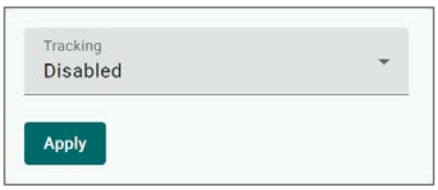
Menu Path: Redundancy > Tracking - Settings

This page lets you create and manage status tracking entries.

Limitations

You can create up to 16 tracking entries across all tracking types. Tracking IDs cannot be shared between entries.

Tracking Settings



UI Setting	Description	Valid Range	Default Value
Tracking	Enable or disable status tracking for the device.	Enabled / Disabled	Disabled

Tracking List of Interface

If **Tracking List of Interface** is selected, this table will appear.



UI Setting	Description
Tracking ID	Shows the tracking ID of the entry.
Status	Shows whether the entry is enabled.
Interface	Shows the interface monitored by the tracking ID.
Down to Up	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.
Up Delay (sec.)	Shows the delay in seconds the interface status must stay up to be detected as a down to up status change.
Up tp Down	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.
Down Delay (sec.)	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 **Create** 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.



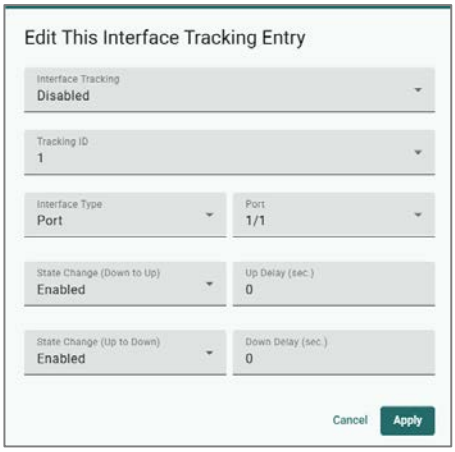
UI Setting	Description	Valid Range	Default Value
Interface Tracking	Enable or disable the interface tracking ID.	Enabled / Disabled	Disabled
Tracking ID	Specify the tracking ID to use for this entry.	Drop-down list of tracking IDs	N/A
Interface Type	Select the interface type to monitor with this entry.	Port / Network Interface	N/A
Port (If Interface Type is Port)	Specify which port to monitor with this entry.	Drop-down list of ports	N/A
Network Interface (If Interface Type is Network Interface)	Specify which network interface to monitor with this entry.	Drop-down list of interfaces	N/A
State Change (Down to Up)	Enable or disable down to up state change with this entry. • **Enabled:** The state for the tracking ID will change to Up when the interface status transitions from down to up. • **Disabled:** The state for the tracking ID will not change when the interface status transitions from down to up.	Enabled / Disabled	Enabled
Up Delay	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
State Change (Up to Down)	Enable or disable up to down state change with this entry. • **Enabled:** The state for the tracking ID will change to Down when the interface status transitions from up to down. • **Disabled:** The state for the tracking ID will not change when the interface status transitions from up to down.	Enabled / Disabled	Enabled
Down Delay	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.



UI Setting	Description	Valid Range	Default Value
Interface Tracking	Enable or disable the interface tracking ID.	Enabled / Disabled	Disabled
Tracking ID	Specify the tracking ID to use for this entry.	Drop-down list of tracking IDs	N/A
Interface Type	Select the interface type to monitor with this entry.	Port / Network Interface	N/A
Port (If Interface Type is Port)	Specify which port to monitor with this entry.	Drop-down list of ports	N/A
Network Interface (If Interface Type is Network Interface)	Specify which network interface to monitor with this entry.	Drop-down list of interfaces	N/A

UI Setting	Description	Valid Range	Default Value
State Change (Down to Up)	Enable or disable down to up state change with this entry. • **Enabled:** The state for the tracking ID will change to Up when the interface status transitions from down to up. • **Disabled:** The state for the tracking ID will not change when the interface status transitions from down to up.	Enabled / Disabled	Enabled
Up Delay	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
State Change (Up to Down)	Enable or disable up to down state change with this entry. • **Enabled:** The state for the tracking ID will change to Down when the interface status transitions from up to down. • **Disabled:** The state for the tracking ID will not change when the interface status transitions from up to down.	Enabled / Disabled	Enabled
Down Delay	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, this table will appear.



UI Setting	Description
Tracking ID	Shows the tracking ID of the entry.
Status	Shows whether the entry is enabled.
IP Address	Shows the IP address monitored by the tracking ID.
Interval (ms)	Shows the interval in milliseconds between state checks for the entry.
Timeout (ms)	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.
Down to Up	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.
Received (packets)	Shows the number of ping response packets that must be received before the status of the IP address changes to up.
Up to Down	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.
Lost (packets)	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 **Create** 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.



UI Setting	Description	Valid Range	Default Value
Ping Tracking	Enable or disable the ping tracking ID.	Enabled / Disabled	Disabled
Tracking ID	Specify the tracking ID to use for this entry.	Drop-down list of Tracking IDs	N/A
IP Address	Specify the IP address to monitor with this entry.	Valid IP address	N/A
Interval	Specify the interval in milliseconds between state checks for the entry.	500 to 100000	1000
Timeout	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 to 100000	1000
State Change (Down to Up)	Enable or disable down to up state change with this entry. • **Enabled:** The state for the tracking ID will change to Up when the IP address status transitions from down to up. • **Disabled:** The state for the tracking ID will not change when the IP address status transitions from down to up.	Enabled / Disabled	Enabled
Received	Specify the number of ping response packets that must be received before the status of the IP address changes to up.	1 to 99	3

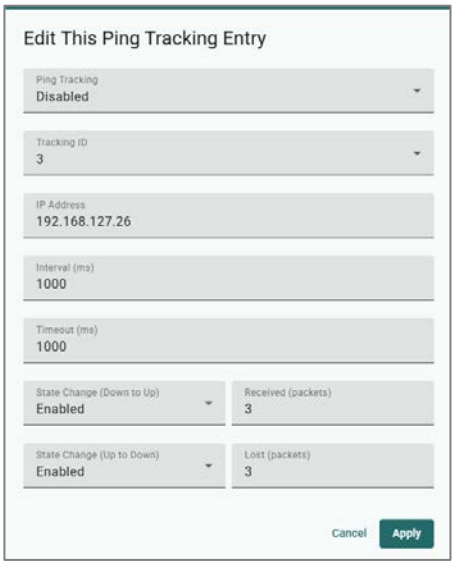
UI Setting	Description	Valid Range	Default Value
State Change (Up to Down)	Enable or disable up to down state change with this entry. • **Enabled:** The state for the tracking ID will change to Down when the IP address status transitions from up to down. • **Disabled:** The state for the tracking ID will not change when the IP address status transitions from up to down.	Enabled / Disabled	Enabled
Lost	Specify the number of ping request packets that must be lost before the status of the IP address changes to down.	1 to 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.



UI Setting	Description	Valid Range	Default Value
Ping Tracking	Enable or disable the ping tracking ID.	Enabled / Disabled	Disabled

UI Setting	Description	Valid Range	Default Value
Tracking ID	Specify the tracking ID to use for this entry.	Drop-down list of Tracking IDs	N/A
IP Address	Specify the IP address to monitor with this entry.	Valid IP address	N/A
Interval	Specify the interval in milliseconds between state checks for the entry.	500 to 100000	1000
Timeout	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 to 100000	1000
State Change (Down to Up)	Enable or disable down to up state change with this entry. • **Enabled:** The state for the tracking ID will change to Up when the IP address status transitions from down to up. • **Disabled:** The state for the tracking ID will not change when the IP address status transitions from down to up.	Enabled / Disabled	Enabled
Received	Specify the number of ping response packets that must be received before the status of the IP address changes to up.	1 to 99	3
State Change (Up to Down)	Enable or disable up to down state change with this entry. • **Enabled:** The state for the tracking ID will change to Down when the IP address status transitions from up to down. • **Disabled:** The state for the tracking ID will not change when the IP address status transitions from up to down.	Enabled / Disabled	Enabled
Lost	Specify the number of ping request packets that must be lost before the status of the IP address changes to down.	1 to 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, this table will appear.



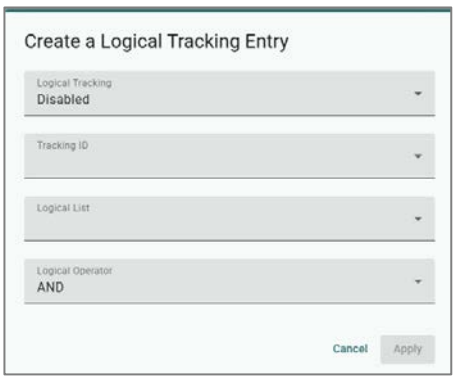
UI Setting	Description
Tracking ID	Shows the tracking ID of the entry.
Status	Shows whether the entry is enabled.
Logical List	Shows the logical rule and the tracking IDs it contains.

Creating a Logical Tracking Entry

Menu Path: Redundancy > Tracking - Settings

Clicking **Create** 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.



UI Setting	Description	Valid Range	Default Value
Logical Tracking	Enable or disable the logical tracking ID.	Enabled / Disabled	Disabled

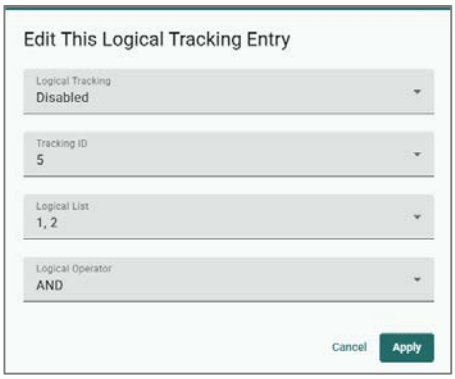
UI Setting	Description	Valid Range	Default Value
Tracking ID	Specify the tracking ID to use for this entry. **Note** The tracking ID for a logical tracking rule must be higher than the tracking IDs used in the logical list for the rule.	Drop-down list of tracking IDs	N/A
Logical List	Specify which tracking IDs you want to monitor for this entry. **Note** You need to set up a tracking ID before you can select it from the list.	Drop-down list of existing tracking IDs	N/A
Logical Operator	Specify how the state of the logical tracking rule should change based on the state of the tracking IDs in the logical list. • **AND**: When all tracking IDs in the logical list are Up, the state will be Up. Otherwise, the state will be Down. • **OR:** If any of the tracking IDs in the logical list are Up, the state will be Up. Otherwise, the state will be Down. • **NAND:** When all tracking IDs in the logical list are Up, the state will be Down. Otherwise, the state will be Up. • **NOR:** If any of the tracking IDs in the logical list are Up, the state will be Down. Otherwise, the state will be Up.	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.



UI Setting	Description	Valid Range	Default Value
Logical Tracking	Enable or disable the logical tracking ID.	Enabled / Disabled	Disabled
Tracking ID	Specify the tracking ID to use for this entry. **Note** The tracking ID for a logical tracking rule must be higher than the tracking IDs used in the logical list for the rule.	Drop-down list of tracking IDs	N/A
Logical List	Specify which tracking IDs you want to monitor for this entry. **Note** You need to set up a tracking ID before you can select it from the list.	Drop-down list of existing tracking IDs	N/A
Logical Operator	Specify how the state of the logical tracking rule should change based on the state of the tracking IDs in the logical list. • **AND**: When all tracking IDs in the logical list are Up, the state will be Up. Otherwise, the state will be Down. • **OR:** If any of the tracking IDs in the logical list are Up, the state will be Up. Otherwise, the state will be Down. • **NAND:** When all tracking IDs in the logical list are Up, the state will be Down. Otherwise, the state will be Up. • **NOR:** If any of the tracking IDs in the logical list are Up, the state will be Down. Otherwise, the state will be Up.	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.

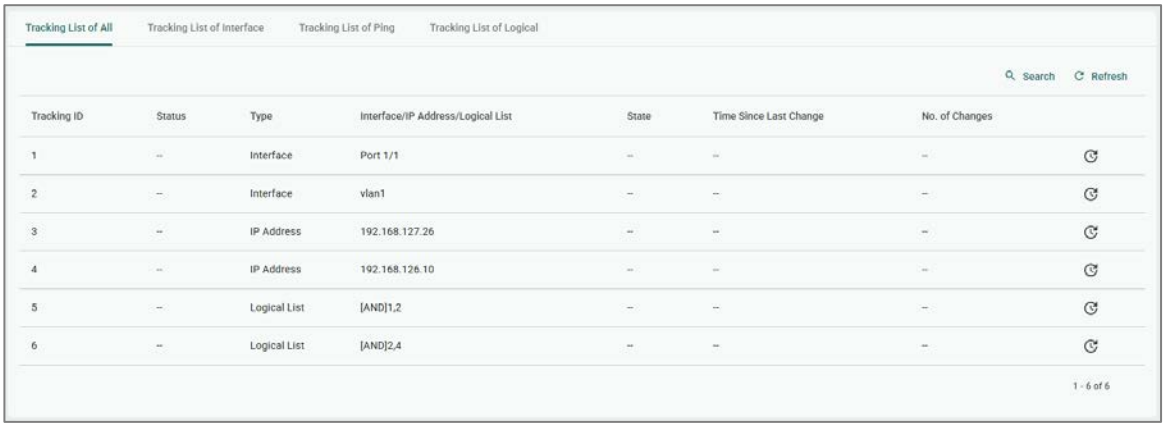
Tracking - Status

Menu Path: Redundancy > Tracking - Status

This page lets you see the status of your tracking entries.

Tracking Status List

You can use the tabs at the top of the table to view all tracking entries, or only tracking entries of a specific type.



UI Setting	Description
Tracking ID	Shows the tracking ID of the entry.
Status	Shows whether the entry is enabled.
Type	Shows the type of the entry.
Interface / IP Address / Logical List	Shows the interface, IP address, logical list this entry is monitoring, based on the entry's type.
State	Shows the current state of the tracking ID.
Time Since Last Change	Shows the time since the last state change for the tracking ID.

UI Setting	Description
No. of Changes	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 (for L2 models)
- DHCP Relay Agent
- DNS Settings

Network Service - User Privileges

Privileges to settings are granted to the different authority levels as follows. Refer to User Accounts for more information on user accounts.

Settings	Admin	Supervisor	User
DHCP Server (for L2 models)	R/W	R/W	R
DHCP Relay Agent	R/W	R/W	R
DNS Settings	R/W	R/W	R

Configuring DHCP Server Functions

Moxa routers and L2 switches support DHCP server functionality, allowing auto-assignment of IP configurations.

Note

This feature supports weaker authentication or encryption, and may not be secure over untrusted networks. Take appropriate security precautions.

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.

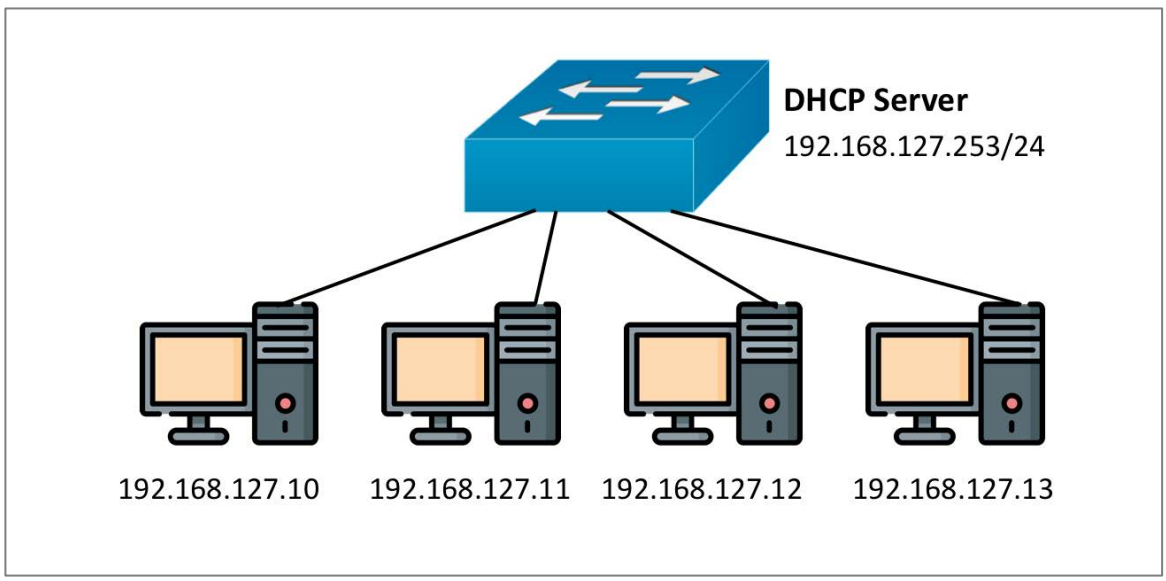
Port-based IP Assignment

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
Starting IP Address	192.168.127.10
Subnet Mask	**24 (255.255.255.0)**
Ending IP Address	192.168.127.20
Default Gateway	192.168.127.253
Lease Time	1440
DNS Server IP Address 1	8.8.8.8
DNS Server IP Address 2	8.8.8.4
NTP Server IP Address	8.8.8.10

6. Click **Apply** to save your settings.

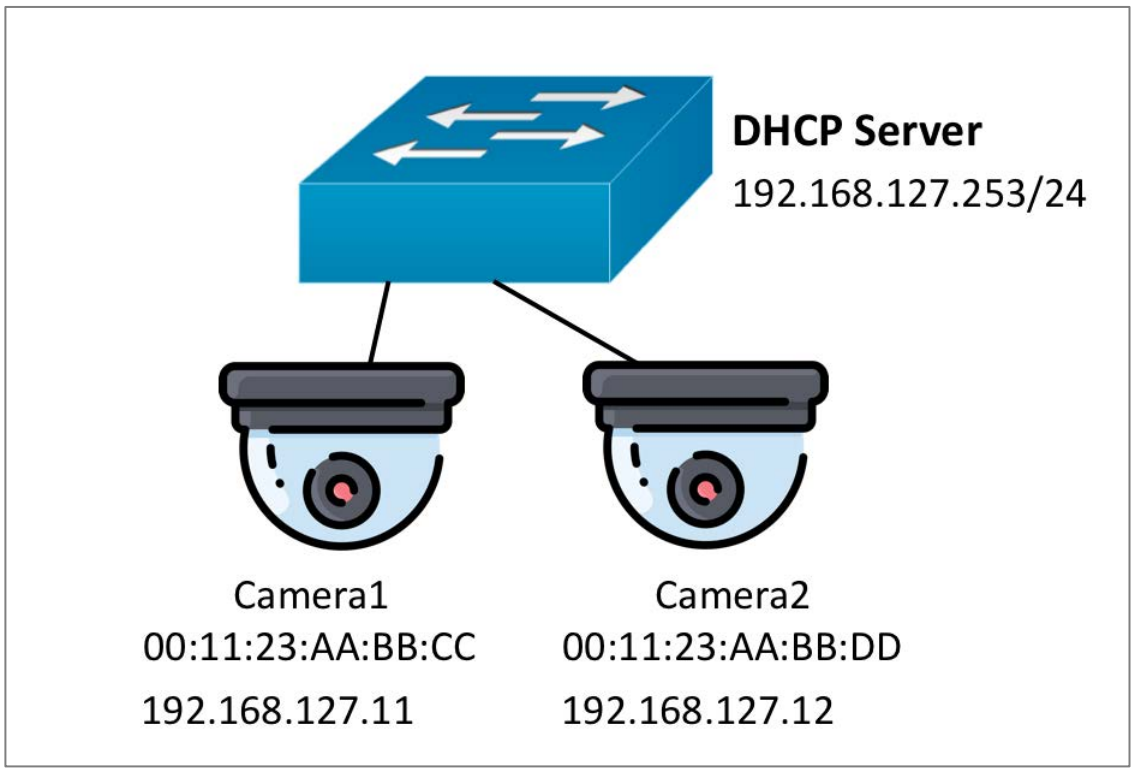
Note

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
Enable	**Enabled**
Hostname	Camera1
IP Address	192.168.127.11
Subnet Mask	**24 (255.255.255.0)**

Option	Value
MAC Address	00:11:23:AA:BB:CC
Default Gateway	192.168.127.253
Lease Time	1440
DNS Server IP Address1	8.8.8.8
DNS Server IP Address1	8.8.8.4
NTP Server IP Address	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
Enable	**Enabled**
Hostname	Camera2
IP Address	192.168.127.12
Subnet Mask	**24 (255.255.255.0)**
MAC Address	00:11:23:AA:BB:CC
Default Gateway	192.168.127.253
Lease Time	1440
DNS Server IP Address1	8.8.8.8
DNS Server IP Address1	8.8.8.4
NTP Server IP Address	8.8.8.10

The entry will appear in the table.

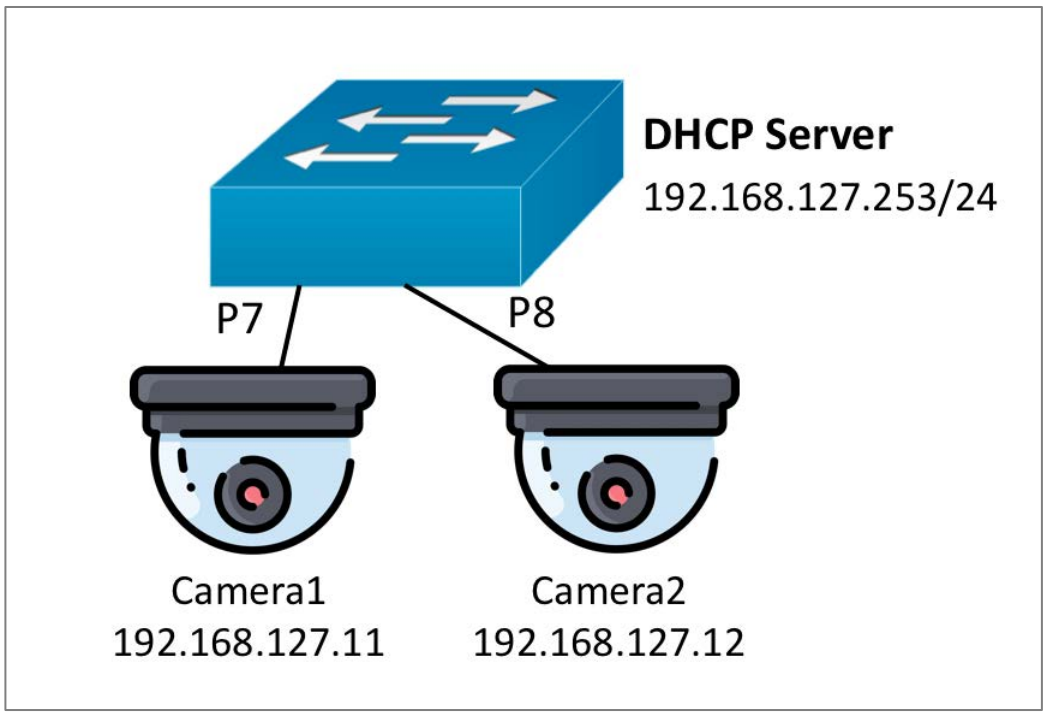
Note

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
Enable	**Enabled**
Port	**7**
IP Address	192.168.127.11
Subnet Mask	**24 (255.255.255.0)**
Default Gateway	192.168.127.253
Lease Time	1440
DNS Server IP Address1	8.8.8.8
DNS Server IP Address1	8.8.8.4
NTP Server IP Address	8.8.8.10
Hostname	Camera1

The entry will appear in the table.

6. Repeat this process for the second camera, with the following settings:

Option	Value
Enable	**Enabled**
MAC Address	00:11:23:AA:BB:CC
IP Address	192.168.127.12
Subnet Mask	**24 (255.255.255.0)**
Default Gateway	192.168.127.253
Lease Time	1440
DNS Server IP Address1	8.8.8.8
DNS Server IP Address1	8.8.8.4

Option	Value
NTP Server IP Address	8.8.8.10
Hostname	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

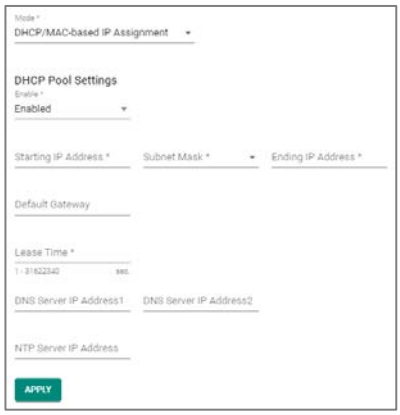
This page lets you configure the DHCP server mode and port settings.

Limitations

You can create up to 256 DHCP/MAC-based IP assignments.

DHCP Server Settings - DHCP / MAC-based IP Assignment

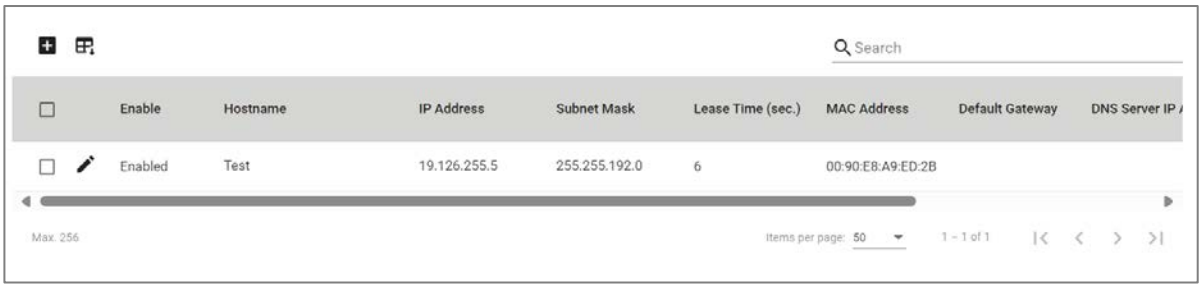
If **Mode** is set to **DHCP / MAC-based IP Assignment**, and **DHCP Pool Settings** is **Enabled**, these settings will appear.



UI Setting	Description	Valid Range	Default Value
Mode	Select a DHCP server mode.	Disabled / DHCP/MAC-based IP Assignment / Port-based IP Assignment	Disabled
Enable	Enable or disable use of a DHCP pool.	Enabled / Disabled	Disabled
Starting IP Address	Specify the starting IP address of the DHCP IP pool.	Valid unicast IP address	N/A
Subnet Mask	Specify the subnet mask for DHCP clients in the pool.	Valid subnet mask	N/A
Ending IP Address	Specify the ending IP address of the DHCP IP pool.	Valid unicast IP address	N/A
Default Gateway	Specify the default gateway to use for DHCP clients in the pool.	Valid IP address	N/A
Lease Time	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
DNS Server IP Address1	Specify the IP address of the first DNS server to use for DHCP clients in the pool.	Valid IP address	N/A
DNS Server IP Address2	Specify the IP address of the second DNS server to use for DHCP clients in the pool.	Valid IP address	N/A
NTP Server IP Address	Specify the IP address of the NTP server to use for DHCP clients in the pool.	Valid IP address	N/A

DHCP Server List - DHCP/MAC-based Assignment

If **DHCP Server Mode** is set to **DHCP/MAC-based IP Assignment**, this table will appear.



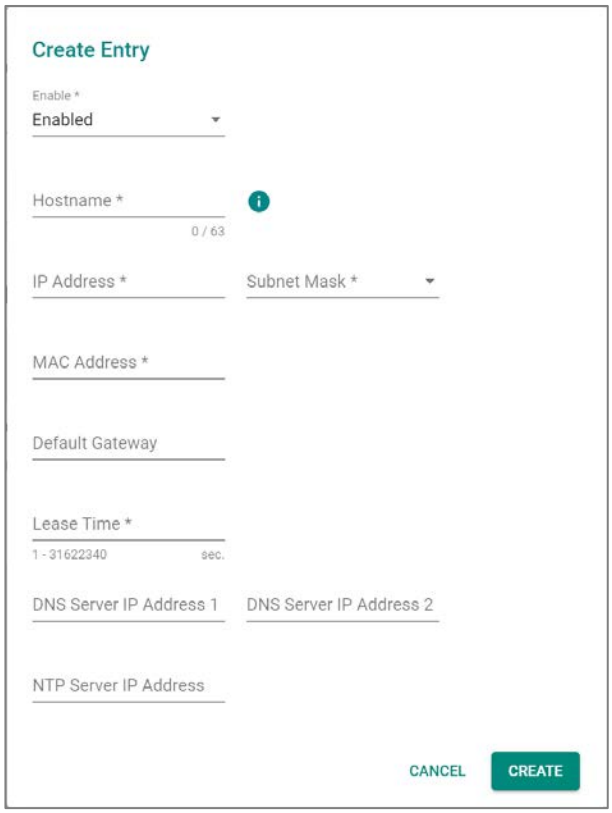
UI Setting	Description
Enable	Shows whether MAC-based IP assignment is enabled for the MAC address.
Hostname	Shows the hostname to use for clients that connect to the MAC address.
IP Address	Shows the IP address assigned to clients that connect to the MAC address.
Subnet Mask	Shows the subnet mask assigned to clients that connect to the MAC address.
Lease Time (sec.)	Shows the lease time in seconds for IP assignments through the MAC address.
MAC Address	Shows the MAC address of the MAC-based IP assignment.
Default Gateway	Shows the default gateway for clients that connect to the MAC address.
DNS Server IP Address 1	Shows the IP address of the first DNS server to use for clients that connect to the MAC address.
DNS Server IP Address 2	Shows the IP address of the second DNS server to use for clients that connect to the MAC address.
NTP Server IP Address	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 **Create** on the **Network Service > DHCP Server - General** page when **Mode** is set to **DHCP/MAC-based IP Assignment** will open this dialog box. This dialog lets you create a new entry.

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



UI Setting	Description	Valid Range	Default Value
Enable	Enable or disable the MAC-based IP assignment entry.	Enabled / Disabled	Enabled
Hostname	Specify a hostname for the IP assignment.	Drop-down list of ports	N/A
IP Address	Specify the IP address for the IP assignment.	Valid IP address	N/A
Subnet Mask	Select the subnet mask for the IP assignment.	Drop-down list of subnet masks	N/A
MAC Address	Specify the MAC address that this IP assignment will apply to.	Valid MAC address	
Default Gateway	Specify the default gateway for the IP assignment.	Valid IP address	N/A
Lease Time	Specify the lease time in seconds for the IP assignment.	1 to 31622340	

UI Setting	Description	Valid Range	Default Value
DNS Server IP Address1	Specify the IP address of the first DNS server to use for the IP assignment.	Valid IP address	N/A
DNS Server IP Address2	Specify the IP address of the second DNS server to use for the IP assignment.	Valid IP address	N/A
NTP Server IP Address	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.



UI Setting	Description
Port	Shows the port number the entry is for.
Enable	Shows whether port-based IP assignment is enabled for the port.
IP Address	Shows the IP address assigned to clients that connect to the port.
Subnet Mask	Shows the subnet mask assigned to clients that connect to the port.
Lease Time (sec.)	Shows the lease time in seconds for IP assignments through the port.
Default Gateway	Shows the default gateway for clients that connect to the port.
DNS Server IP Address 1	Shows the IP address of the first DNS server to use for clients that connect to the port.
DNS Server IP Address 2	Shows the IP address of the second DNS server to use for clients that connect to the port.
NTP Server IP Address	Shows the NTP server to use for clients that connect to the port.
Hostname	Shows the hostname to use for clients that connect to the port.

UI Setting	Description
Domain Name	Shows the domain name to use for clients that connect to the port.
Log Server IP Address	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 **Create** on the **Network Service > DHCP Server - General** page when **Mode** is set to **Port-based IP Assignment** will open this dialog box. This dialog lets you create a new entry.

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



UI Setting	Description	Valid Range	Default Value
Enable	Enable or disable the port-based IP assignment entry.	Enabled / Disabled	Enabled
Port	Select which port the DHCP server will assign an IP address for.	Drop-down list of ports	N/A
IP Address	Specify the IP address assigned to clients that connect to the port.	Valid IP address	N/A
Subnet Mask	Select the subnet mask assigned to clients that connect to the port.	Drop-down list of subnet masks	N/A

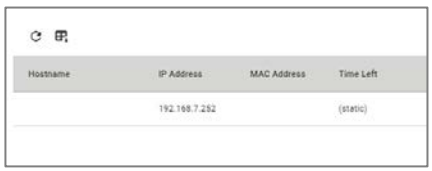
UI Setting	Description	Valid Range	Default Value
Lease Time	Specify the lease time in seconds for IP assignments through the port.	1 to 31622340	N/A
Default Gateway	Specify the default gateway for clients that connect to the port.	Valid IP address	N/A
DNS Server IP Address1	Specify the IP address of the first DNS server to use for clients that connect to the port.	Valid IP address	N/A
DNS Server IP Address2	Specify the IP address of the second DNS server to use for clients that connect to the port.	Valid IP address	N/A
NTP Server IP Address	Specify the NTP server to use for clients that connect to the port.	Valid IP address	N/A
Hostname	Specify the hostname to use for clients that connect to the port.	Up to 63 characters	N/A
Domain Name	Specify the domain name to use for clients that connect to the port.	Up to 63 characters	N/A
Log Server IP Address	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



UI Setting	Description
Hostname	Shows the hostname of the client.
IP Address	Shows the IP address leased to the client.

UI Setting	Description
MAC Address	Shows the MAC address of the client.
Time left	Shows the amount of time left in seconds on the DHCP lease for the client. **(static)** 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.

Note

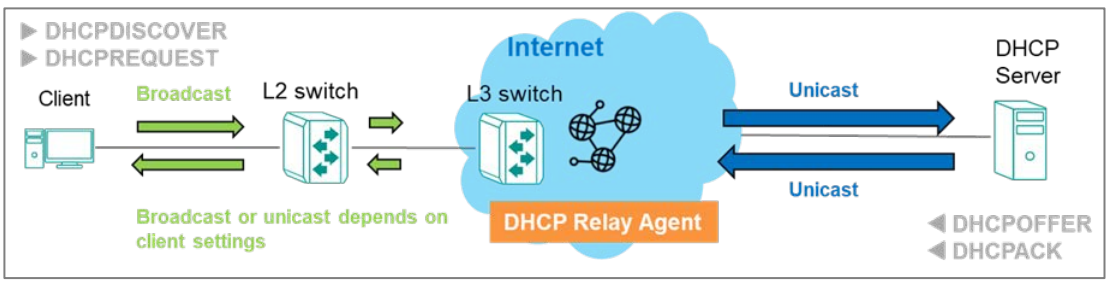
This feature supports weaker authentication or encryption, and may not be secure over untrusted networks. Take appropriate security precautions.

About DHCP Relay Agents

DHCP relay agents can provide a bridge for DHCP communication across network segments.

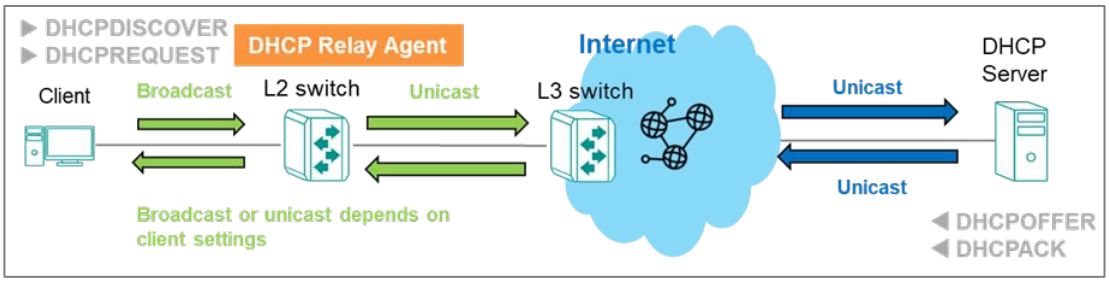
DHCP Relays on L3 Switches

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
Relay	To enable the relay, choose **Enabled**. To disable the relay while retaining settings, choose **Disabled**.
Status	To accept incoming DHCP packets from DHCP servers, choose **Trusted** 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 a 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



UI Setting	Description	Valid Range	Default Value
DHCP Relay Agent	Enable or disable the DHCP Relay Agent feature on your device.	Enabled / Disabled	Disabled
1st / 2nd / 3rd / 4th Server IP Address	Specify the 1st, 2nd, 3rd, and 4th server IP address.	Valid IP address	N/A

DHCP Relay Agent - Port List



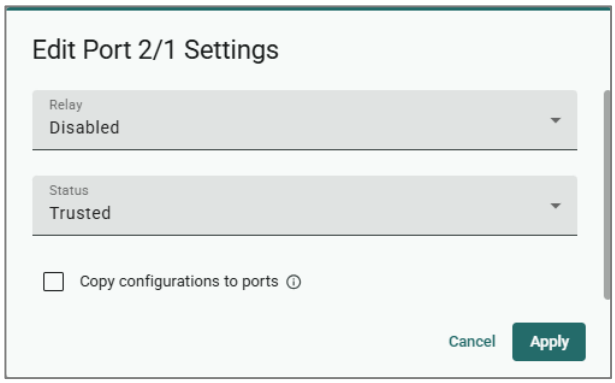
UI Setting	Description
Port	Shows the port number the entry is for.
Relay	Shows whether the relay function is enabled for the port.
Status	Shows the status of the relay on the port.

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
Relay	Enable or disable the relay function for the port.	Enabled / Disabled	Disabled
Status	Specify the relay status for the port. • **Trusted**: DHCP packets with Option 82 or with a non-zero gateway IP address (GIADDR) will be accepted. • **Untrusted**: DHCP packets with Option 82 or with a non-zero gateway IP address (GIADDR) will be discarded.	Trusted / Untrusted	Trusted

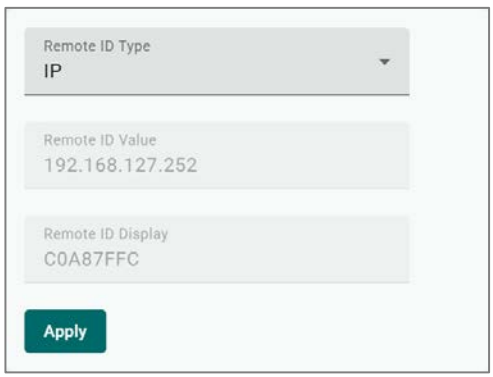
UI Setting	Description	Valid Range	Default Value
Copy configurations to ports	Select the ports you want to copy this configuration to.	Drop-down list of ports	N/A

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



UI Setting	Description	Valid Range	Default Value
Remote ID Type	Specify the remote ID type.	IP / MAC / Client ID / Other	IP
Remote ID Value	If the **Remote ID Type** is **Other**, specify the remote ID value to use. For all other types, this shows the remote ID value for the selected remote ID type and cannot be edited.	Other: 1 to 64 characters All other settings: N/A	IP: • For L2 devices: Device system IP • For L3 devices: First IP in the system MAC: MAC address of the device Client ID: moxa Other: moxa-dhcp-relay

UI Setting	Description	Valid Range	Default Value
Remote ID Display	Shows the remote ID generated from the Remote ID Value. This field is read-only and cannot be changed.	N/A	N/A

Option 82 - Port List



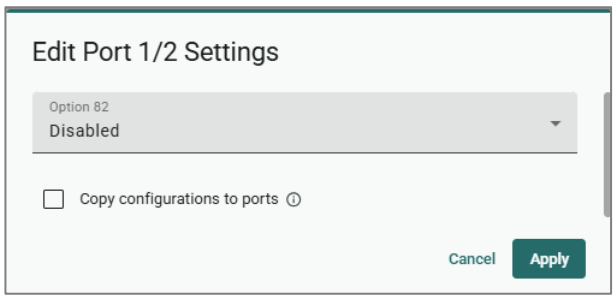
UI Setting	Description
Port	Shows the port number the entry is for.
Option 82	Shows whether Option 82 is enabled for the port.

Option 82 - Edit Port Settings

Menu Path: Network Service > DHCP Relay Agent - Option 82

Clicking the **Edit (✎)** icon for a 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
Option 82	Enable or disable Option 82 for the port.	Enabled / Disabled	Disabled
Copy configurations to ports	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.

> **Note**
>
> This feature supports weaker authentication or encryption, and may not be secure over untrusted networks. Take appropriate security precautions.

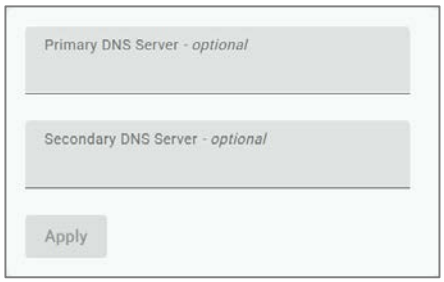
DNS Settings

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



UI Setting	Description	Valid Range	Default Value
Primary DNS Server	Specify the IP address of the primary DNS server used by your network.	Valid IP address	N/A
Secondary DNS Server	Specify the IP address of the secondary DNS server used by your network. The device 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 User Accounts for more information on user accounts.

Settings	Admin	Supervisor	User
Unicast Route			
Static Routing	R/W	R/W	R
RIP	R/W	R/W	R
OSPF	R/W	R/W	R
Routing Table	R	R	R
Multicast Route			
PIM-DM	R/W	R/W	R
PIM-SM	R/W	R/W	R
Multicast Local Route	R/W	R/W	R
Multicast Routing Table	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 unicast 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.

Limitations

You can create up to 256 unicast static routes.

Static Route List



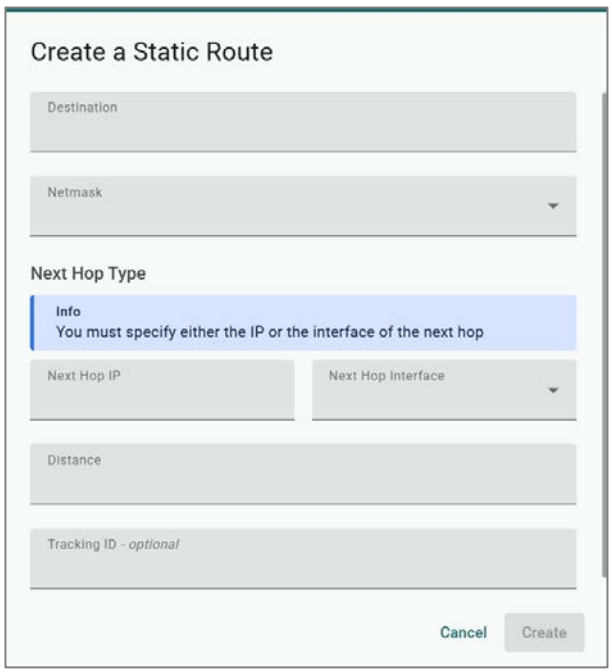
UI Setting	Description
Destination	Shows the destination IP address for the static route.
Netmask	Shows the subnet mask for the destination IP address.
Next Hop IP	Shows the next hop IP on the path to the destination IP address.
Next Hop Interface	Shows the next hop interface on the path to the destination IP address.
Distance	Shows the distance value used to determine the priority of the static route. Lower values have higher priority.
Tracking ID	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 **Create** 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.



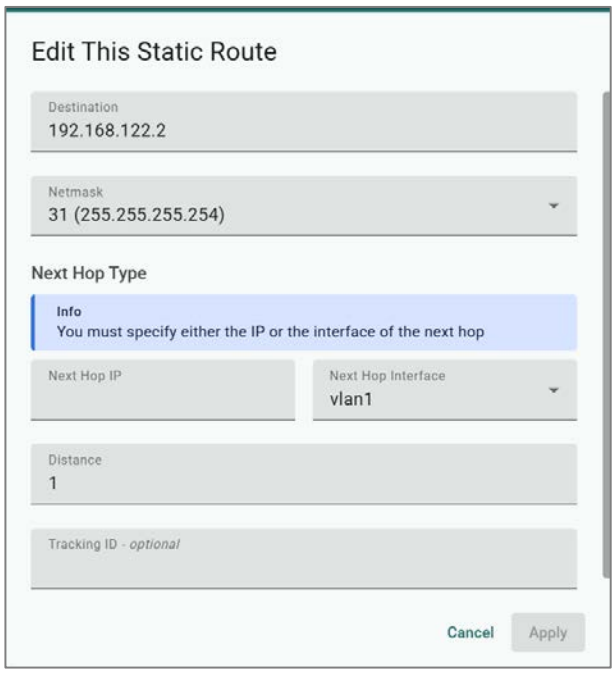
UI Setting	Description	Valid Range	Default Value
Destination	Specify the destination IP address for the static route.	Valid IP address	N/A
Netmask	Specify the subnet mask for the destination IP address.	Drop-down list of subnet masks	N/A
Next Hop IP	Specify the next hop on the path to the destination IP.	Valid IP address	N/A
Next Hop Interface	Select an interface to use for the next hop, or leave this field blank.	Drop-down list of interfaces	N/A
Distance	Specify the distance value to determine the priority of the static route. Lower values have higher priority.	1 to 255	N/A
Tracking ID	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. **Note** You need to create a tracking ID before you can select it. Refer to Tracking for more information.	List of existing tracking IDs	N/A

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.



UI Setting	Description	Valid Range	Default Value
Destination	Specify the destination IP address for the static route.	Valid IP address	N/A
Netmask	Specify the subnet mask for the destination IP address.	Drop-down list of subnet masks	N/A
Next Hop IP	Specify the next hop on the path to the destination IP.	Valid IP address	N/A
Next Hop Interface	Select an interface to use for the next hop, or leave this field blank.	Drop-down list of interfaces	N/A
Distance	Specify the distance value to determine the priority of the static route. Lower values have higher priority.	1 to 255	N/A
Tracking ID	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. **Note** You need to create a tracking ID before you can select it. Refer to Tracking for more information.	List of existing tracking IDs	N/A

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 **Delete**.



RIP

Menu Path: Routing > Unicast Route > RIP

This page lets you manage use of Routing Information Protocol (RIP) for your device.

> **Note**
> This feature supports weaker authentication or encryption, and may not be secure over untrusted networks. Take appropriate security precautions.

About RIP

RIP (Routing Information Protocol) is a dynamic unicast routing protocol that shares information between routers to commute the best routes.

RIP determines optimal routes by counting the number of "hops" or network transitions between networks, and chooses the shortest one. Devices using RIP share routing tables with their neighbours, allowing for mutual updating. This sharing-updating model makes RIP particularly easy to configure.

RIP has two versions:

- v1: Uses classed addressing. Subnet masks are assigned based on the class of IP address. v1 uses unicast updates.
- v2: Uses classless addressing. This makes it able to set arbitrary subnet masks. It uses multicast for table updates, allowing potentially faster propagation.

Both versions of RIP may have slower convergence than other methods, and support a maximum of 15 hops. These limitations make RIP best suited to smaller or less complex networks. For large networks, or networks requiring more than 15 hops, consider routing protocols like OSPF instead.

Enabling RIP

RIP must be enabled on the device before it can be enabled on interfaces.

When designing the network, ensure the hop count does not exceed 15. RIP considers any route with a hop count of 16 or more as unreachable.

To enable RIP:

1. Sign in to the device with administrator credentials.
2. Go to **Routing** > **Unicast Route** > **RIP**.
3. Configure all of the following.

Option	Value
RIP	Choose **Enabled**.
Version	For **RIP**: **Enabled**, choose a protocol version. The default and recommended option is **v2**.**v1**: Uses classful routing. Assigns network addresses to specific classes. Determines subnet masks by network address class. **v2**: Uses classless routing. Assigns network addresses flexibly. Specifies subnet masks independently of network address class.
Static	When **Enabled**, entries set in a static route will be re-distributed. Default: **Disabled**.
Connected	When **Enabled**, entries learned from directly connected interfaces will be re-distributed. Default: **Disabled**.
OSPF	When **Enabled**, entries learned from the OSPF will be re-distributed. Default: **Disabled**.

Note

Redistribution in RIP refers to the process of importing routing information from other routing protocols into the RIP routing table, allowing for interconnectivity between different protocols and complex networks.

4. Select **Apply** to save your changes.

Once enabled globally, continue to configure RIP on required interfaces.

Configuring RIP on Interfaces

RIP must be configured on each interface where it will be used.

- Ensure **RIP** is set to **Enabled**, and that you have chosen a protocol version.
- Configure interfaces before proceeding. Unconfigured interfaces do not appear on **RIP Interface Settings**.

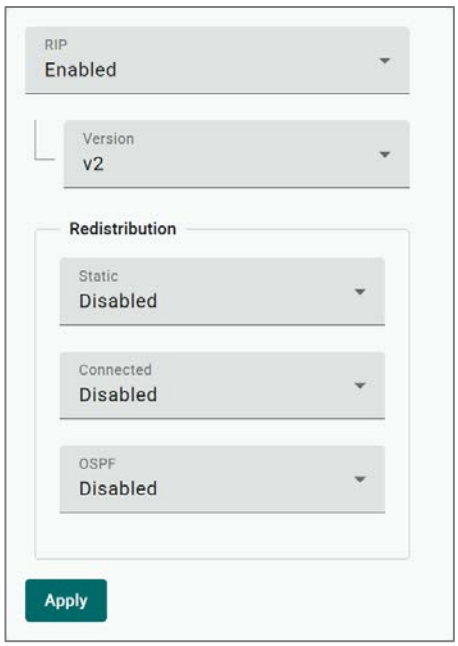
To configure RIP on an interface:

1. Sign in to the device with administrator credentials.
2. Go to **Routing** > **Unicast Route** > **RIP**.
3. On **RIP Interface Settings**, find the interface to configure and select the corresponding **[Edit]**.

   The **Edit RIP Interface Settings** screen appears.
4. Set **RIP** to **Enabled**, and then select **Apply**.

RIP is now configured on selected interfaces. Repeat this task as many times as required to deploy RIP to all interfaces.

RIP Settings



UI Setting	Description	Valid Range	Default Value
RIP	Enable or disable use of RIP for the device.	Enabled / Disabled	Disabled
Version	Select which version of RIP to use. • **v1**: Uses classful routing. Assigns network addresses to specific classes. Determines subnet masks by network address class. • **v2**: Uses classless routing. Assigns network addresses flexibly. Specifies subnet masks independently of network address class.	v1 / v2	v2
Static	Enable or disable static redistribution. When enabled, entries set in a static route will be re-distributed.	Enabled / Disabled	Disabled
Connected	Enable or disable connected redistribution. When enabled, entries learned from directly connected interfaces will be re-distributed.	Enabled / Disabled	Disabled
OSPF	Enable or disable OSPF redistribution. When enabled, entries learned from OSPF will be re-distributed.	Enabled / Disabled	Disabled

RIP Interface Settings



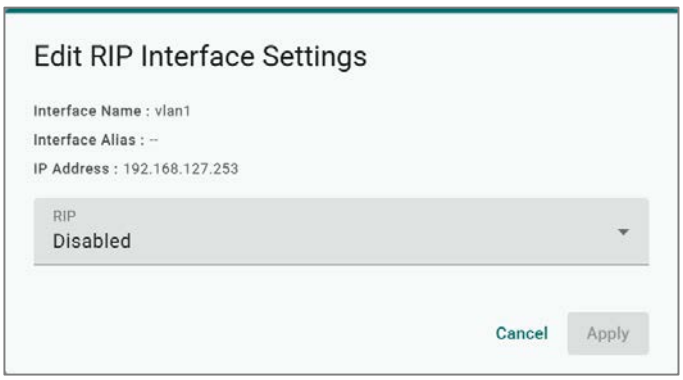
UI Setting	Description
Interface Name	Shows the name of the interface.
Interface Alias	Shows the alias of the interface.
IP Address	Shows the IP address of the interface.
RIP	Shows whether RIP is enabled for the interface.

Edit RIP Interface Settings

Menu Path: Routing > Unicast Route > RIP

Clicking the **Edit (✎)** icon for an interface on the **Routing > Unicast Route > RIP** page will open this dialog box. This dialog lets you edit the RIP settings for the interface.

Click **Apply** to save your changes.



UI Setting	Description	Valid Range	Default Value
RIP	Enable or disable RIP for the interface.	Enabled / Disabled	Disabled

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 - Settings

This page lets you configure OSPF for your device.

This page includes these tabs:

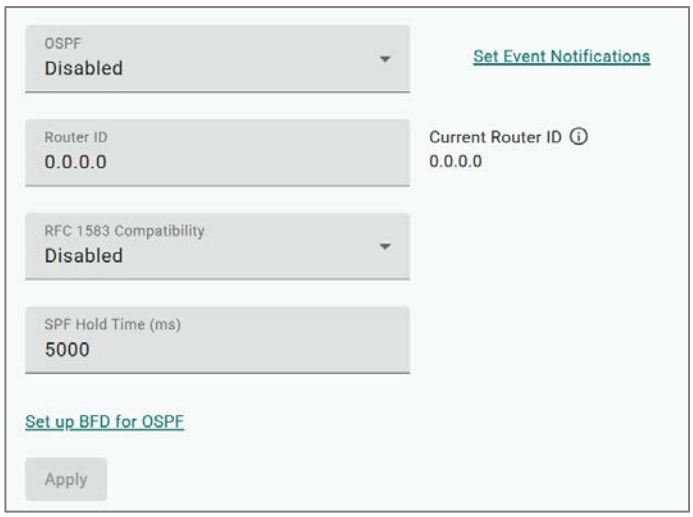
- General
- Area
- Interface
- Neighbor
- Aggregation
- Virtual Link

OSPF Settings - General

Menu Path: Routing > Unicast Route > OSPF - Settings - General

This page lets you configure OSPF general settings.

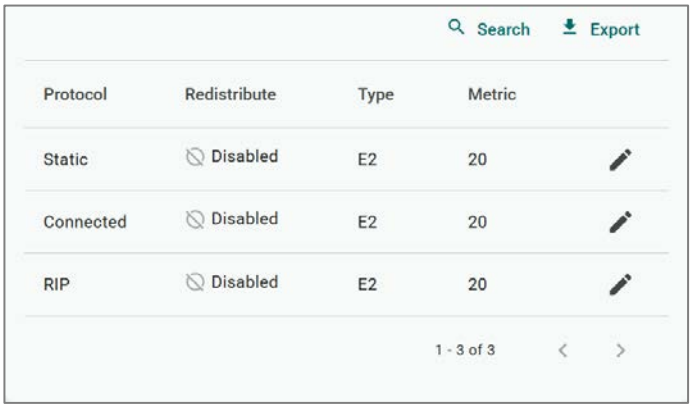
OSPF Settings - General



UI Setting	Description	Valid Range	Default Value
OSPF	Enable or disable OSPF for your device.	Enabled / Disabled	Disabled
Router ID	Specify the router ID for your device. **Note** 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.	Router ID	0.0.0.0
Current Router ID **(View-only)**	Shows the current router ID of your device. **Note** When the Router ID is set to 0.0.0.0, the Current Router ID will automatically use the lowest interface IP address.	Current Router ID	0.0.0.0

UI Setting	Description	Valid Range	Default Value
RFC 1583 Compatibility **(Only in Advanced Mode)**	Enable or disable compatibility with RFC 1583.	Enabled / Disabled	Disabled
SPF Hold Time (ms) **(Only in Advanced Mode)**	Specify the SPF hold time in milliseconds.	0 to 65535	5000

OSPF Protocol List



UI Setting	Description
Protocol	Shows the OSPF protocol the entry is for.
Redistribute	Shows whether redistribution is enabled for the protocol.
Type	Shows the metric type used for routes to be redistributed.
Metric	Shows the metric value used for routes to be redistributed.

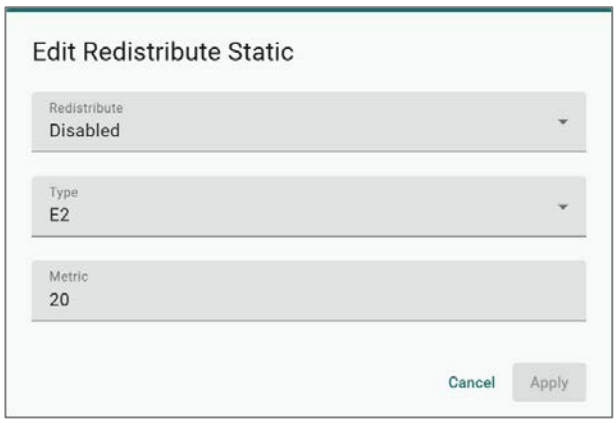
Editing Redistribute Settings

Menu Path: Routing > Unicast Route > OSPF - Settings - General

Clicking the **Edit (✎)** icon for a protocol on the **Routing > Unicast Route > 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.



UI Setting	Description	Valid Range	Default Value
Redistribute	Enable or disable redistribution for the protocol.	Enabled / Disabled	Enabled
Type **(Only in Advanced Mode)**	Select the metric type applied to the routes to be redistributed.	E1/ E2	E2
Metric **(Only in Advanced Mode)**	Specirfy the metric value for the routes to be redistributed into OSPF.	1 to 16777214	20

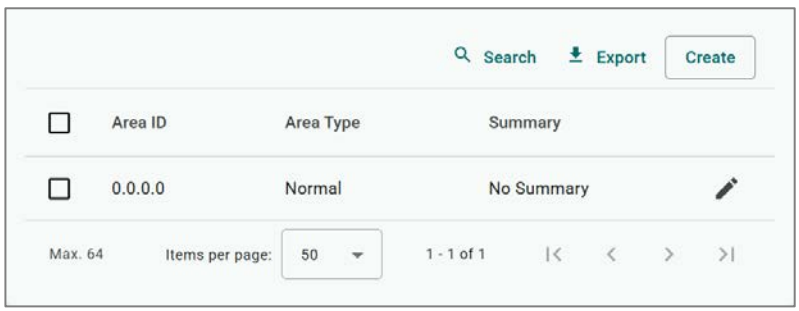
OSPF Settings - Area

Menu Path: Routing > Unicast Route > OSPF - Settings - Area

This page lets you configure OSPF area settings.

Limitations

You can create up to 64 OSPF areas.



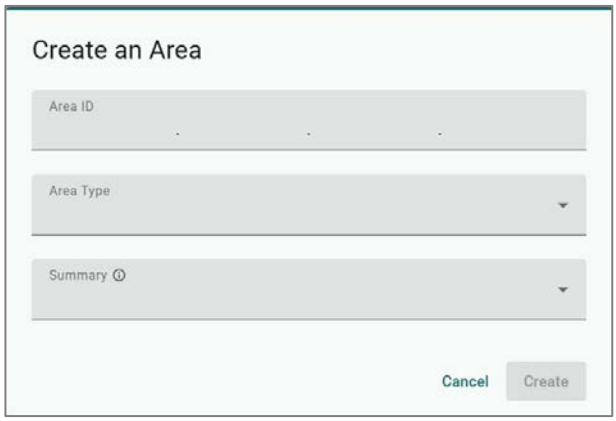
UI Setting	Description
Area ID	Shows the area ID for the area.
Area Type	Shows the type of the area.
Summary	Shows the summary of the area.

Creating an OSPF Area

Menu Path: Routing > Unicast Route > OSPF - Settings - Area

Clicking **Create** on the **Routing > Unicast Route > OSPF - Settings - Area** page will open this dialog box. This dialog lets you add a new OSPF area.

Click **Create** to save your changes.



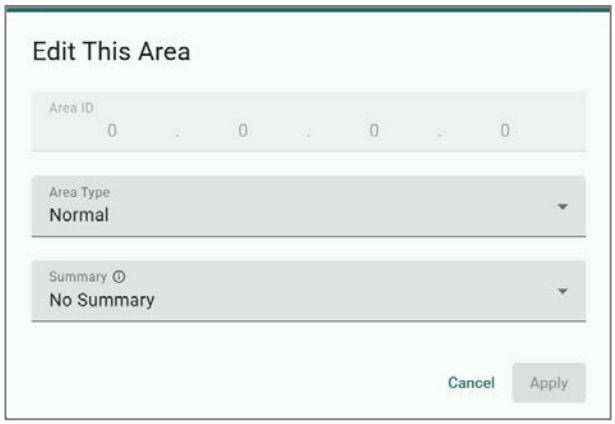
UI Setting	Description	Valid Range	Default Value
Area ID	Specify the area ID for the new area.	0.0.0.0 to 255.255.255.255	0.0.0.0
Area Type	Select the area type to use.	Normal / Stub / NSSA	N/A
Summary	Select whether to include a summary for the area or not. **Note** A summary will not be used if the Area Type is Normal.	Summary / No Summary	N/A

Editing an OSPF Area

Menu Path: Routing > Unicast Route > OSPF - Settings - Area

Clicking the **Edit (✎)** icon for an OSPF area on the **Routing > Unicast Route > 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.



UI Setting	Description	Valid Range	Default Value
Area ID (View-only)	Shows the area ID. This value cannot be changed.	N/A	N/A
Area Type	Select the area type to use.	Normal / Stub / NSSA	N/A
Summary	Select whether to include a summary for the area or not. **Note** A summary will not be used if the Area Type is Normal.	Summary / No Summary	N/A

Deleting an Area

Menu Path: Routing > Unicast Route > 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 - Settings - Interface

This page lets you configure OSPF interface settings.

OSPF Interface List



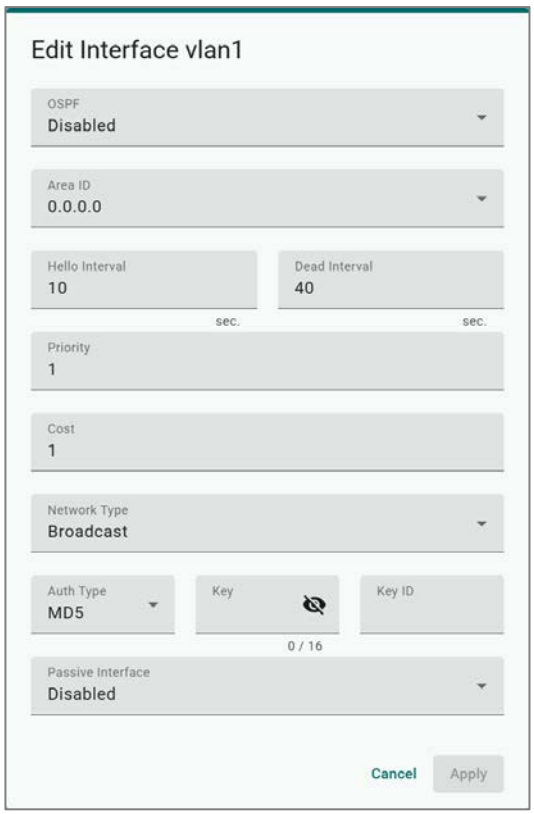
UI Setting	Description
Interface Name	Shows the name of the interface this entry is for.
Interface Alias	Shows the alias for the interface.
IP Address	Shows the IP address for the interface.
OSPF	Shows whether OSPF is enabled for the interface.
Area ID	Shows the area ID for the interface.
Hello Interval (sec.)	Shows the hello packet send interval in seconds for the interface.
Dead Interval (sec.)	Shows the dead interval in seconds for the interface.
Priority	Shows the L3 priority for the interface.
Cost	Shows the cost for the interface. Lower values mean higher priority.
Network Type **(Only in Advanced Mode)**	Shows the network type assigned to the interface to determine how hello packets will be sent.
Auth Type	Shows the OSPF authentication type used for the interface.
Key ID	Shows the OSPF authentication key ID used for the interface.
Passive Mode **(Only in Advanced Mode)**	Shows whether passive mode is enabled for the interface.

Editing an OSPF Interface

Menu Path: Routing > Unicast Route > OSPF - Settings - Interface

Clicking the **Edit (✎)** icon for an interface on the **Routing > Unicast Route > 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.



UI Setting	Description	Valid Range	Default Value
OSPF	Enable or disable the OSPF function for the interface.	Enabled/ Disabled	Disabled
Area ID	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
Hello Interval	Specify the hello packet send interval in seconds. Hello packets are packets sent to OSPF neighbors to maintain connectivity with those neighbors. **Note** The value of all hello intervals must be the same within a network.	1 to 65535	10
Dead Interval	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. **Note** The dead interval is often set as four times the hello interval.	1 to 65535	40
Priority	Specify the L3 priority for the interface. Higher values mean higher priority to be selected as the designated router.	0 to 255	1
Cost	Specify cost for the interface. Lower values mean higher priority.	1 to 65535	1
Network Type **(Only in Advanced Mode)**	Select the network type for the interface to determine how hello packets will be sent. **Note** When the network type is set to Non-broadcast or Point-to-multipoint, you will need to add a neighbor manually.	Broadcast / Non-broadcast / Point-to-multipoint / Point-to-point	Broadcast
Auth Type	Specify the OSPF authentication type to use when authenticating OSPF neighbors, or select **None** for no authentication. **Note** If OSPF authentication is used, all L3 switches and routers on the same segment must use the same authentication method and key.	None / Simple / MD5 / SHA1 / SHA-224 / SHA-256 / SHA-385 / SHA-512	N/A

UI Setting	Description	Valid Range	Default Value
Key **(If Auth Type is not None)**	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
Key ID **(If Auth Type is not None or Simple)**	Specify the key ID for OSPF authentication.	1 to 255 characters	N/A
Passive Interface **(Only in Advanced Mode)**	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 - Settings - Neighbor

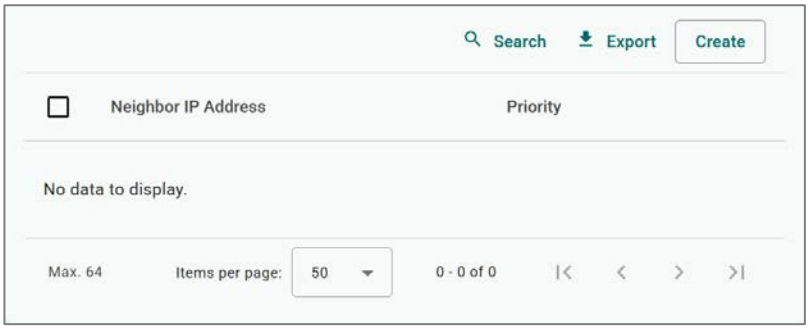
This page lets you configure OSPF neighbor settings.

> **Note**
> This page is only available in Advanced Mode.

Limitations

You can create up to 64 OSPF neighbors.

OSPF Neighbor List



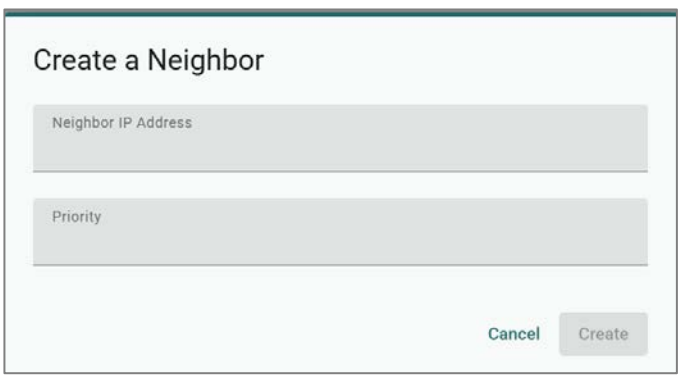
UI Setting	Description
Neighbor IP Address	Shows the IP address of the neighbor device.
Priority	Shows the L3 priority of the neighbor. Higher values mean higher priority for becoming the designated router. A value of 0 means this neighbor will not become a designated router.

Creating an OSPF Neighbor

Menu Path: Routing > Unicast Route > OSPF - Settings - Neighbor

Clicking **Create** on the **Routing > Unicast Route > OSPF - Settings - Neighbor** page will open this dialog box. This dialog lets you add an OSPF neighbor.

Click **Create** to save your changes.



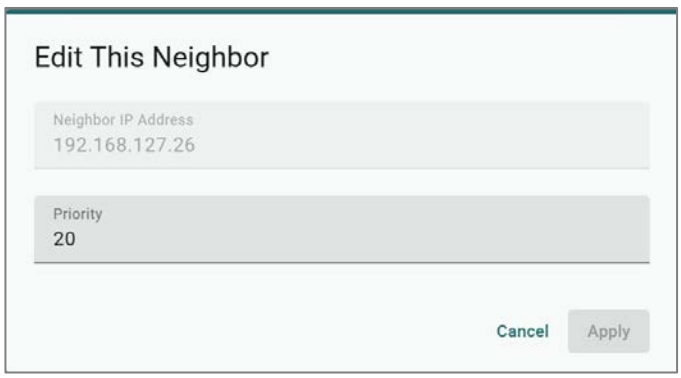
UI Setting	Description	Valid Range	Default Value
Neighbor IP Address	Specify the IP address for the neighbor.	Valid IP address	N/A
Priority	Specify the priority for the neighbor. Higher values mean higher priority for becoming the designated router. A value of 0 means this neighbor will not become a designated router.	0 to 255	N/A

Editing an OSPF Neighbor

Menu Path: Routing > Unicast Route > OSPF - Settings - Neighbor

Clicking the **Edit (✎)** icon for an OSPF neighbor on the **Routing > Unicast Route > OSPF - Settings - Neighbor** page will open this dialog box. This dialog lets you edit the OSPF neighbor.

Click **Apply** to save your changes.



UI Setting	Description	Valid Range	Default Value
Neighbor IP Address (View-only)	Shows the IP address for the neighbor. This value cannot be changed.	N/A	Neighbor IP address
Priority	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 - 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

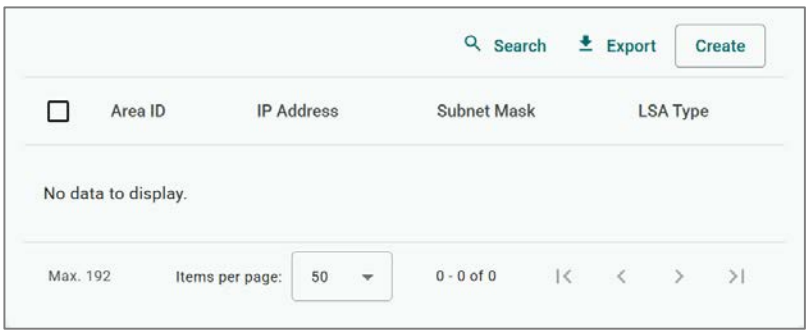
Menu Path: Routing > Unicast Route > OSPF - Settings - Aggregation

This page lets you configure OSPF aggregation settings.

Limitations

You can create up to 192 OSPF aggregations.

OSPF Aggregation List



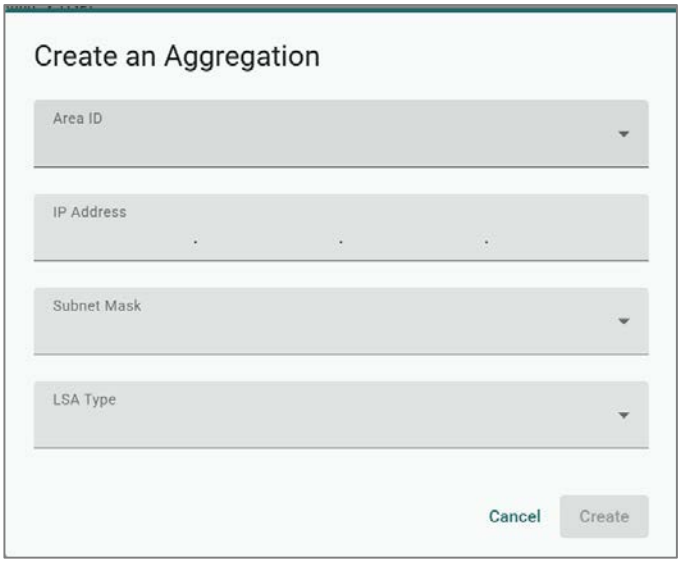
UI Setting	Description
Area ID	Shows the area ID of the aggregation.
IP Address	Shows the IP address of the aggregation.
Subnet Mask	Shows the subnet mask of the aggregation.
LSA Type	Shows the LSA type used for the aggregation.

Creating an OSPF Aggregation

Menu Path: Routing > Unicast Route > OSPF - Settings - Aggregation

Clicking **Create** on the **Routing > Unicast Route > OSPF - Settings - Aggregation** page will open this dialog box. This dialog lets you create an OSPF aggregation.

Click **Create** to save your changes.



UI Setting	Description	Valid Range	Default Value
Area ID	Select the Area ID that you want to use for the aggregation.	Drop-down list of area IDs	0.0.0.0
IP Address	Specify the IP address for the aggregation.	Valid IP address	N/A
Subnet Mask	Specify the subnet mask for the aggregation.	Drop-down list of subnet masks	N/A
LSA Type	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 - 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

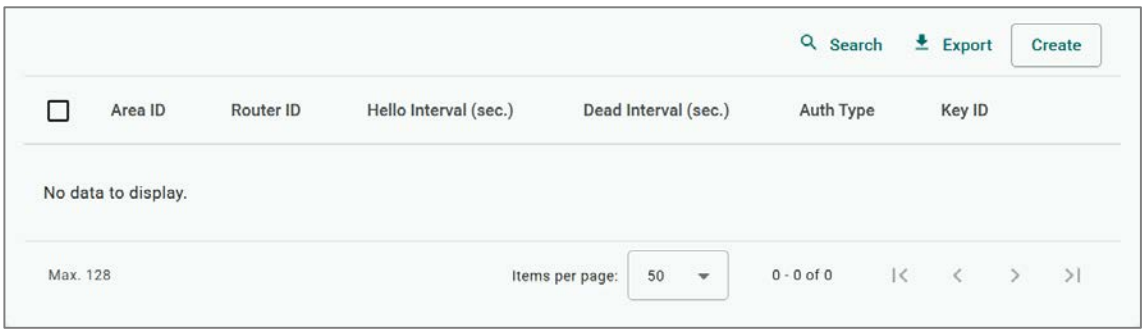
Menu Path: Routing > Unicast Route > OSPF - Settings - Virtual Link

This page lets you configure OSPF virtual link settings.

Limitations

You can create up to 128 OSPF virtual links.

OSPF Virtual Link List



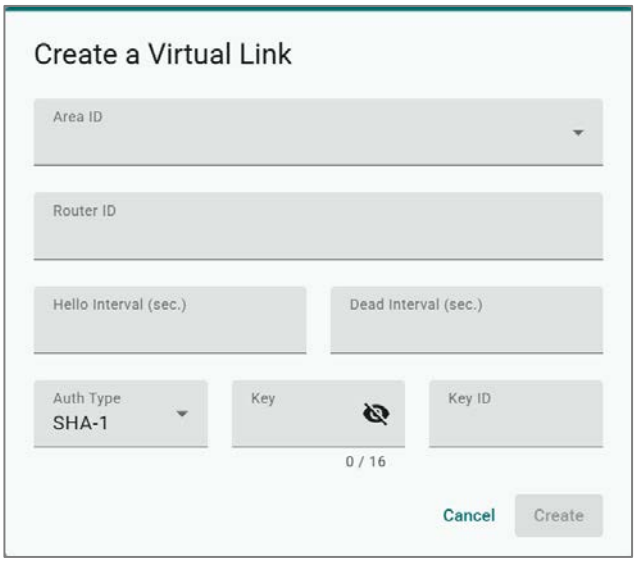
UI Setting	Description
Area ID	Shows the area ID for the virtual link.
Router ID	Shows the router ID for the virtual link.
Hello Interval (sec.)	Shows the hello packet send interval in seconds for the virtual link.
Dead Interval (sec.)	Shows the dead interval in seconds for the virtual link.
Auth Type	Shows the OSPF authentication type used for the virtual link.
Key ID	Shows the OSPF authentication key ID used for the virtual link.

Creating an OSPF Virtual Link

Menu Path: Routing > Unicast Route > OSPF - Settings - Virtual Link

Clicking **Create** on the **Routing > Unicast Route > 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.



UI Setting	Description	Valid Range	Default Value
Area ID	Select the area ID to use for the virtual link.	Drop-down list of area IDs	N/A
Router ID	Specify the L3 switch or router ID to use for the virtual link.	Valid router ID	N/A
Hello Interval	Specify the hello packet send interval in seconds. Hello packets are packets sent to OSPF neighbors to maintain connectivity with those neighbors. **Note** The value of all hello intervals must be the same within a network.	1 to 65535	N/A
Dead Interval	Specify the dead interval in seconds. **Note** The dead interval is often set as four times the hello interval.	1 to 65535	N/A

UI Setting	Description	Valid Range	Default Value
Auth Type	Specify the OSPF authentication type to use when authenticating OSPF neighbors, or select **None** for no authentication. **Note** If OSPF authentication is used, all L3 switches and routers on the same segment must use the same authentication method and key.	None / Simple / MD5 / SHA1 / SHA-224 / SHA-256 / SHA-385 / SHA-512	N/A
Key **(If Auth Type is not None)**	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
Key ID **(If Auth Type is not None or Simple)**	Specify the key ID for OSPF authentication.	1 to 255 characters	N/A

Deleting an OSPF Virtual Link

Menu Path: Routing > Unicast Route > 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 - Status

This page lets you monitor OSPF status information.

This page includes these tabs:

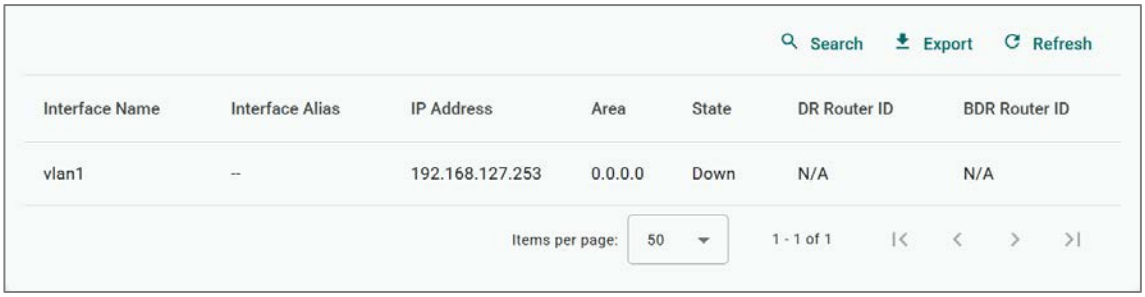
- Interface
- Neighbor
- Database
- Virtual Link

OSPF Status - Interface

Menu Path: Routing > Unicast Route > OSPF - Status - Interface

This page lets you view the status of your device's OSPF interfaces.

OSPF Interface Status



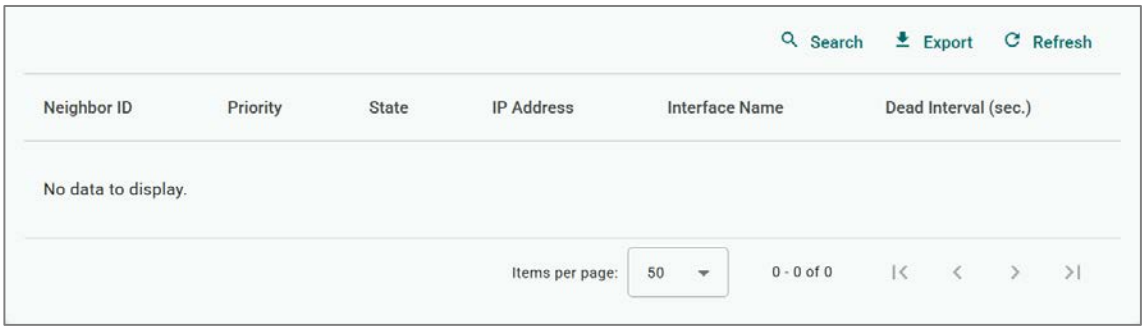
UI Setting	Description
Interface Name	Shows the name of the interface this entry is for.
Interface Alias	Shows the alias for the interface.
IP Address	Shows the IP address for the interface.
Area	Shows the area ID for the interface.
State	Shows whether the interface is currently up or down.
DR Router ID	Shows the ID of the designated router (DR).
BDR Router ID	Shows the ID of the backup designated router (BDR).

OSPF Status - Neighbor

Menu Path: Routing > Unicast Route > OSPF - Status - Neighbor

This page lets you view the status of your device's OSPF neighbors.

OSPF Neighbor Status



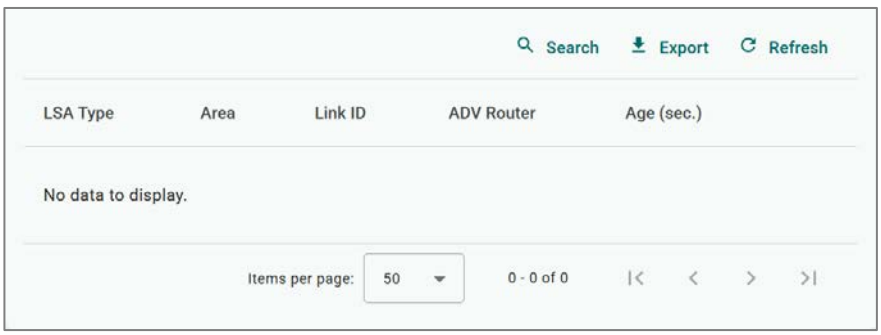
UI Setting	Description
Neighbor ID	Shows the ID of the neighbor device.
Priority	Shows the L3 priority of the neighbor.
State	Shows the state of the neighbor.
IP Address	Shows the IP address of the neighbor device.
Interface Name	Shows which interface the neighbor is connected to.
Dead Interval (sec.)	Shows the dead interval in seconds for the neighbor.

OSPF Status - Database

Menu Path: Routing > Unicast Route > OSPF - Status - Database

This page lets you view the status of your device's OSPF database.

OSPF Database Status



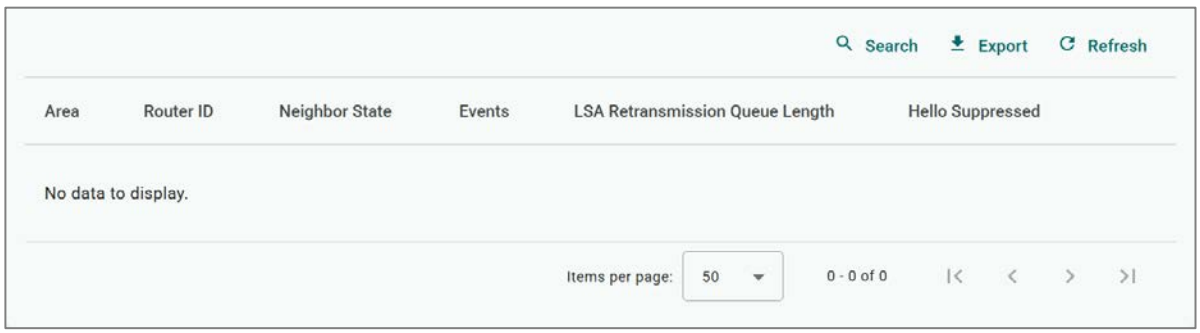
UI Setting	Description
LSA Type	Shows the type of the link state advertisement (LSA).
Area	Shows the area ID of the LSA.
Link ID	Shows the link ID of the LSA.
ADV Router	Shows the router where the LSA originated from.
Age (sec.)	Shows the age of the LSA in seconds.

OSPF Status - Virtual Link

Menu Path: Routing > Unicast Route > OSPF - Status - Virtual Link

This page lets you view the status of your device's OSPF virtual links.

OSPF Virtual Link Status



UI Setting	Description
Area	Shows the area ID for the virtual link.
Router ID	Shows the router ID for the virtual link.
Neighbor State	Shows the current state of the neighbor.
Events	Shows the number of events that have occurred since the device was booted. Events include the state of the virtual link changing and errors.
LSA Retransmission Queue Length	Shows the current length of the LSA retransmission queue.

UI Setting	Description
Hello Suppressed	Shows whether hello messages to the neighbor are being suppressed.

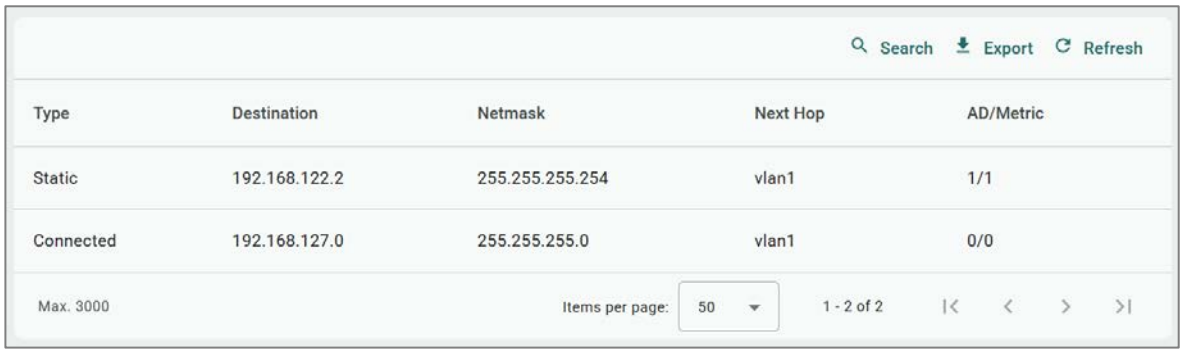
Routing Table

Menu Path: Routing > Unicast Route > Routing Table

This page lets you see the current routing table for your device.

Limitations

The unicast routing table can hold up to 3000 entries.



UI Setting	Description
Type	Shows the source type of the route.
Destination	Shows the address of the destination network for the route.
Netmask	Shows the netmask of the destination network for the route.
Next Hop	Shows the IP address or interface of the next hop that the packet should be forwarded to.
AD / Metric	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

About PIM-DM

Protocol Independent Multicast - Dense Mode (PIM-DM) is a multicast routing protocol for dense networks. It operates by assuming all devices on the network want to receive multicast packets, and then accepts pruning requests for devices to opt-out. This is useful for high-density networks where bandwidth is plentiful and network distances are short.

PIM-DM is a Layer 3 multicast routing protocol, which interacts with IGMP Snooping to convert Class D (multicast) IP Addresses (224.0.0.0 to 239.255.255.255) into multicast MAC addresses to allow L2 addressing.

PIM-DM Mechanisms

PIM-DM uses 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 without interested receivers for multicast traffic send prune messages to their upstream neighbors, stopping further unwanted traffic.
- Periodic Flooding: To account for changes in group membership, PIM-DM periodically refloods the multicast traffic to ensure that new receivers have the opportunity to 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.

> **Note**
>
> This feature supports weaker authentication or encryption, and may not be secure over untrusted networks. Take appropriate security precautions.

Enabling PIM-DM

Enable PIM-DM on the switch to support dense mode multicast routing on configured VLANs and interfaces.

- PIM-SM and Multicast Local Route must both be disabled.
- VLANs must have been created and assigned. Refer to About VLAN.
- IGMP Snooping must be enabled for the interfaces

1. Sign in to the device with administrator credentials.
2. Go to **Routing** > **Multicast Route** > **PIM-DM**, and then click **Settings**.
3. Click **PIM-DM** and choose **Enable**, and then click **Apply**.

Note: All switches in the PIM-DM topology should be configured as PIM-DM mode, and should have same **State Refresh** and **State Refresh Interval** settings. Click **Apply** after changing these settings.

4. On the Interface Table, click **Edit** corresponding to the interface.

The Edit Interface screen appears.

5. Click **PIM-DM** and choose **Enable**, and then click **Apply**.

You can enable PIM-DM on additional interfaces as needed.

To view Multicast Route Entries for PIM-DM, click **Neighbor** at the top of the screen.

PIM-DM

Menu Path: Routing > Multicast Route > PIM-DM

This page lets you manage PIM-DM for your device.

This page includes these tabs:

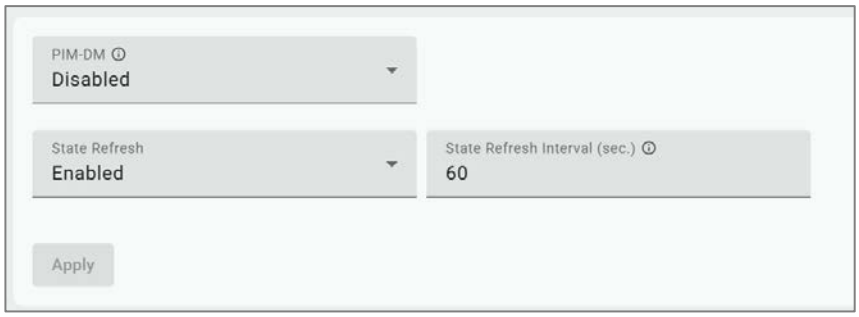
- Settings
- Neighbor

PIM-DM - Settings

Menu Path: Routing > Multicast Route > PIM-DM - Settings

This page lets you configure PIM-DM for your device.

PIM-DM Settings



UI Setting	Description	Valid Range	Default Value
PIM-DM	Enable or disable use of PIM-DM protocol. **Note** Only one multicast routing protocol can be active. If you want to enable PIM-DM, make sure you disable PIM-SM and Multicast Local Route.	Enabled / Disabled	Disabled
State Refresh	Enable or disable state refresh.	Enabled / Disabled	Enabled
State Refresh Interval	Specify the interval in seconds for the state to refresh.	10 to 100	60

PIM-DM Interface List



UI Setting	Description
Interface Name	Shows the name of the interface.
Interface Alias	Shows the alias of the interface.
IP Address	Shows the IP address of the interface.
PIM-DM	Shows whether PIM-DM is enabled on the interface.
Hello Interval (sec.)	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.



UI Setting	Description	Valid Range	Default Value
PIM-DM	Enable or disable PIM-DM for the interface.	Enabled / Disabled	Disabled
Hello Interval	Specify the interval in seconds between sending Hello messages.	10 to 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



UI Setting	Description
Neighbor	Shows the PIM-DM neighbor this entry is for.
Interface Name	Shows which interface the neighbor is connected to.
Uptime	Shows how long this multicast route entry has been maintained by this device.
Expiration Time	Shows the time remaining before this multicast route is removed from the PIM-DM neighbor list if it is not refreshed.

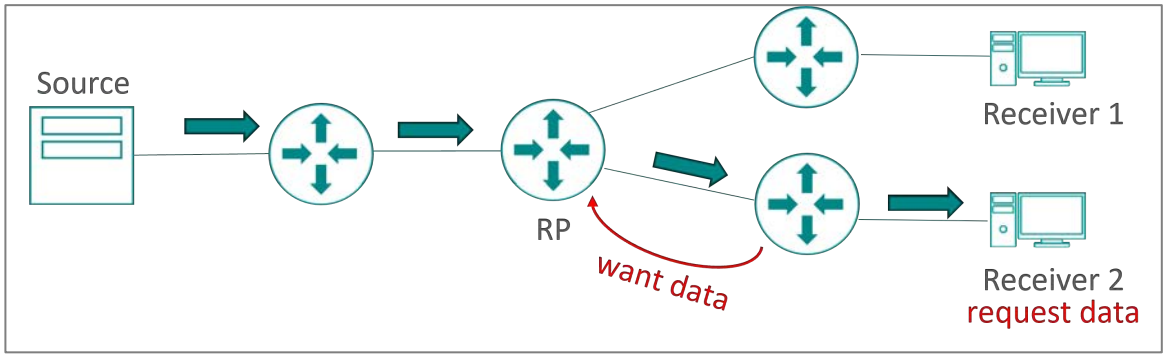
About PIM-SM

Protocol Independent Multicast – Sparse Mode (PIM-SM) is a multicast routing protocol designed for environments where multicast receivers are sparsely distributed across the

network. It assumes that only a very low percentage of receivers subscribe to a particular multicast group.

The key component of PIM-SM is the Rendezvous Point (RP), which forms 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 a Shortest Path Tree (SPT) switchover to switch to a newly identified shortest path.

Since PIM-SM only forwards multicast data to the requester and always tries to route traffic through the shortest path, it is more scalable and efficient than PIM-DM.



Note

This feature supports weaker authentication or encryption, and may not be secure over untrusted networks. Take appropriate security precautions.

PIM-SM RP Identification and Pathing # PIM-SM RP Identification and Pathing

PIM-SM follows a specific process to create and maintain paths.

Rendezvous Point (RP)

The RP plays a crucial role in PIM-SM. It is responsible for receiving multicast traffic from all sources and forwarding it down the multicast distribution tree to all receivers that have joined the multicast group. The RP can be statically configured or elected dynamically using a Bootstrap Router (BSR) mechanism.

Multicast Group Join Messages

When a host wants to receive multicast traffic for a specific group, the corresponding local router sends a PIM Join message to the RP. This message is propagated hop-by-hop until it reaches the RP, building a shared tree along the path.

Shortest Path Trees

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, routers close 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.

Tree Maintenance

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.

Configuring Non-RP Interfaces for PIM-SM

Enable PIM-SM on interfaces to participate in multicast routing without configuring the device as a Rendezvous Point (RP).

- PIM-DM and Multicast Local Route must both be disabled.
- VLANs must have been created and assigned. Refer to About VLAN.
- IGMP Snooping must be enabled for the interfaces.

1. Sign in to the device with administrator credentials.
2. Go to **Routing** > **Multicast Route** > **PIM-SM** > **Settings**, and then click **General**.
3. Select **PIM-SM**, choose **Enabled**, and then click **Apply**.
4. From the table of interfaces, locate the interface that will connect to the Static RP, and then click **Edit**.

The Edit Interface screen appears.

5. Click **PIM-SM**, choose **Enable**, and then click **Apply**.

PIM-SM is now enabled. The device will participate in PIM-SM multicast routing using other RPs.

Designating a Static RP

Configure a static Rendezvous Point (RP) for PIM-SM by enabling multicast routing settings and defining RP parameters for multicast groups.

- PIM-DM and Multicast Local Route must both be disabled.
- VLANs must have been created and assigned. Refer to About VLAN.
- IGMP Snooping must be enabled for the interfaces.

1. Sign in to the device with administrator credentials.
2. Go to **Routing** > **Multicast Route** > **PIM-SM** > **Settings**, and then click **General**.
3. Select **PIM-SM**, choose **Enabled**, and then click **Apply**.
4. From the table of interfaces, locate the interface that will connect to the Static RP, and then click **Edit**.

The Edit Interface screen appears.

5. Click **PIM-SM**, choose **Enable**, and then click **Apply**.
6. Go to **Routing** > **Multicast Route** > **PIM-SM** > **Settings**, and then click **RP**.
7. Under Static RP, click **Add**.

The Create Static RP screen appears.

8. Specify all of the following, and then click **Apply**:

Option	Value
Group Address	Specify the PIM multicast group IP address.
Group Mask	Select the subnet mask of the group.
RP Address	Specify the IP address of the static RP for this multicast group.
Override	**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.

The Static RP appears on the list.

Designating a Dynamic RP Candidate

Configure the device as a dynamic RP candidate for PIM-SM by enabling BSR and specifying multicast group settings.

- PIM-DM and Multicast Local Route must both be disabled.
- VLANs must have been created and assigned. Refer to About VLAN.
- IGMP Snooping must be enabled for the interfaces.

1. Sign in to the device with administrator credentials.
2. Go to **Routing** > **Multicast Route** > **PIM-SM** > **Settings**, and then click **General**.
3. Select **PIM-SM**, choose **Enabled**, and then click **Apply**.
4. From the table of interfaces, locate the interface that will connect to the Static RP, and then click **Edit**.
5. Set both **PIM-SM** and **BSR Candidate** to **Enabled**, and then click **Apply**.
6. Go to **Routing** > **Multicast Route** > **PIM-SM** > **Settings**, and then click **RP**.
7. Under Candidate RP, click **Add**

The Create Candidate RP screen appears.

8. Configure the all of following, and then click **Apply**:

Option	Value
Group Address	Specify the multicast group(s) that this Candidate RP serves.
Group Mask	Specify the mask of the **Group Address**.
RP Interface Name (RP Address)	Specify the IP the device advertises as its RP address to other PIM routers.
RP Priority	Choose a value from 0 to 255. Lower numbers are high priority.

The selected RP will now be included in the candidate pool. You can view the current candidates under **Status** from **Routing** > **Multicast Route** > **PIM-SM** > **Settings.**

PIM-SM

Menu Path: Routing > Multicast Route > PIM-SM

This page lets you manage PIM-SM for your device.

This page includes these tabs:

- Settings
- Status

PIM-SM Settings

Menu Path: Routing > Multicast Route > 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 - Settings - General

This page lets you configure PIM-SM general settings.

PIM-SM Settings



UI Setting	Description	Valid Range	Default Value
PIM-SM	Enable or disable use of PIM-SM protocol. **Note** Only one multicast routing protocol can be active. If you want to enable PIM-SM, make sure you disable PIM-DM and Multicast Local Route.	Enabled / Disabled	Disabled
Shortest-path Tree Switchover Method	Select whether the device should switch over to the shortest-path tree if one is found.	Never / Immediate	Never

PIM-SM Interface List



UI Setting	Description
Interface Name	Shows the name of the interface.
Interface Alias	Shows the alias of the interface.
IP Address	Shows the IP address of the interface.
PIM-SM	Shows whether PIM-SM is enabled on the interface.

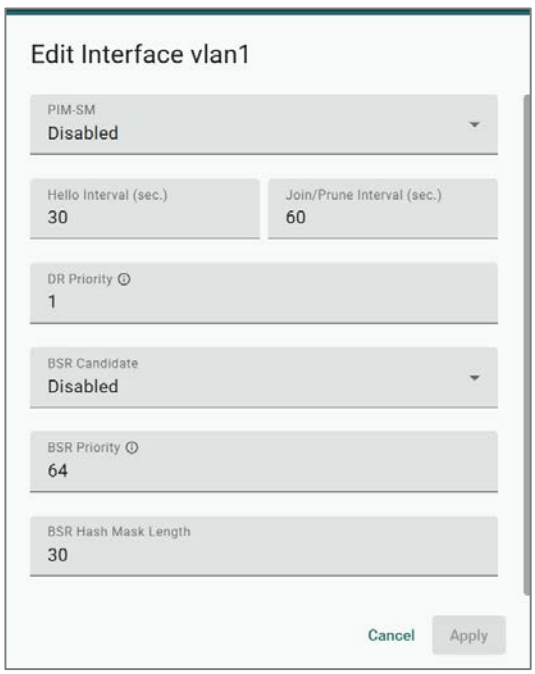
UI Setting	Description
Hello Interval (sec.)	Shows the interval in seconds to send Hello messages for the interface.
Join/Prune Interval (sec.)	Shows the interval in seconds to send Join/Prune messages.
DR Priority	Shows the DR (Designated Router) priority for the interface. Higher values have higher preference for the DR election process.
BSR Candidate	Shows whether the interface can be a BSR (Bootstrap Router) Candidate.
BSR Priority	Shows the BSR priority for the interface. Higher values have higher preference for the BSR election process.
BSR Hash Mask Length	Shows the mask length in bits to use for the BSR hash.

Editing a PIM-SM Interface

Menu Path: Routing > Multicast Route > PIM-SM - Settings - General

Clicking the **Edit (✎)** icon for an interface on the **Routing > Multicast Route > 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 Setting	Description	Valid Range	Default Value
PIM-SM	Enable or disable PIM-SM for the interface.	Enabled / Disabled	Disabled
Hello Interval	Specify the interval in seconds to send Hello messages.	10 to 3600	30
Join/Prune Interval	Specify the interval in seconds to send Join/Prune messages.	10 to 3600	60
DR Priority	Specify the DR (Designated Router) priority for the interface. Higher values have higher preference for the DR election process.	1	4294967295
BSR Candidate	Enable or disable whether the interface can be a BSR (Bootstrap Router) candidate.	Enabled / Disabled	Disabled
BSR Priority	Specify the BSR priority for the interface. Higher values have higher preference for the BSR election process.	0 to 255	64
BSR Hash Mask Length	Specify the mask length in bits to use for the BSR hash.	4 to 32	30

PIM-SM Settings - RP

Menu Path: Routing > Multicast Route > PIM-SM - Settings - RP

This page lets you configure PIM-SM Rendezvous Point (RP) related settings.

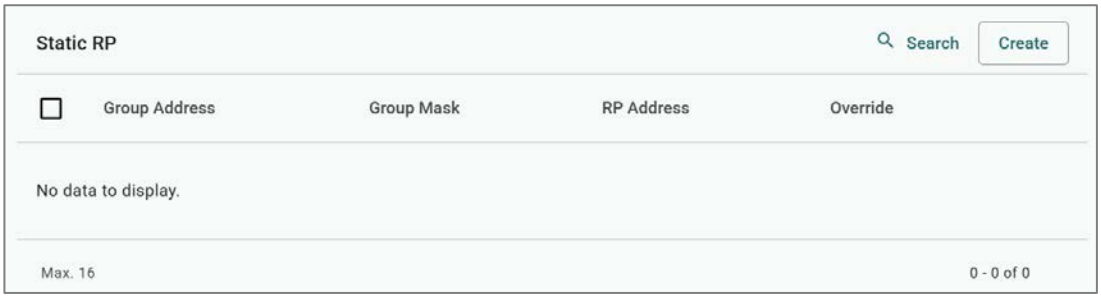
Limitations

You can create up to 16 static RP entries.

Limitations

You can create up to 16 candidate RP entries.

Static RP List



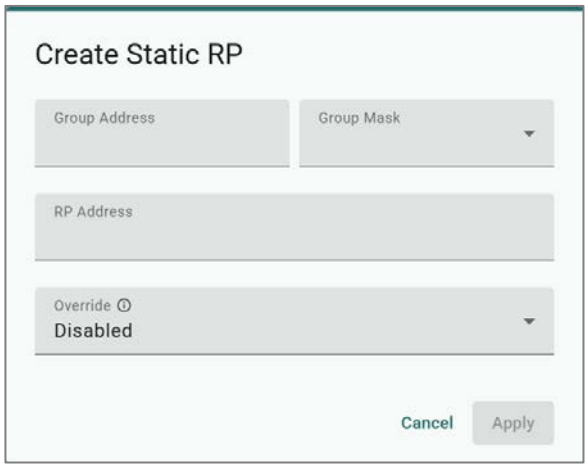
UI Setting	Description
Group Address	Shows the address of the PIM multicast group this entry is for.
Group Mask	Shows the subnet mask of the group.
RP Address	Shows the RP address of the static RP.
Override	Shows whether override is enabled for the group.

Creating a Static RP

Menu Path: Routing > Multicast Route > PIM-SM - Settings - RP

Clicking **Create** for the Static RP list on the **Routing > Multicast Route > 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.



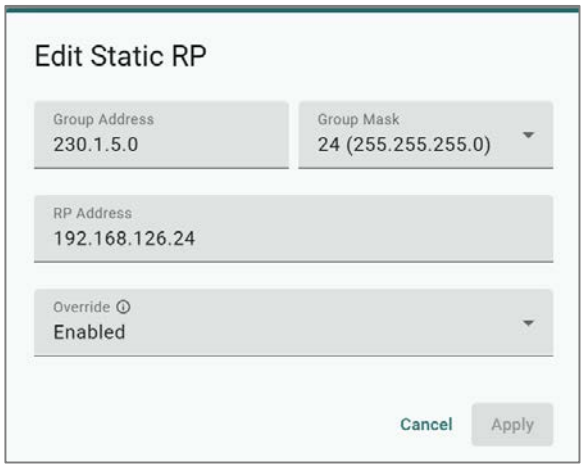
UI Setting	Description	Valid Range	Default Value
Group Address	Specify the PIM multicast group address.	224.0.0.0 to 239.255.255.255	N/A
Group Mask	Specify the subnet mask of the group.	Drop-down list of subnet masks	N/A
RP Address	Specify the IP address of the static RP for this multicast group.	Valid IP address	N/A
Override	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	Disabled

Editing a Static RP

Menu Path: Routing > Multicast Route > PIM-SM - Settings - RP

Clicking the **Edit (✎)** icon for a static RP on the **Routing > Multicast Route > 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 Setting	Description	Valid Range	Default Value
Group Address	Specify the PIM multicast group address.	224.0.0.0 to 239.255.255.255	N/A
Group Mask	Specify the subnet mask of the group.	Drop-down list of subnet masks	N/A
RP Address	Specify the IP address of the static RP for this multicast group.	Valid IP address	N/A
Override	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	Disabled

Deleting a Static RP

Menu Path: Routing > Multicast Route > 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.

Candidate RP List



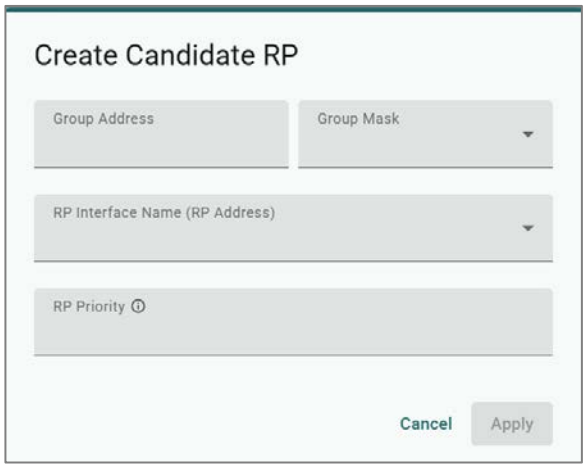
UI Setting	Description
Group Address	Shows the address of the PIM multicast group this entry is for.
Group Mask	Shows the subnet mask of the group.
RP Interface Name	Shows the interface of the candidate RP for the group.
RP Address	Shows the address of the candidate RP for the group.
RP Priority	Shows the RP priority. Lower values have higher preference for the RP election process.

Creating a Candidate RP

Menu Path: Routing > Multicast Route > PIM-SM - Settings - RP

Clicking **Create** for the Candidate RP list on the **Routing > Multicast Route > PIM-SM - Settings - RP** page will open this dialog box. This dialog lets you create a new candidate RP.

Click **Create** to save your changes and add the new candidate RP.



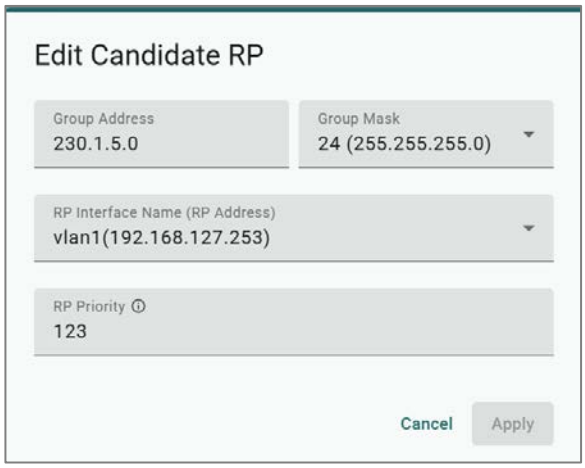
UI Setting	Description	Valid Range	Default Value
Group Address	Specify the PIM multicast group address.	224.0.0.0 to 239.255.255.25	N/A
Group Mask	Specify the subnet mask of the group.	Drop-down list of subnet masks	N/A
RP Interface Name (RP Address)	Specify the interface of the candidate RP for this group.	Drop-down list of interfaces	N/A
RP Priority	Specify the RP priority. Lower values have higher preference for the RP election process. **Note** If the RP Priority is not set, the default value of 192 will be used.	0 to 255	N/A

Editing a Candidate RP

Menu Path: Routing > Multicast Route > PIM-SM - Settings - RP

Clicking the **Edit (✎)** icon for a candidate RP on the **Routing > Multicast Route > 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 Setting	Description	Valid Range	Default Value
Group Address	Specify the PIM multicast group address.	224.0.0.0 to 239.255.255.25	N/A
Group Mask	Specify the subnet mask of the group.	Drop-down list of subnet masks	N/A
RP Interface Name (RP Address)	Specify the interface of the candidate RP for this group.	Drop-down list of interfaces	N/A
RP Priority	Specify the RP priority. Lower values have higher preference for the RP election process. **Note** If the RP Priority is not set, the default value of 192 will be used.	0 to 255	N/A

Deleting a Candidate RP

Menu Path: Routing > Multicast Route > 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 - Settings - SSM

This page lets you configure PIM Source-specific Multicast (SSM) related settings.

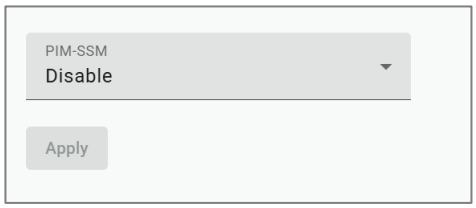
Note

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

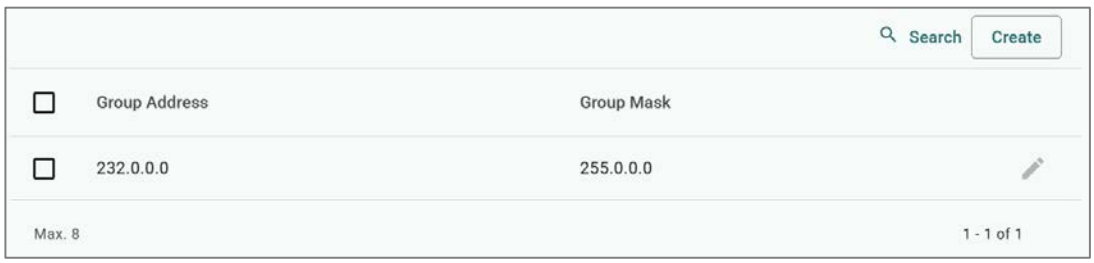
You can create up to 8 SSM sources.

PIM-SSM Settings



UI Setting	Description	Valid Range	Default Value
PIM-SMM	Enable or disable Source-specific Multicast (SSM). **Note** When enabling SSM, the source range for 232.0.0.0/8 will be enabled automatically.	Enabled / Disabled	Disabled

PIM-SSM Range List



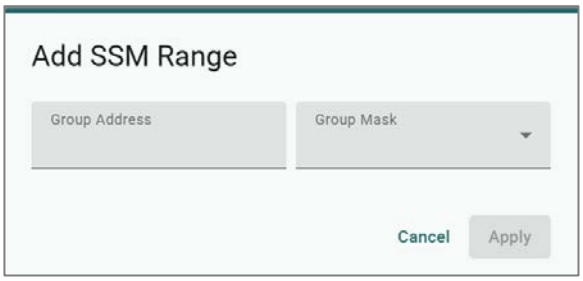
UI Setting	Description
Group Address	Shows the group address for the PIM-SSM range.
Group Mask	Shows the subnet mask of the group address for the PIM-SSM range.

Creating a PIM-SSM Range

Menu Path: Routing > Multicast Route > PIM-SM - Settings - SSM

Clicking **Create** on the **Routing > Multicast Route > 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 Setting	Description	Valid Range	Default Value
Group Address	Specify the group address for the PIM-SSM range.	Valid multicast IP address	N/A
Group Mask	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

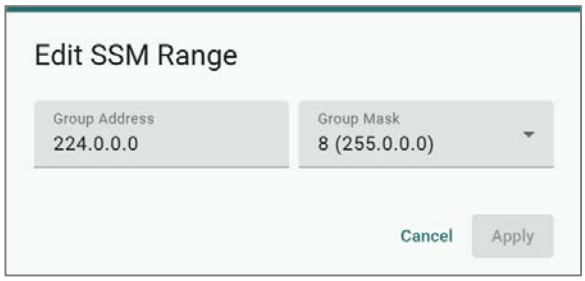
Menu Path: Routing > Multicast Route > PIM-SM - Settings - SSM

Clicking the **Edit (✎)** icon for a PIM-SSM range on the **Routing > Multicast Route > 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 Setting	Description	Valid Range	Default Value
Group Address	Specify the group address for the PIM-SSM range.	Valid multicast IP address	N/A
Group Mask	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 - 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 - 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 - Status - Interface

This page lets you monitor the PIM-SM status of your device's interfaces.



UI Setting	Description
Interface Name	Shows the name of the interface.
Interface Alias	Shows the alias of the interface.
IP Address	Shows the IP address of the interface.
PIM-SM	Shows whether PIM-SM is enabled or disabled on this interface.
DR Address	Shows the DR address of the interface.

PIM-SM Status - Neighbor

Menu Path: Routing > Multicast Route > PIM-SM - Status - Neighbor

This page lets you monitor the status of PIM-SM neighbors.



UI Setting	Description
Neighbor	Shows the IP address of the neighbor connected to your device.
Interface Name	Shows the interface the neighbor is connected to.
Uptime	Shows how long this multicast route entry has been maintained by this device.
Expiration Time	Shows the time remaining before this multicast route is removed from the multicast routing table if it is not refreshed.
DR Priority	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 - Status - BSR/RP

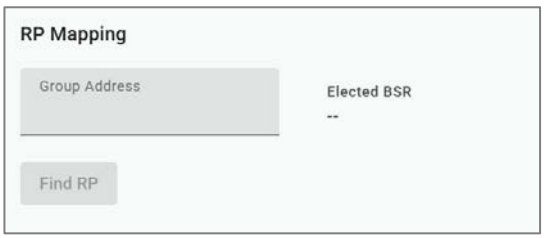
This page lets you monitor the BSR and static RP status of PIM-SM in the network.

Elected BSR



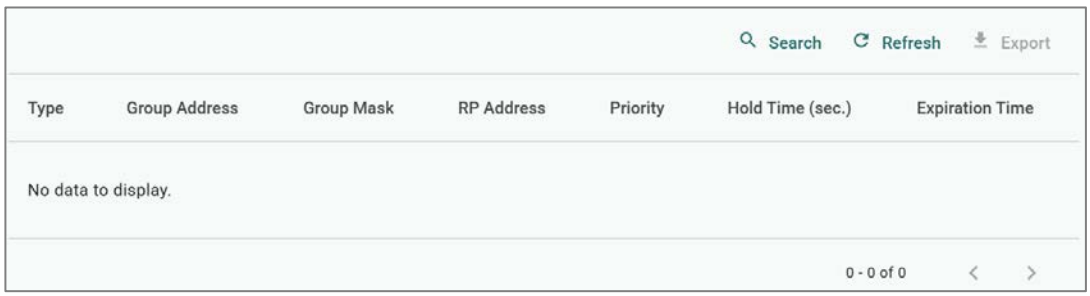
UI Setting	Description
BSR Address	Shows the address of the current elected BSR.
BSR Priority	Shows the priority of the BSR.
BSR Hash Mask Length	Shows the hash mask length of the BSR.

RP Mapping



UI Setting	Description
Group Address	Enter a group address and click **Find RP** to search for the RP for the group address.
RP Mapping Result	Shows the result of the RP search.

PIM-SM Status - BSR/RP List



UI Setting	Description
Type	Shows the role type of this entry.
Group Address	Shows the group address of the BSR or RP this entry is for.
Group Mask	Shows the subnet mask of the group address.

UI Setting	Description
RP Address	Shows the RP of this group address.
Priority	Shows the RP priority. Lower values have higher preference for the RP election process.
Hold Time (sec.)	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.
Expiration Time	Shows the time remaining before this multicast route is removed from the multicast routing table if it is not refreshed.

About Multicast Local Routes

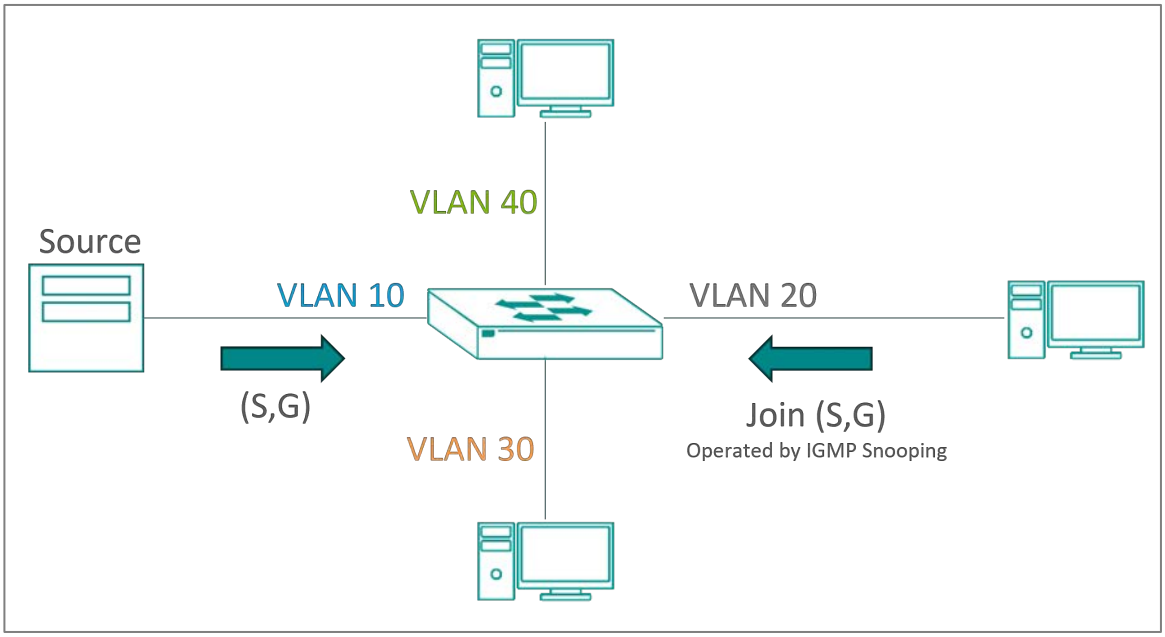
Multicast Local Routes—coupled with Multicast Access Control Lists— limit multicast traffic forwarding to multicast groups based on source and downstream VLAN settings. They enable precise control over multicast traffic within a network by allowing specific multicast streams to be permitted or denied.

Multicast Local Routes

Multicast Local Routes are entries created on the device that delineate multicast streams between VLANs. Once the traffic is identified, it can be managed with Multicast Access Control Lists. This kind of filtering is most effective when multicast source and destination VLANs are clearly defined.

Multicast Access Control Lists

The Multicast Access Control List, called Multicast ACL or MACL, determines whether to allow or block multicast streams (defined by the routes, above). 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.



Enabling Multicast Local Route

Multicast Local Route must be enabled before routes and MACLs can take effect.

- Make sure PIM-SM and PIM-DM are disabled.
- Make sure that you have created both Source and Downstream L3 VLAN interfaces.
- Make sure IGMP Snooping on the interfaces is enabled.

1. Sign in to the device with administrator credentials.
2. Go to **Routing** > **Multicast Route** > **Multicast Local Route**, and then click **General**.
3. Set **Multicast Local Route** to **Enabled**, and then click **Apply**.

Note

Enable VRRP Master Only if you want to ensure that multicast traffic is forwarded only by the current VRRP master (if your topology uses VRRP). This helps prevent duplicate multicast streams and ensures consistent traffic flow in redundant configurations.

Configuring Multicast Routes

Define Multicast Local Routes to manage with Multicast Access Control Lists

1. Sign in to the device with administrator credentials.
2. Go to **Routing** > **Multicast Route** > **Multicast Local Route**, and then click **Routes**.
3. Click **Add**, configure all of the following, and then click **Apply**:

Option	Value
Source VLAN	Specify the origin VLAN allowed to send multicast packets.
Destination VLAN	Specify the target VLAN allowed to receive multicast packets.

The multicast route appears on the table.

Configuring Multicast Access Control Lists (MACL)

Multicast Access Control Lists allow the creation of allowlists/blocklists for multicast routes.

1. Sign in to the device with administrator credentials.
2. To configure the Multicast Access Control List, go to **Routing** > **Multicast Route** > **Multicast Local Route**, and then click **MACL**.
3. Select **Add**, and configure the following:

Option	Value
MACL ID	Choose an ID for the Access Control List. Lower numbers have higher priority in decisions.
Multicast Group	Specify a multicast group IP address. Serves as the "Destination" for the Access Control List entry.
Group Mask	Select a subnet mask for **Multicast Group**.
Source IP Address	Select the IP address from which the multicast packets originate.
Source IP Mask	Select a subnet mask for **Source IP Address**.
Source VLAN	Specify the source VLAN ID for Access Control List entry.

Option	Value
Downstream VLAN	Specify the downstream VLAN for the Access Control List entry.
Action	Select the action to take for this route. • **Permit:** Allow matching traffic • **Deny:** Drop matching traffic |

4. Click **Create**.

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:

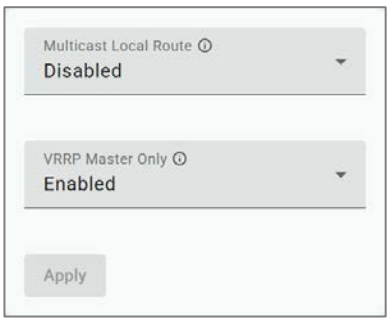
- General
- Routes
- MACL

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



UI Setting	Description	Valid Range	Default Value
Multicast Local Route	Enable or disable multicast local routing. **Note** Multicast local routing is based on IGMP snooping, so if you enable Multicast Local Route, make sure IGMP snooping is enabled. Refer to IGMP Snooping for more information. **Note** Only one multicast routing protocol can be active, so if you enable **Multicast Local Route**, make sure you disable PIM-DM and PIM-SM. Refer to PIM-DM and PIM-SM for more information.	Enabled / Disabled	DIsabled
VRRP Master Only	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.

Limitations

You can create up to 16 multicast local routes.

Multicast Local Route List



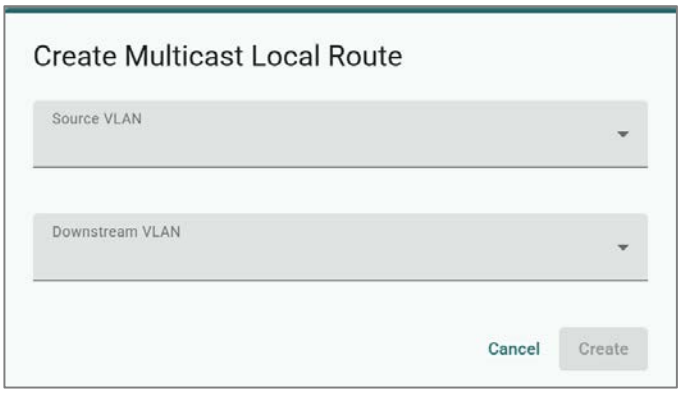
UI Setting	Description
Source VLAN	Shows the source VLAN of the multicast route.
Downstream VLAN	Shows the downstream VLANs of the multicast route.

Creating a Multicast Local Route

Menu Path: Routing > Multicast Route > Multicast Local Route - Routes

Clicking **Create** 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.



UI Setting	Description	Valid Range	Default Value
Source VLAN	Select the source VLAN of this multicast route. **Note** A VLAN must be created and set to an L3 interface before you can select it.	Drop-down list of VLAN interfaces	N/A

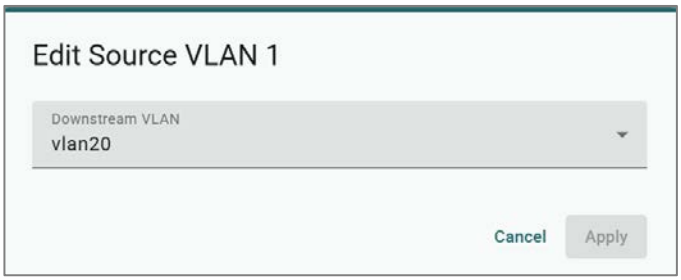
UI Setting	Description	Valid Range	Default Value
Downstream VLAN	Select the downstream VLANs for this multicast route. You can select multiple VLANs. **Note** A VLAN must be created and set to an L3 interface before you can select it.	Drop-down list of VLAN interfaces, multiple VLANs can be selected	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.



UI Setting	Description	Valid Range	Default Value
Downstream VLAN	Select the downstream VLANs for this multicast route. You can select multiple VLANs. **Note** A VLAN must be created and set to an L3 interface before you can select it.	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).

Limitations

You can create up to 16 multicast access control list entries.



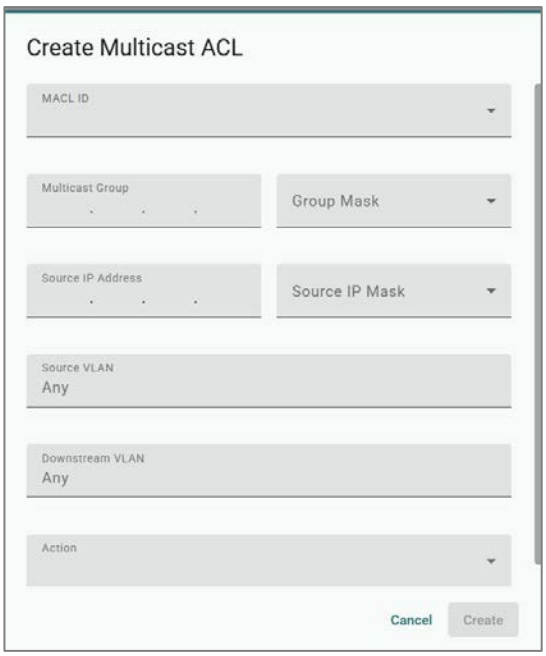
UI Setting	Description
MACL ID	Shows the ID for this MACL entry.
Multicast Group	Shows the multicast group of this multicast route.
Group Mask	Shows the group subnet mask of this multicast route.
Source IP Address	Shows the source IP address of this multicast route.
Source IP Mask	Shows the subnet mask of the source IP.
Source VLAN	Shows the source VLAN ID for the source IP.
Downstream VLAN	Shows the downstream VLAN for this multicast route.
Action	Shows the action to take for this route. • **Permit:** Traffic using this route will be permitted. • **Deny:** Traffic through this route will be dropped.

Creating a MACL Entry

Menu Path: Routing > Multicast Route > Multicast Local Route - MACL

Clicking **Create** 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.



UI Setting	Description	Valid Range	Default Value
MACL ID	Specify the ID for this MACL entry.	1 to 16	N/A
Multicast Group	Specify the multicast group of this multicast route.	224.0.0.0 to 239.255.255.25	N/A
Group Mask	Select the group subnet mask of this multicast route.	Drop-down list of subnet masks	N/A
Source IP Address	Specify the source IP address of this multicast route.	Valid IP address	N/A
Source IP Mask	Select the subnet mask of the source IP.	Drop-down list of subnet masks	N/A
Source VLAN	Specify the source VLAN ID for the source IP.	1 to 4094	N/A

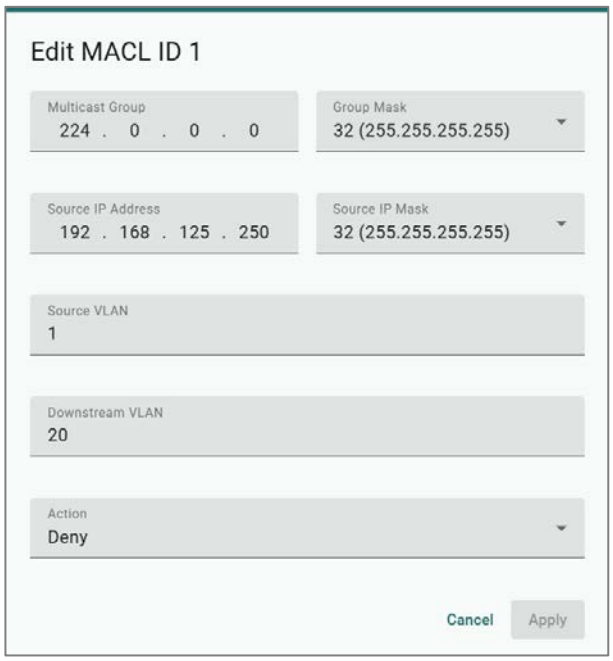
UI Setting	Description	Valid Range	Default Value
Downstream VLAN	Specify the downstream VLAN for this multicast route.	1 to 4094	N/A
Action	Select the action to take for this route. • **Permit:** Traffic using this route will be permitted. • **Deny:** Traffic through this route will be dropped.	Permit / 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.



UI Setting	Description	Valid Range	Default Value
Multicast Group	Specify the multicast group of this multicast route.	224.0.0.0 to 239.255.255.25	N/A

UI Setting	Description	Valid Range	Default Value
Group Mask	Select the group subnet mask of this multicast route.	Drop-down list of subnet masks	N/A
Source IP Address	Specify the source IP address of this multicast route.	Valid IP address	N/A
Source IP Mask	Select the subnet mask of the source IP.	Drop-down list of subnet masks	N/A
Source VLAN	Specify the source VLAN ID for the source IP.	1 to 4094	N/A
Downstream VLAN	Specify the downstream VLAN for this multicast route.	1 to 4094	N/A
Action	Select the action to take for this route. • **Permit:** Traffic using this route will be permitted. • **Deny:** Traffic through this route will be dropped.	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.

Limitations

The multicast routing table can hold up to 1024 entries.

Multicast Routing Table



UI Setting	Description
Mode	Shows the multicast routing protocol used for the route this entry is for.
Multicast Group	Shows the group address of the route.
Source	Shows the source IP of the multicast group.
Upstream Neighbor	Shows the closest neighbor forwarding multicast traffic to this device for this route.
Uptime	Shows how long this multicast route entry has been maintained by this device.
Expiration Time	Shows the time remaining before this multicast route is removed from the multicast routing table if it is not refreshed.
Incoming Interface	Shows the interface receiving multicast traffic for this route.
Outgoing Interface	Shows the interface forwarding multicast traffic for this route.

About Bidirectional Forwarding Detection (BFD)

Bidirectional Forwarding Detection (BFD) is a standardized, protocol-independent mechanism designed for rapid failure detection across different media types.

BFD provides:

- A consistent, rapid fault detection for upper-layer applications.
- A failure detection time of less than one second for faster network convergence, short application interruptions, and enhanced network reliability.

MX-NOS devices support asynchronous detection mode. In this mode, the devices periodically send BFD control packets to peers in the same session. Consecutive packet losses by a device is considered a down session. Asynchronous mode is useful because it requires half as many packets to achieve a given detection time compared to other modes.

> **Note**
>
> This feature supports weaker authentication or encryption, and may not be secure over untrusted networks. Take appropriate security precautions.

BFD In Depth

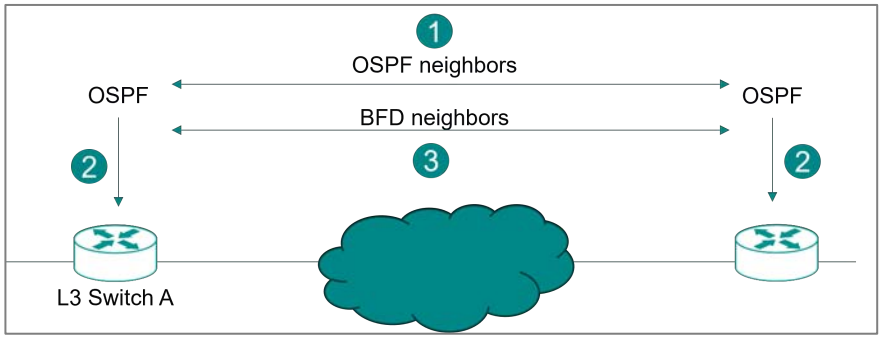
BFD is a protocol for quickly detecting link failures and notifying routing protocols of the problem. BFD can help for scenarios that do not allow failure detection rates longer than one second.

A link failure or topology change may lead to route recalculation. Different routing protocols use varying methods and timers to detect the loss of a routing adjacency with a peer. Devices can use the hello mechanism of a protocol for failure detection, which has a failure detection rate of more than one second, but this may be too slow for some applications.

Moxa implements the BFD mechanism to work with the OSPF routing protocol. BFD for OSPF can associate a BFD session with OSPF to reduce the routing path recovery time when the there is an OSPF network path failure or abnormal operation.

OSPF establishes a BFD session through the following process:

1. OSPF uses the Hello mechanism to discover neighbors and establishes a neighbor relationship (Adjacency in Full state).
2. OSPF notifies BFD with neighbor information, including source and destination addresses.
3. BFD sets up a session based on received neighbor information.
4. After the BFD session is established, BFD starts to monitor the link and responds quickly to any link faults.



For MX-NOS switches, BFD sessions for OSPF are only created in dynamic mode and do not support connecting to the device in static mode.

Enabling Bidirectional Forwarding Detection

BFD must be enabled before use.

1. Sign in to the device with administrator credentials.
2. Go to **Routing** > **BFD** and then click **Settings**.
3. Set **BFD for OSPF** to **Enabled**.
4. Configure the following:

Option	Value
Min. Tx Interval (ms)	Specify the minimum Tx interval to negotiate with the peer device.
Min. Rx Interval (ms)	Specify the minimum Rx interval to negotiate with the peer device.
Detect Multiplier	Specify the minimum detect multiplier to negotiate with the peer device.

5. Select **Apply** to save changes.

Enable BFD on interfaces by selecting **[Edit]**, setting **BFD for OSPF** to **Enabled**, and then clicking **Apply**.

Note

Bidirectional Forwarding can only be enabled on interfaces that already exist. OSPF must be enabled for the interfaces.

BFD

Menu Path: Routing > BFD

This page lets you manage Bidirectional Forwarding Detection (BFD) for your device.

This page includes these tabs:

- Settings
- Status

BFD Settings

Menu Path: Routing > BFD - Settings

This page lets you configure Bidirectional Forwarding Detection (BFD) for your device and allows you to specify which interface to apply BFD to.

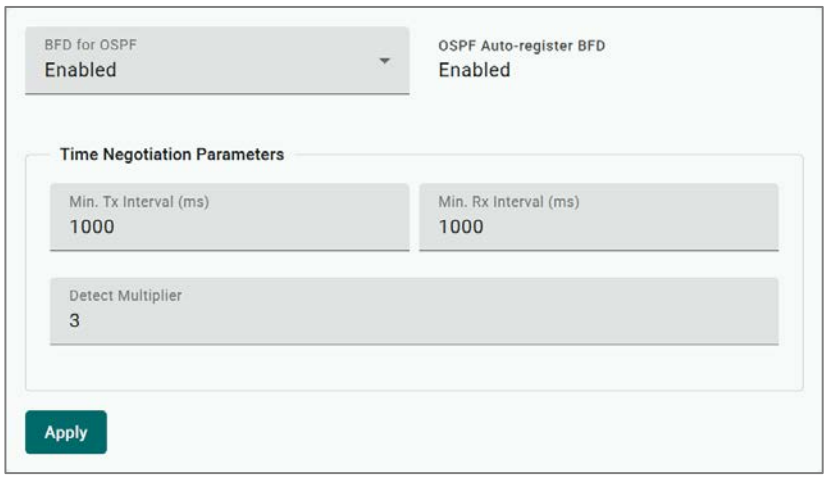
BFD Settings

Note

The transmit interval that will be used with a peer is the highest value between the device's Min. Tx Interval and the peer's Min. Rx Interval.

The detection interval that will be used with a peer is the highest value between the device's Min. Rx Interval and the peer's Min. Tx Interval, multiplied by the peer's Detect Multiplier.

If a BFD packet is not received from the peer within the detection interval, a link failure will be detected.



UI Setting	Description	Valid Range	Default Value
BFD for OSPF	Enable or disable use of BFD for OSPF.	Enabled/Disabled	Disabled
Min. Tx Interval (ms)	Specify the minimum Tx interval in milliseconds between sending BFD packets.	500 to 10000	1000
Min. Rx Interval (ms)	Specify the minimum Rx interval in milliseconds for receiving BFD packets.	500 to 10000	1000
Detect Multiplier	Specify the detect multiplier to use. This is used to determine the detect time.	3 to 50	3

BFD-OSPF Interface Settings



UI Setting	Description
Interface Name	Shows the name of the interface.
Interface Alias	Shows the alias of the interface.
IP Address	Shows the IP address of the interface.

UI Setting	Description
BFD to OSPF	Shows whether BFD for OSPF is enabled on the interface.

Edit BFD-OSPF Interface Settings

Menu Path: Routing > BFD - Settings

Clicking the **Edit (✎)** icon for an interface on the **Routing > BFD - Settings** page will open this dialog box. This dialog lets you configure the BFD-OSPF settings for the interface.

Click **Apply** to save your changes.



UI Setting	Description	Valid Range	Default Value
BFP to OSPF	Enable or disable BFD to OSPF for the interface.	Enabled / Disabled	Disabled

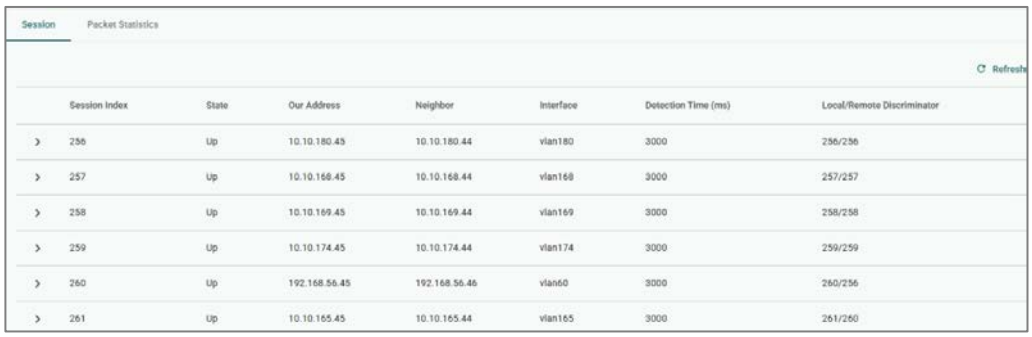
BFD Status

Menu Path: Routing > BFD - Status

This page lets you view the current BFD status of your device.

Session

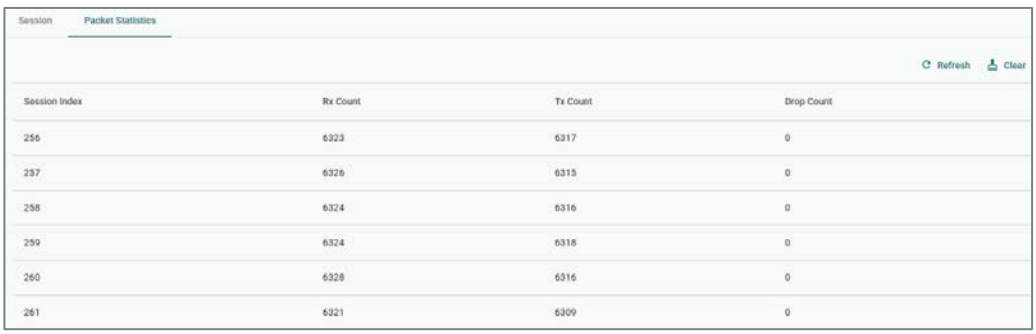
When **Session** is selected, this information will appear.



UI Setting	Description
Session Index	Shows the ID for the BFD session.
State	Shows the state of the BFD session.
Our Address	Shows the local IP address used to establish the BFD session.
Neighbor	Shows the peer IP address for the BFD session.
Interface	Shows the interface this BFD session is operating on.
Detection Time (ms)	Shows the amount of time in milliseconds the local system will wait for a valid BFD control packet from the peer before declaring the BFD session is down.
Local/Remote Discriminator	Shows the local device's and the peer's discriminators that uniquely identify the BFD session.

Packet Statistics

When **Packet Statistics** is selected, this information will appear.



UI Setting	Description
Session Index	Shows the ID for this BFD session.
Rx Count	Shows the number of BFD control packets that were received and associated with this BFD session.
Tx Count	Shows the number of BFD control packets transmitted by this BFD session to the peer.
Drop Count	Shows the number of received BFD control packets that were dropped due to validation failure or session mismatch.

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 User Accounts for more information on user accounts.

Settings	Admin	Supervisor	User
Device Security			
Login Policy	R/W	R	R
Trusted Access	R/W	R	R
SSH & SSL	R/W	R/W	-
Network Security			
IEEE 802.1X	R/W	R/W	R
MAC Authentication Bypass	R/W	R/W	R
MACsec	R/W	R/W	R
Port Security	R/W	R/W	R
Traffic Storm Control	R/W	R/W	R
Access Control List	R/W	R/W	R

Settings	Admin	Supervisor	User
Network Loop Protection	R/W	R/W	R
Binding Database	R/W	R/W	R
DHCP Snooping	R/W	R/W	R
IP Source Guard	R/W	R/W	R
Dynamic ARP Inspection	R/W	R/W	R
Authentication			
Login Authentication	R/W	-	-
RADIUS	R/W	-	-
TACACS+	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.

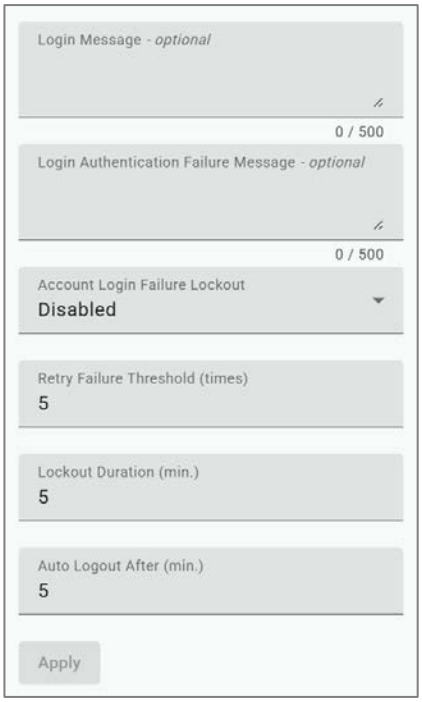
Login Policy

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



UI Setting	Description	Valid Range	Default Value
Login Message	Specify the welcome message to display when users log in to the device.	0 to 500 characters	N/A
Login Authentication Failure Message	Specify the message to display if the user fails to log in. **⚠ Warning** The Login Authentication Failure Message should not include information about passwords or other sensitive information.	0 to 500 characters	N/A

UI Setting	Description	Valid Range	Default Value
Account Login Failure Lockout	Enable or disable the lockout function, which will temporarily prevent users from logging in for the **Lockout Duration** after the **Retry Failure Threshold** is exceeded. This can be useful for preventing brute force attacks.	Enabled / Disabled	Disabled
Retry Failure Threshold (times)	Specify the number of login retry attempts allowed before the user is locked out for the **Lockout Duration**.	1 to 10	5
Lockout Duration (min.)	Specify the lockout duration in minutes during which a locked-out user will be unable to log in.	1 to 10	5
Auto Logout After (min.)	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 enabled 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 ***[Create]***.

   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

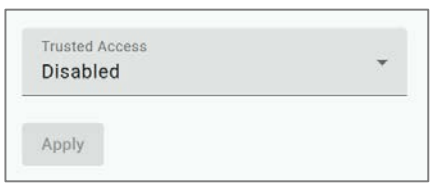
Menu Path: Security > Device Security > Trusted Access

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

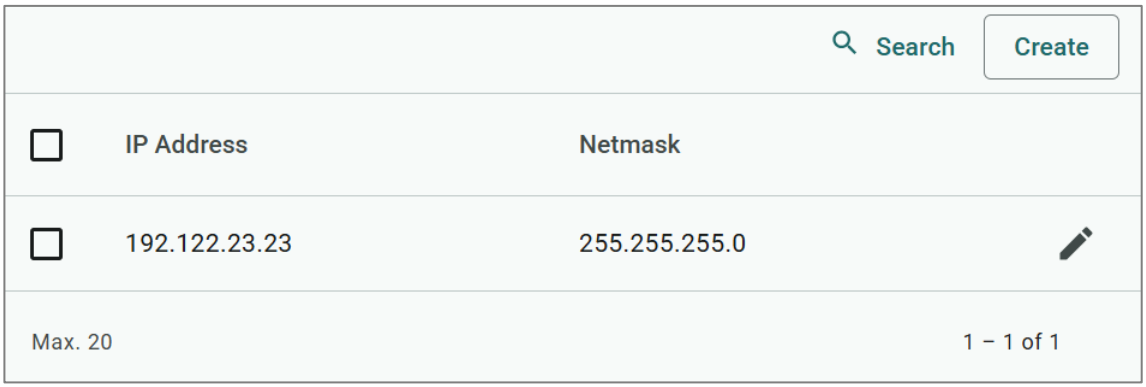
You can create up to 20 trusted IP entries.

Trusted Access Settings



UI Setting	Description	Valid Range	Default Value
Trusted Access	Enable or disable the Trusted IP List. **Enabled:** Only IP addresses in the Trusted IP List can access the device. **Disabled:** Any IP address can access the device. **Note** Trusted Access cannot be enabled if there are no entries in the Trusted Access List. **Warning** 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.	Enabled / Disabled	Disabled

Trusted Access List



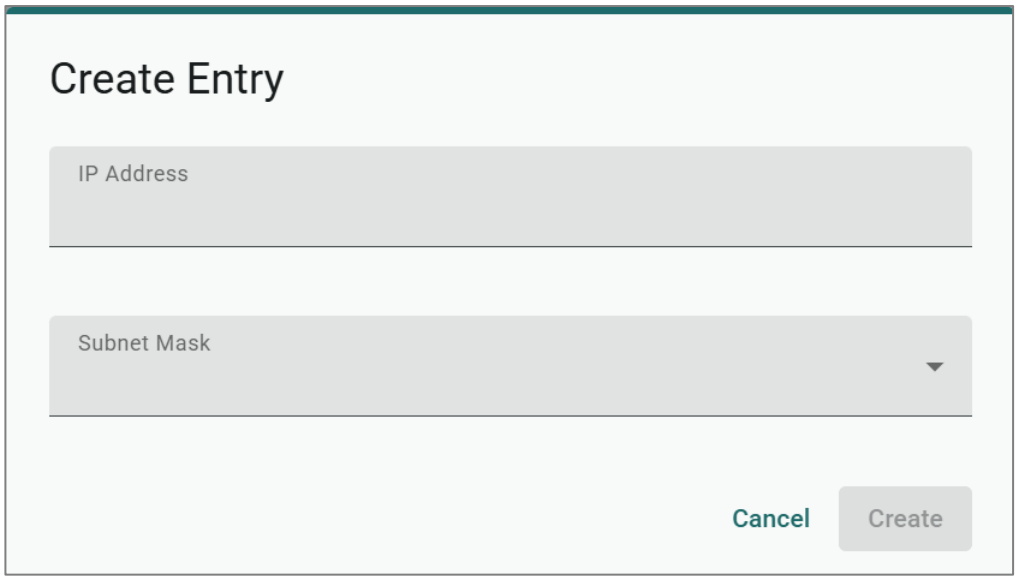
UI Setting	Description
IP Address	Shows the IP address of the Trusted IP entry.
Subnet Mask	Shows the netmask of the Trusted IP entry.

Trusted Access - Create Entry

Menu Path: Security > Device Security > Trusted Access

Clicking the **Create** button 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.



UI Setting	Description	Valid Range	Default Value
IP Address	Specify the IP address of the trusted host(s).	Valid IP address	N/A
Subnet Mask	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



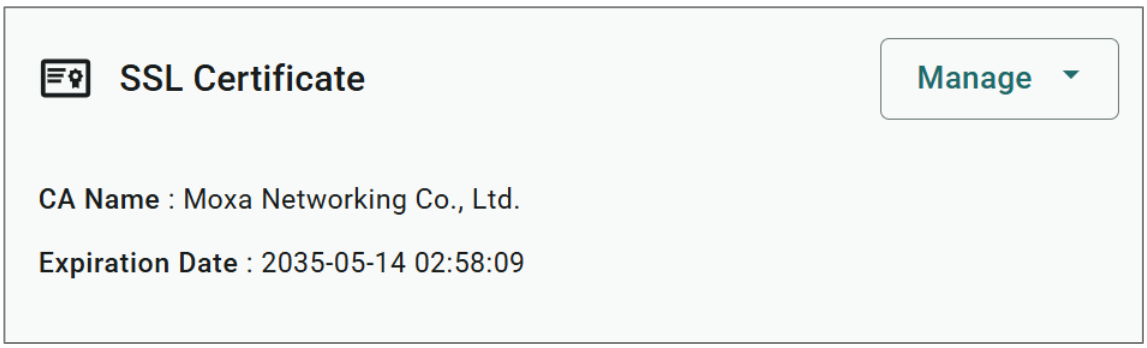
UI Setting	Description	Valid Range	Default Value
Regenerate SSH Key	Click **Regenerate** to regenerate the SSH key. **Warning** Regenerating the SSH key will restart the device's system services and will make the device temporarily unavailable.	N/A	N/A

SSL

Menu Path: Security > Device Security > SSH & SSL - SSL

This page lets you manage your device's SSL certificate.

Certificate Information



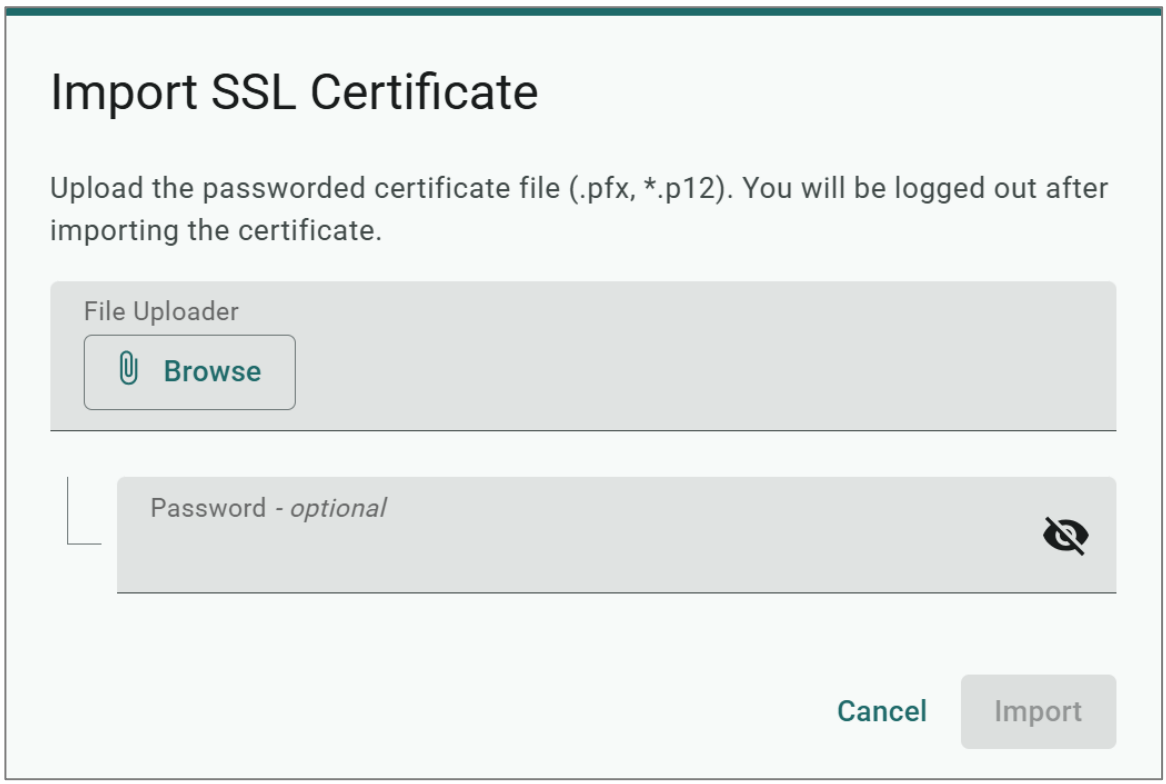
UI Setting	Description
CA Name	Shows the CA name of the SSL certificate.
Expiration Date	Shows when the current certificate will expire.

Import SSL Certificate

Menu Path: Security > Device Security > SSH & SSL - SSL

Clicking the **Manage** button on the **Security > Device Security > SSH & SSL - SSL** page and selecting **Import SSL Certificate** will open this dialog box. This dialog lets you import a SSL certificate.

Click **Import** to save your changes and add the new SSL certificate.



UI Setting	Description	Valid Range	Default Value
File Uploader	Select and upload an SSL certificate file (.pfx, *.p12) from your computer.	N/A	N/A

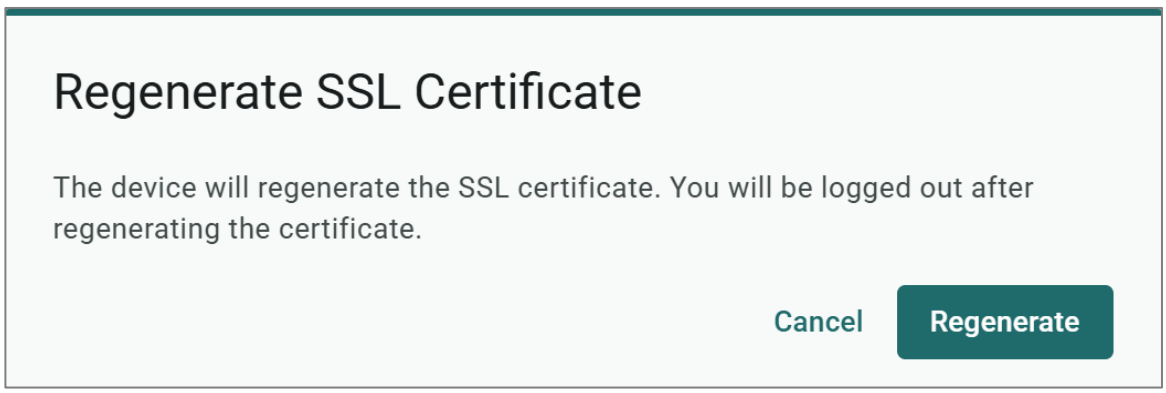
UI Setting	Description	Valid Range	Default Value
Password	Specify the password for the selected SSL certificate, if applicable.	N/A	N/A

Regenerate SSL Certificate

Menu Path: Security > Device Security > SSH & SSL - SSL

Clicking the **Manage** button on the **Security > Device Security > SSH & SSL - SSL** page and selecting **Regenerate SSL Certificate** will open this dialog box. This dialog lets you regenerate the SSL certificate.

Click **Regenerate** to regenerate the SSL certificate. You will be logged out after regenerating the certificate.



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
- MAC Security
- 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.

> **Note**
>
> This feature supports weaker authentication or encryption, and may not be secure over untrusted networks. Take appropriate security precautions.

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:

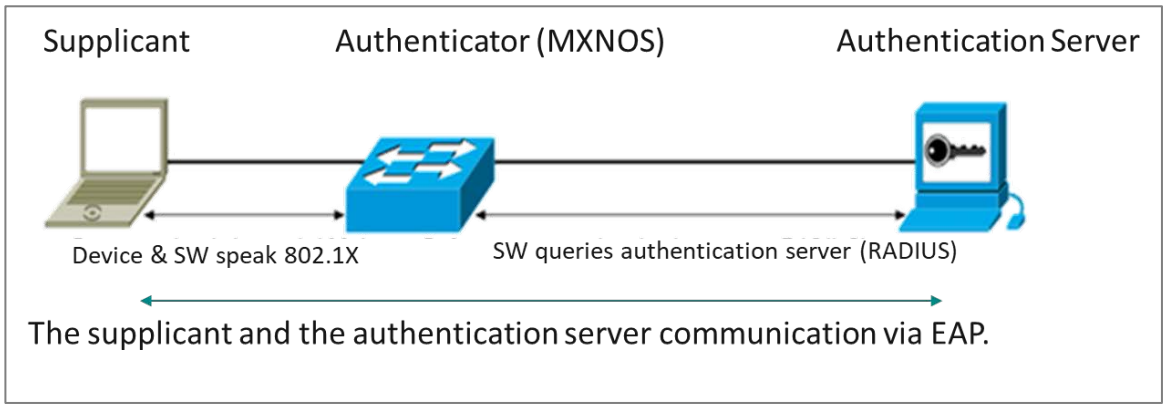
- Supplicant: The client device (e.g., laptop, smartphone) seeking network access.
- Authenticator: The network device (e.g., switch, wireless access point) that controls access to the network ports.
- Authentication Server: A server that performs the actual authentication of the supplicant. It could 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.

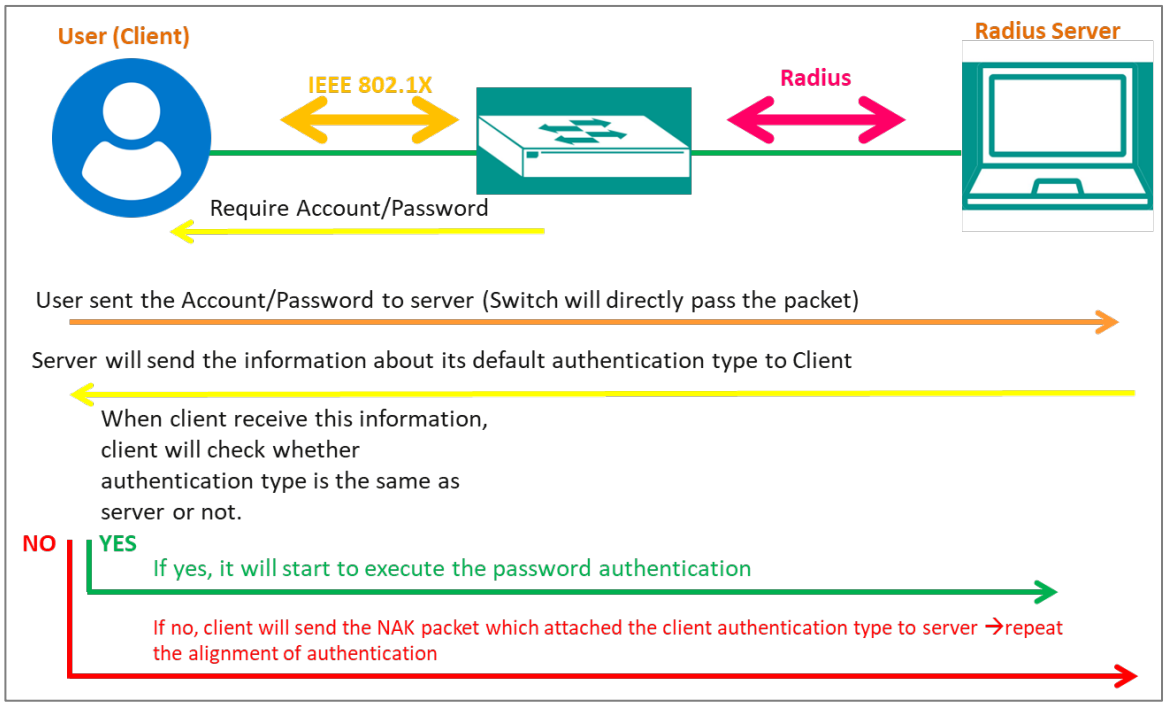


Note

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:

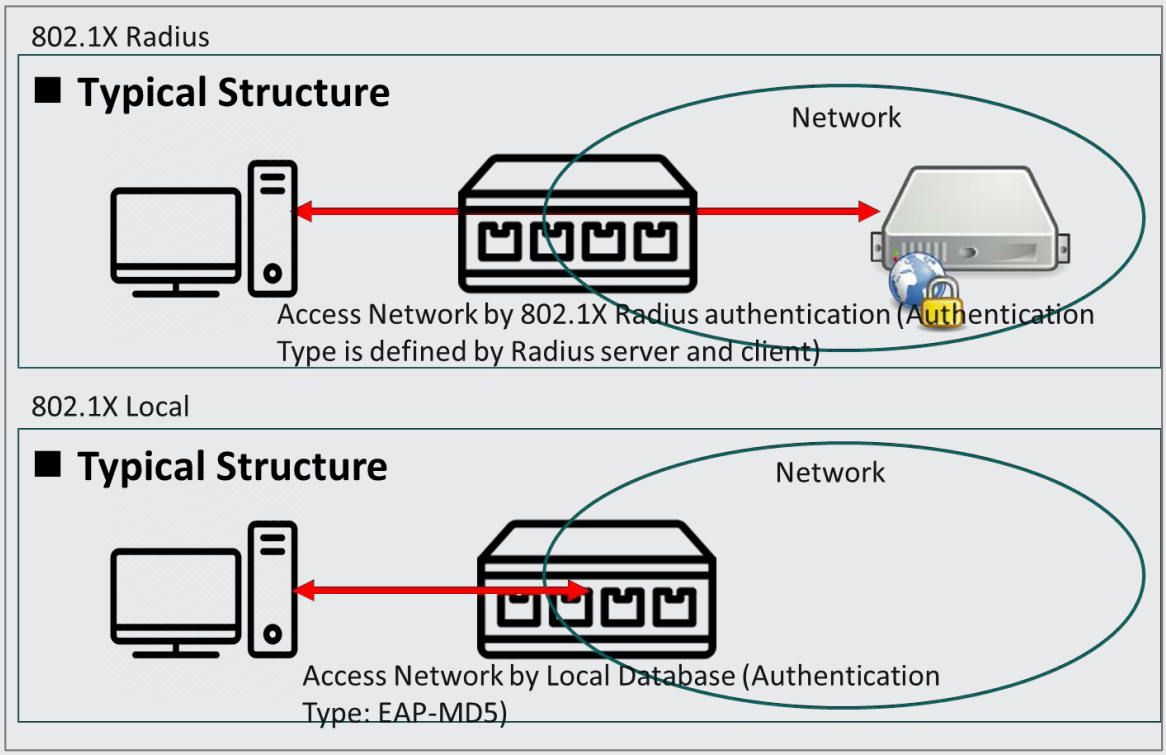


1. Initialization: The supplicant sends an EAPOL (Extensible Authentication Protocol Over LAN) start message to the authenticator.
2. Authentication Request: The authenticator replies with an EAP Request/Identity message, prompting the supplicant to provide its identity.
3. Identity Response: The supplicant 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

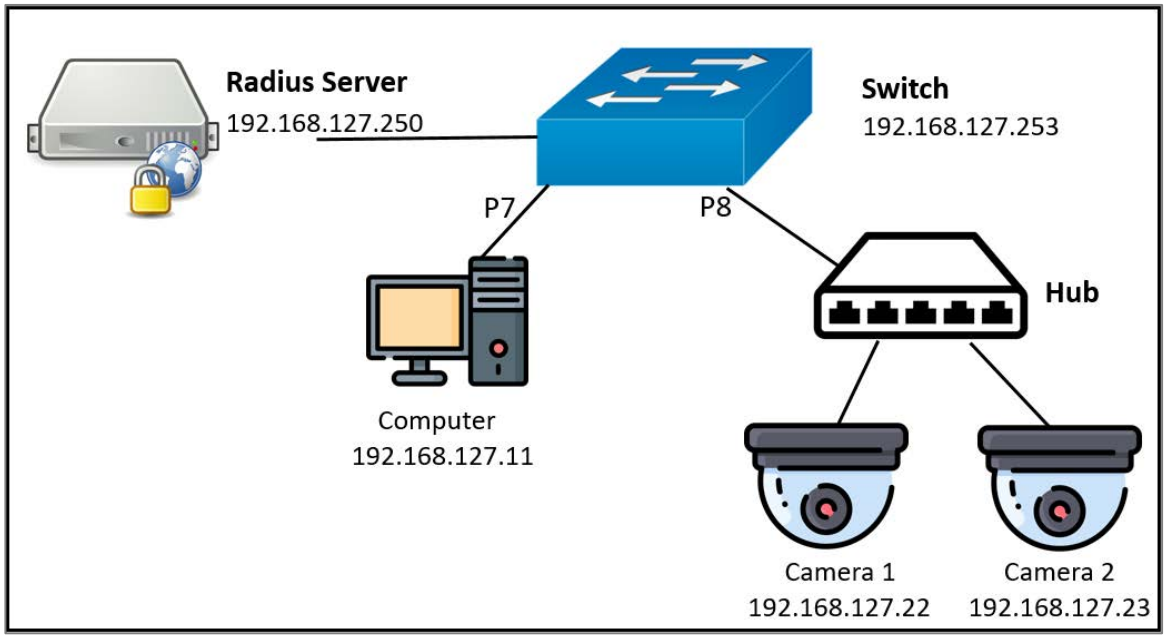
Authentication can also be initiated by the authenticator. Ordinarily, supplicants initiate the authentication process, with an EAPOL-Start frame sent to the authenticator. When the authenticator initiates the authentication process (either on its own, or on receipt of an EAPOL-Start frame), it sends an EAP Request/Identity frame to ask for the username of the supplicant.



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
Server IP Address 1	192.168.127.11
Auth Port	1812
Share Key	Type your key here
Timeout	**5**
Retransmit	**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.

Note

The following authentication protocols are supported:

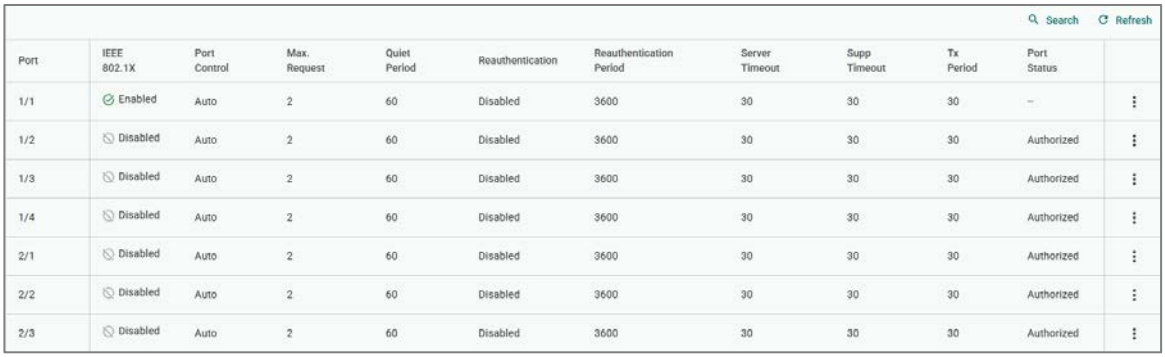
- EAP-MD5
- EAP-PEAP
- EAP-TLS
- EAP-MSCHAPv2

IEEE 802.1X Settings



UI Setting	Description	Valid Range	Default Value
IEEE 802.1X	Enable or disable IEEE 802.1X authentication. **Note** As of MX-NOS v5.0, enabling IEEE 802.1X allows VLAN assignment through a RADIUS server, but the VLAN must already exist.	Enabled / Disabled	Disabled
Authentication Mode	Specify the authentication mode to use. • **RADIUS**: Use a RADIUS server for authentication. • **Local Database**: Use the local database for authentication.	RADIUS / Local Database	Local Database

IEEE 802.1X List



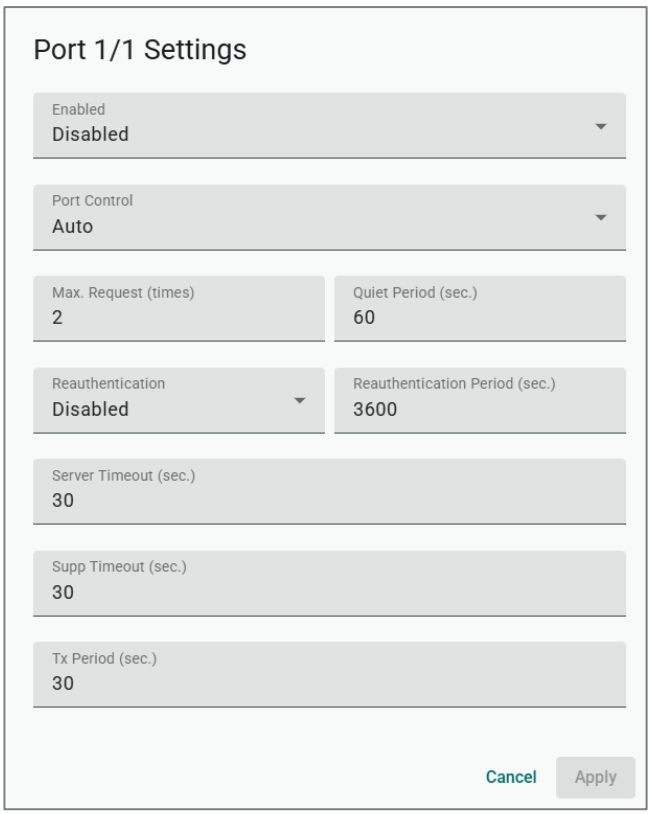
UI Setting	Description
Port	Shows the port number the entry is for.
IEEE 802.1X	Shows whether IEEE 802.1X is enabled for the port.
Port Control	Shows the port control method used for the port.
Max. Request	Shows the maximum number of re-authentication requests allowed for the port.
Quiet Period	Shows 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.
Reauthentication	Shows whether IEEE 802.1X reauthentication is enabled for the port.
Reauthentication Period **(Only in Advanced Mode)**	Shows the amount of time in seconds to wait in between reauthentication attempts for the port.
Server Timeout **(Only in Advanced Mode)**	Shows the amount of time in seconds the device will try to retransmit packets to an authentication server.
Supp Timeout **(Only in Advanced Mode)**	Shows the amount of time in seconds the device will try to retransmit packets to a supplicant, such as a client PC.
Tx Period **(Only in Advanced Mode)**	Shows the amount of time in seconds the device will try to retransmit the data to a client.
Port Status	Shows the current authorization status of the port.

IEEE 802.1X - Edit Port Settings

Menu Path: Security > Network Security > IEEE 802.1X - General

Clicking the **Actions (⋮)** icon then **Edit** 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.



UI Setting	Description	Valid Range	Default Value
Enabled	Enable or disable IEEE 802.1X authentication for the port.	Enabled / Disabled	Disabled

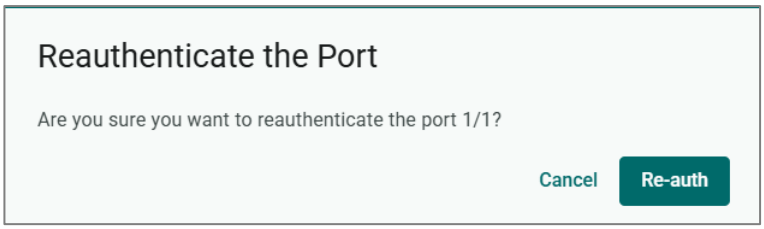
UI Setting	Description	Valid Range	Default Value
Port Control	Select the port control method to use for the port. • **Force Unauthorized**: The controlled port will stay in the unauthorized state. • **Auto**: The controlled port will be set to the authorized or unauthorized state based on the outcome of an authentication exchange between the supplicant and the authentication server. • **Force Authorized**: The controlled port will stay in the authorized state.	Force Unauthorized / Auto / Force Authorized	Auto
Max. Request	Specify how many times to attempt reauthentication for the port.	1 to 10	2
Quiet Period	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
Reauthentication	Enable/disable IEEE 802.1X reauthentication for the port.	Enabled / Disabled	Disabled
Reauthentication Period **(Only in Advanced Mode)**	Specify the amount of time in seconds to wait in between reauthentication attempts for the port.	1 to 65535	3600
Server Timeout **(Only in Advanced Mode)**	Specify the amount of time in seconds the device will try to retransmit packets to an authentication server.	1 to 65535	30
Supp Timeout **(Only in Advanced Mode)**	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
Tx Period **(Only in Advanced Mode)**	Specify the amount of time in seconds the device will try to retransmit the data to a client.	1 to 65535	30
Copy configurations to ports	Select the ports you want to copy this configuration to.	Drop-down list of ports	N/A

IEEE 802.1X - Reauthenticate Port Settings

Menu Path: Security > Network Security > IEEE 802.1X - General

Clicking the **Actions (⋮)** icon then **Reauthenticate** for a port on the **Security > Network Security > IEEE 802.1X - General** page will open this dialog box. This dialog lets you reauthenticate the IEEE 802.1X settings for the port.

Click **Apply** to save your changes.



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.

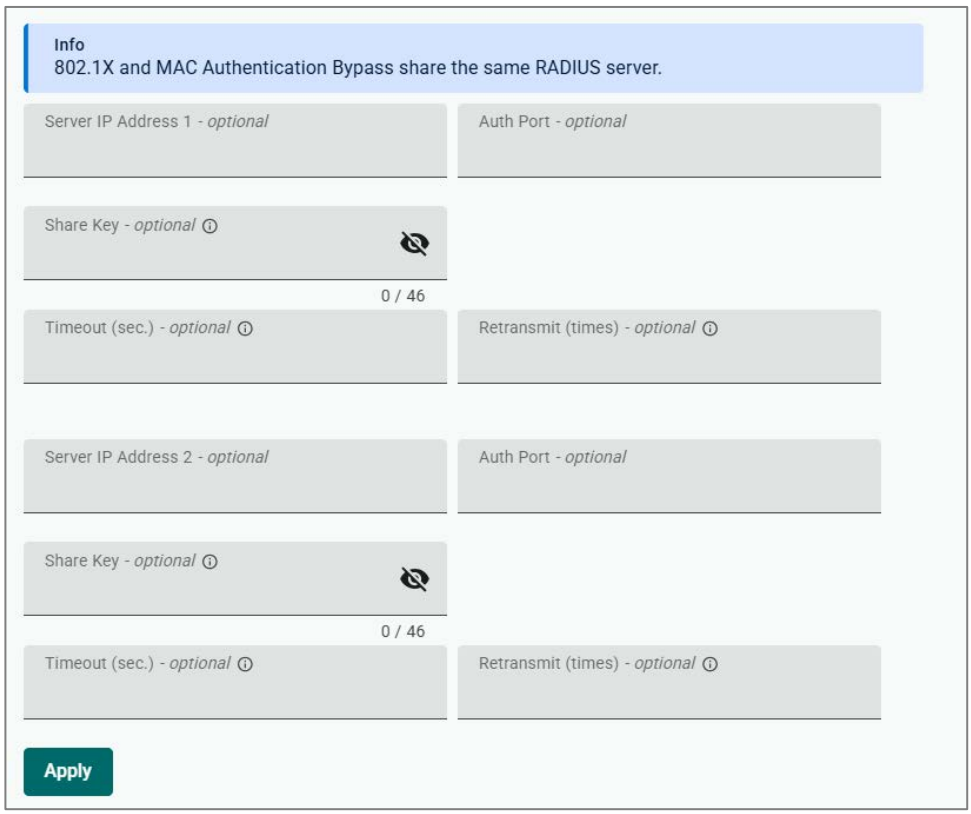
Note

This feature supports weaker authentication or encryption, and may not be secure over untrusted networks. Take appropriate security precautions.

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.



UI Setting	Description	Valid Range	Default Value
Server IP Address 1 / 2	Specify the IP address of the 1st/2nd server.	Valid IP address	N/A
Auth Port	Specify the authentication port number for the RADIUS server.	1 to 65535	N/A
Share Key	Specify the share key for the server.	0 to 46 characters	N/A
Timeout	Specify how long to wait in seconds before a device is logged out.	1 to 120	N/A
Retransmit	Specify how many times to retry data transmission.	1 to 254	N/A

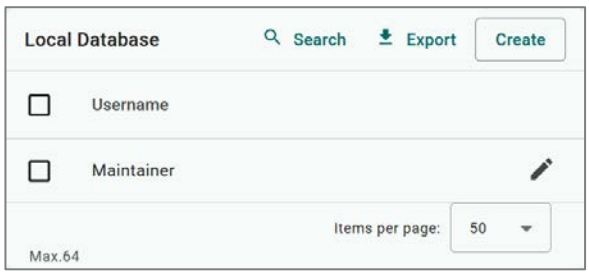
IEEE 802.1X - Local Database

Menu Path: Security > Network Security > IEEE 802.1X - Local Database

This page lets you create local database user accounts to use with IEEE 802.1X authentication.

Limitations

You can create up to 64 IEEE 802.1X local database accounts.



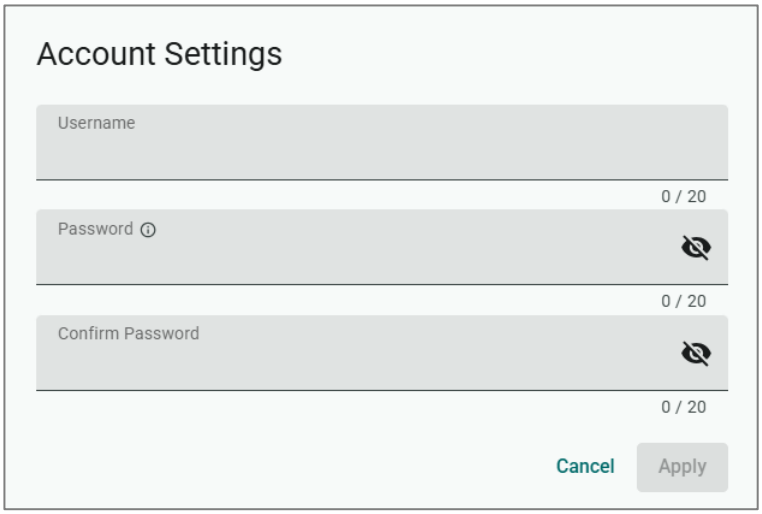
UI Setting	Description
Username	Shows the username of the account.

IEEE 802.1X - Local Database - Account Settings

Menu Path: Security > Network Security > IEEE 802.1X - Local Database

Clicking **Create** 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.



UI Setting	Description	Valid Range	Default Value
Username	Specify the username for this account.	1 to 20 characters	N/A
Password	Specify the password for this user account.	4 to 20 characters	N/A
Confirm Password	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.

> **Note**
>
> This feature supports weaker authentication or encryption, and may not be secure over untrusted networks. Take appropriate security precautions.

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.

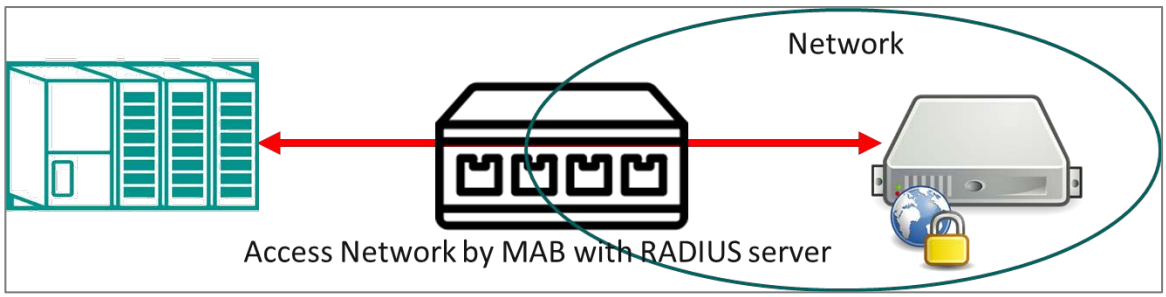
When to Use MAB

- **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 adequete 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:

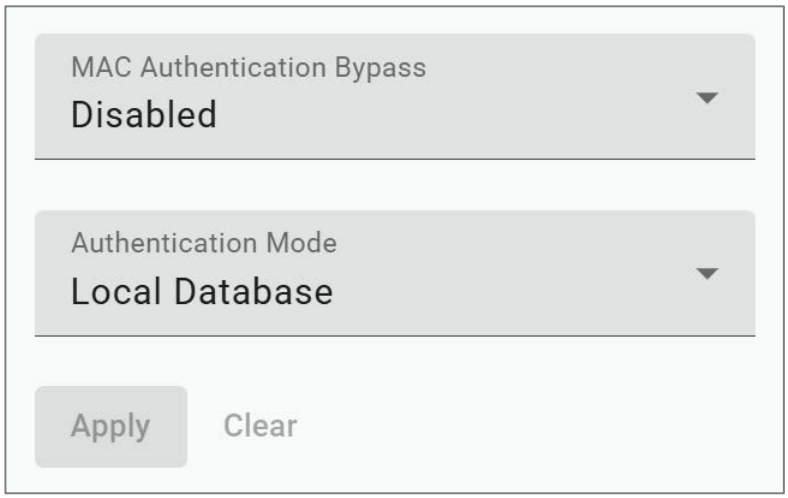
- General
- RADIUS
- Local Database

MAC Authentication Bypass - General

Menu Path: Security > Network Security > MAC Authentication Bypass - General

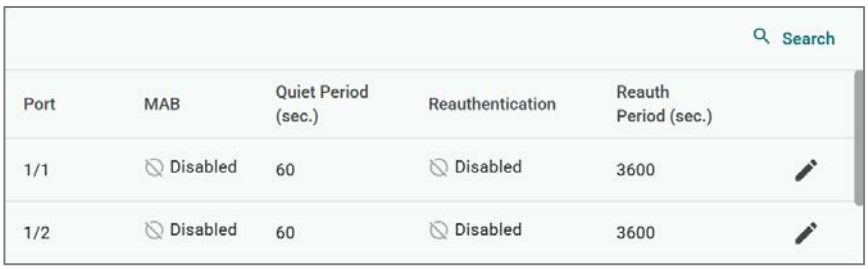
This page lets you configure general settings for MAC authentication bypass.

MAC Authentication Bypass Settings



UI Setting	Description	Valid Range	Default Value
MAC Authentication Bypass	Enable or disable MAC authentication bypass (MAB).	Enabled / Disabled	Disabled
Authentication Mode	Specify the authentication mode for MAC authentication bypass.	RADIUS / Local Database	Local Database
Authentication Type **(If Authentication Mode is RADIUS)**	Select which authentication type to use for RADIUS authentication.	CHAP / PAP / MS-CHAPv2	CHAP

MAC Authentication Bypass List



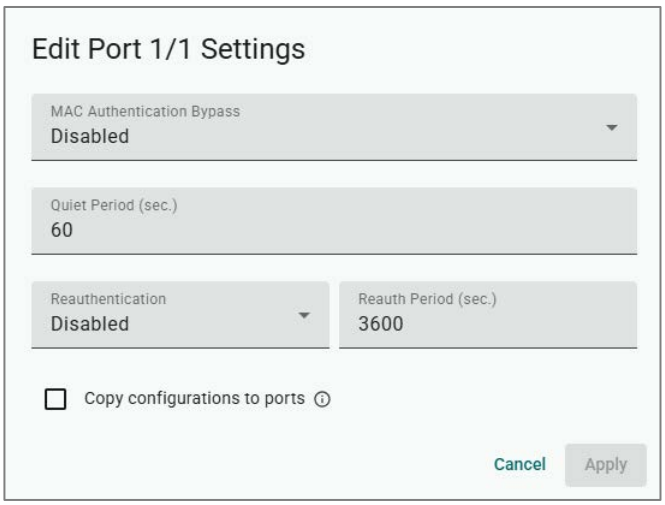
UI Setting	Description
Port	Shows the port number the entry is for.
MAB	Shows whether MAC Authentication Bypass is enabled for the port.
Quiet Period	Show the amount of time in seconds the device will remain in a quiet state following a failed authentication exchange with a client through the port.
Reauthentication	Shows whether IEEE 802.1X reauthentication is enabled for the port.
Reauthentication Period	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.



UI Setting	Description	Valid Range	Default Value
MAC Authentication Bypass	Enable or disable MAC Authentication Bypass for the port.	Enabled / Disabled	Disabled
Quiet Period	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.
Reauthentication	Enable or disable IEEE 802.1X reauthentication for the port.	Enabled / Disabled	Disabled
Reauthentication Period	Specify the amount of time in seconds to wait in between reauthentication attempts for the port.	60 to 65535	3600 sec.
Copy configurations to ports	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

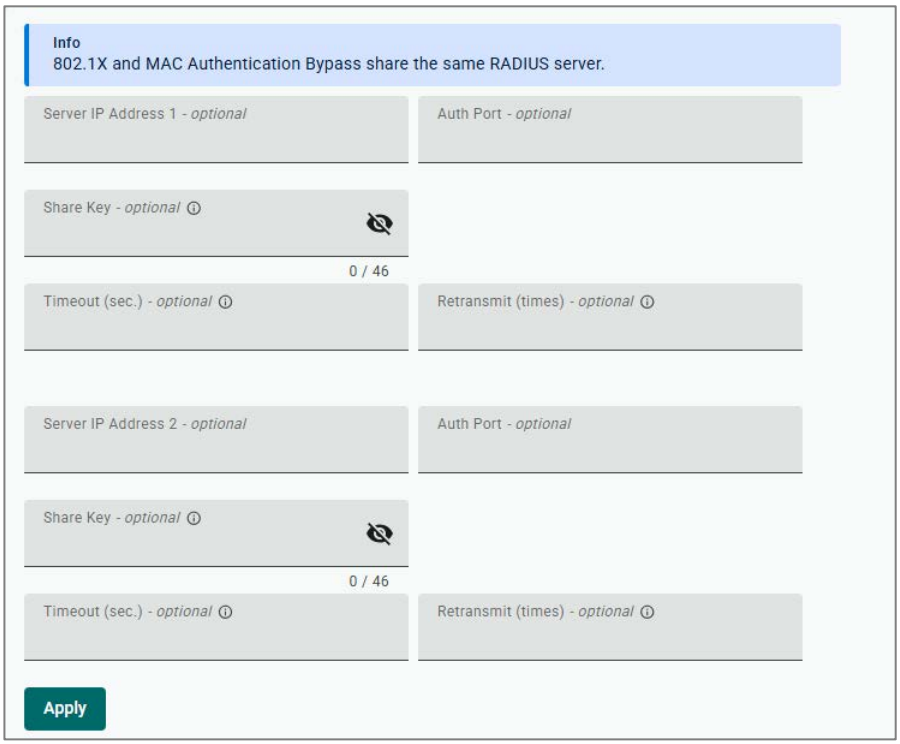
This page lets you configure the RADIUS settings for MAC authentication bypass.

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	Valid Range	Default Value
Server IP Address 1 / 2	Specify the IP address of the 1st/2nd server.	Valid IP address	N/A
Auth Port	Specify the authentication port number for the RADIUS server.	1 to 65535	N/A
Share Key	Specify the share key for the server.	0 to 46 characters	N/A
Timeout	Specify how long to wait in seconds before a device is logged out.	1 to 120	N/A

UI Setting	Description	Valid Range	Default Value
Retransmit	Specify how many times to retry data transmission.	1 to 254	N/A

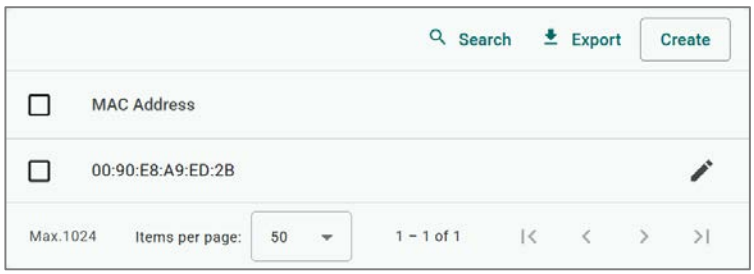
MAC Authentication Bypass - Local Database

Menu Path: Security > Network Security > MAC Authentication Bypass - Local Database

This page lets you manage local database entries for MAC authentication bypass.

Limitations

You can create up to 1024 MAC authentication bypass local database entries.



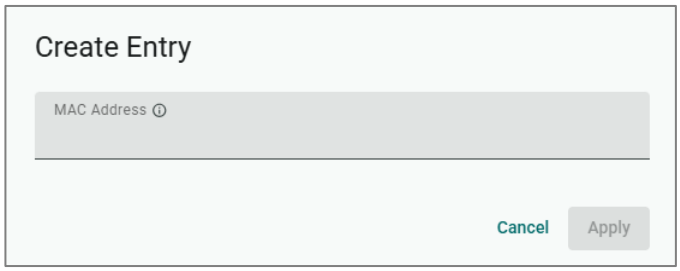
UI Setting	Description
MAC Address	Shows the MAC address used for MAC authentication bypass.

MAC Authentication Bypass - Local Database - Create Entry

Menu Path: Security > Network Security > MAC Authentication Bypass - Local Database

Clicking **Create** 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
MAC Address	Specify the MAC address to use for MAC authentication bypass.	Valid unicast MAC address	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.

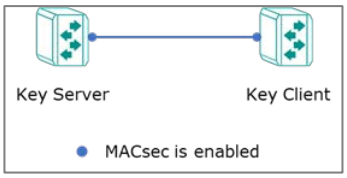
MAC security involves two standards: IEEE802.1AE and 802.1X. The frame format for data encapsulation, encryption, and authentication is defined in IEEE802.1AE. MACsec Key Agreement (MKA), a key management protocol, is defined in IEEE 802.1X-2010. MKA provides agreement for MAC security policy and key 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.

> **Note**
>
> The assignment of Key Server roles is determined by an election process based on the Key Server Priority setting. Connected switches will compare their priority values to automatically negotiate and determine their respective roles. MACsec interoperability requires peer devices support the same key server selection mechanism.

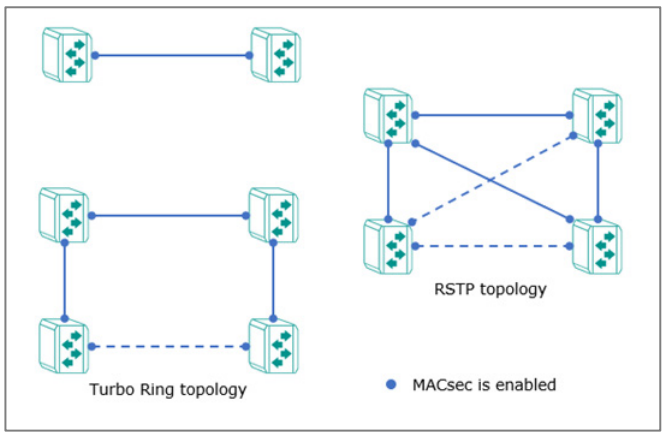
To ensure data traffic is transmitted securely, all data traffic ports must enable MAC security.



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.

Note

IEEE 802.1X must be enabled before MAC Security can be configured.

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
Status	**Enabled**
Participant CKN	Specify a Connectivity association Key Name of 1-16 characters.
Participant CAK	Select **Change CKN and CAK** to adjust. Specify a Connectivity association Key of 1-16 characters.
Key Server Priority	Specify the Key server priority value for key server election between 0-112. Smaller values are higher priority.

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 sec on all relevant devices and ports.

MAC Security (MACsec)

Menu Path: Security > Network Security > MACsec

This page lets you manage MAC security for your device.

This page includes these tabs:

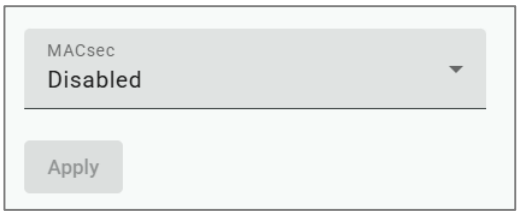
- General
- MKA Status

MACsec - General

Menu Path: Security > Network Security > MACsec - General

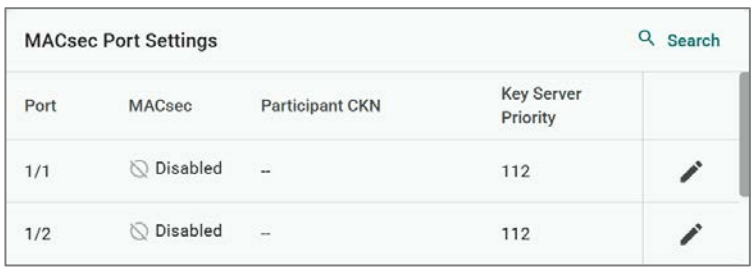
This section lets you configure MAC security for your device.

MACsec Settings



UI Setting	Description	Valid Range	Default Value
MACsec	Enable or disable MAC security (MACsec) for your device.	Enabled / Disabled	Disabled

MACsec Port Settings



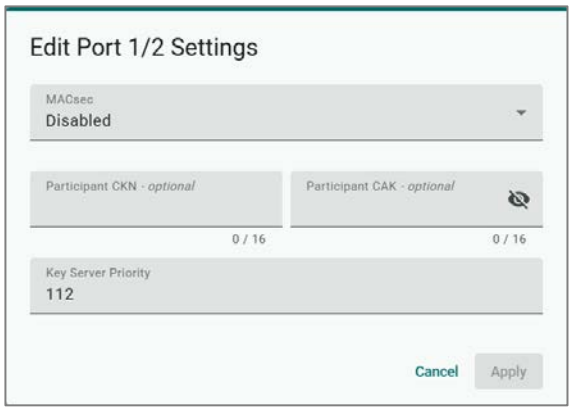
UI Setting	Description
Port	Shows the port this entry is for.
Status	Shows whether MAC security is enabled for the port.
Participant CKN	Shows the Connectivity association Key Name (CKN) configured for the port as the pre-shared key.
Key Server Priority	Shows the priority of the switch for key server election. Lower values will have higher priority.

Editing a MACsec Port

Menu Path: Security > Network Security > MACsec - General

Clicking the **Edit** (✎) icon for a port on the **Security > Network Security > MACsec - General** page will open this dialog box. This dialog lets you edit the port's MAC security settings.

Click **Apply** to save your changes.



UI Setting	Description	Valid Range	Default Value
MACsec	Enable or disable MAC security for this port.	Enabled / Disabled	Disabled

UI Setting	Description	Valid Range	Default Value
Participant CKN	Specify the Connectivity association Key Name (CKN) to use for the port. If a participant CKN and CAK have already been specified for the port, click **Change CKN and CAK** to edit them. **Note** • The CKN configured for this port should be the same as the connected port on the peer switch to enable MACsec for data exchange. • Multiple CKNs are not allowed for a single port. • Different CKNs on a device should be unique. • A CKN can only contain the letters a-z, A-Z, numbers 0-9, special characters @%^*()-_+={}[]:.,~$`, and cannot have any spaces. • CKNs and CAKs must be configured in pairs, and cannot be partially configured (such as configuring one, but not the other). • Deleting a CKN may also delete its corresponding CAK.	0 to 16 characters	N/A
Participant CAK	Specify the Connectivity Association Key (CAK) to use for the port. If a participant CKN and CAK have already been specified for the port, click **Change CKN and CAK** to edit them. **Note** • The CAK configured for this port should be the same as the connected port on the peer switch to enable MACsec for data exchange. • Multiple CAKs are not allowed for a single port. • Different CAKs on a device should be unique. • A CAK can only contain the letters a-z, A-Z, numbers 0-9, special characters @%^*()-_+={}[]:.,~$`, and cannot have any spaces. • CKNs and CAKs must be configured in pairs, and cannot be partially configured (such as configuring one, but not the other). • Deleting a CAK may also delete its corresponding CKN.	0 to 16 characters	N/A
Key Server Priority	Specify the priority of the switch for key server election. Lower values will have higher priority.	0 to 255	112

MAC Security - MKA Status

Menu Path: Security > Network Security > MACsec - MKA Status

This page lets you view the current MAC security status for your device.

MKA Status Port List



UI Setting	Description
Port	Shows the port this entry is for.
Key Server	Shows the key server selected for this entry.
Peer List Member Identifier (MI)	Shows the member identifier of the connected switch.
Peer List Message Number (MN)	Shows the message number received from the connected switch.
Secure Channel ID (SCI)	Shows the session ID for the channel to the other switch.
Peer List Type	Shows the peer list type. • **Potential Peer List**: The MI from the sender cannot be recognized by the receiver. • **Live Peer List**: 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.

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



UI Setting	Description	Valid Range	Default Value
Port Security	Enable or disable port security.	Enabled / Disabled	Enabled
Port Security Mode	Select a port security mode. **⚠ Warning** When changing the port security mode, all configured port security entries in the Static Port Lock/MAC Sticky tab will be deleted.	Static Port Lock / MAC Sticky	Static Port Lock

Port Security List - Static Port Lock

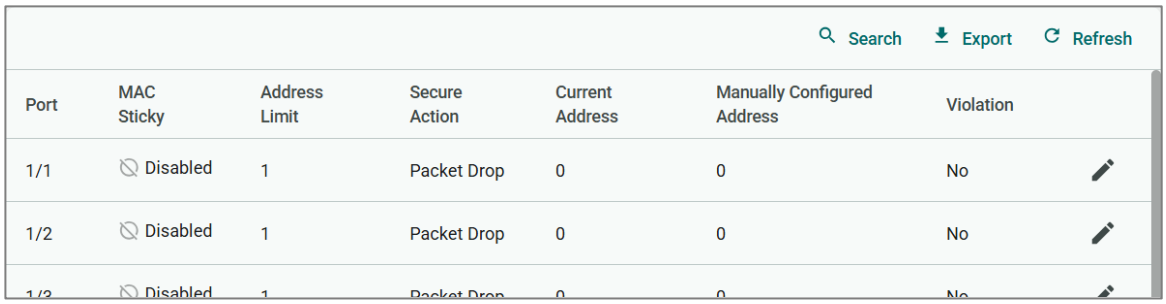
If **Port Security Mode** is set to **Static Port Lock**, the following table will appear.



UI Setting	Description
Port	Shows the port number the entry is for.
Static Port Lock	Shows whether static port lock is enabled for the port.
Manually Configured Address	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.



UI Setting	Description
Port	Shows the port number the entry is for.
MAC Sticky	Shows whether MAC Sticky mode is enabled for the port.
Address Limit	Shows the maximum number of MAC addresses to learn for the port.
Secure Action	Shows the action the device will take when the number of MAC addresses exceeds the address limit.

UI Setting	Description
Current Address	Shows the current number of MAC addresses learned for the port.
Manually Configured Address	Shows the number of manually configured MAC addresses for the port.
Violation	Shows whether there have been any violations for the port.

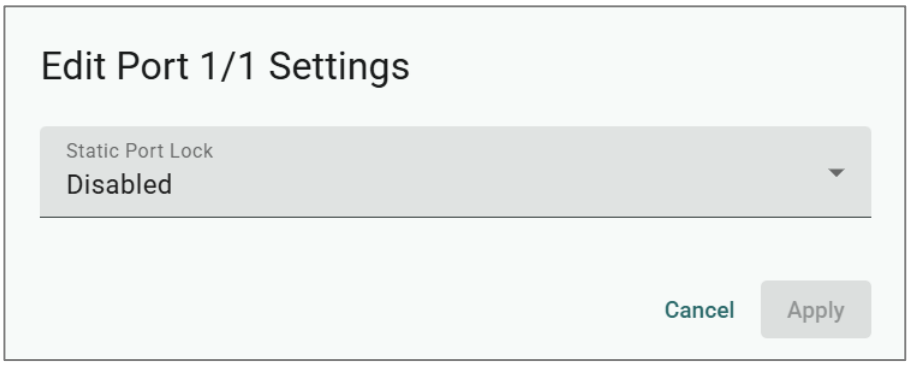
Port Security - Edit Port Settings

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.

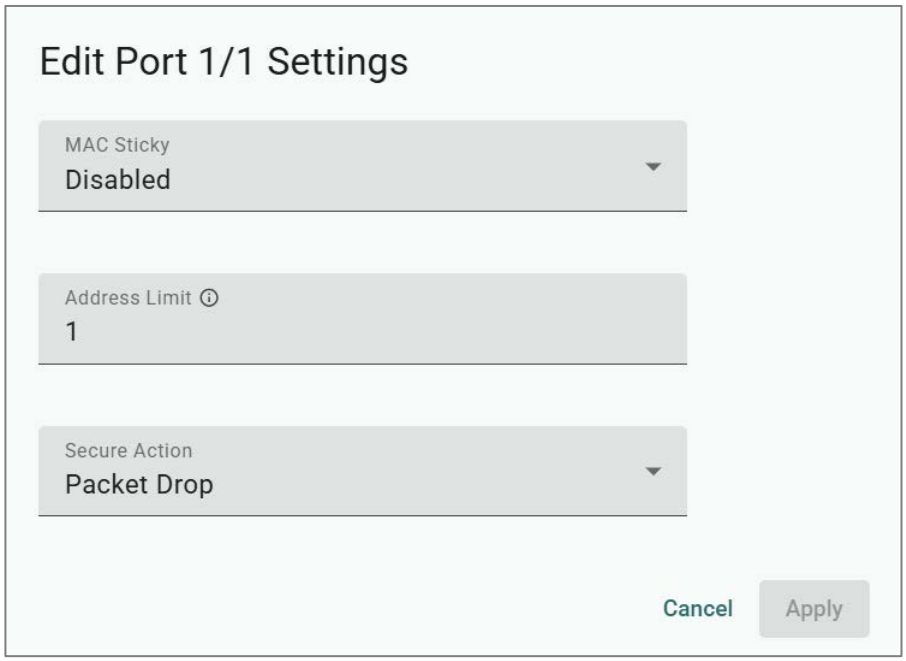
Click **Apply** to save your changes.

If **Port Security Mode** is set to **Static Port Lock**, the following dialog will appear when editing port security settings.



UI Setting	Description	Valid Range	Default Value
Static Port Lock	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.



UI Setting	Description	Valid Range	Default Value
MAC Sticky	Enable or disable MAC Sticky for the port.	Enabled / Disabled	Disabled
Address Limit	Specify the maximum number of the learned and configured MAC addresses allowed for the port. **Note** Changing the address limit will clear all currently configured MAC addresses for the port.	1 to 1001	1

UI Setting	Description	Valid Range	Default Value
Secure Action	Specify the action to take when a violation occurs. • **Port Shutdown**: The port will be shut down. • **Packet Drop**: Packets for the additional MAC addresses will be dropped. **Note** When using Port Shutdown, ports that are shut down follow this behavior: • If a port is shut down due to a violation and then an admin saves the device's configuration, the port will remain down after a system reboot. • If a port is shut down due to a violation and an admin does not save the device's configuration, the port will stay down until re-enabled by an admin or a system reboot.	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.

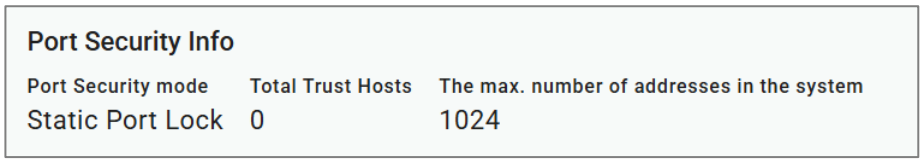
Note

This page 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



UI Setting	Description
Port Security mode	Shows the port security mode being used.
Total Trust Hosts	Shows the number of trusted hosts allowed to access the network.
The max. number of addresses in the system	Show the maximum number of MAC addresses allowed to be learned or specified for port security.

Static Port Lock - Port List



UI Setting	Description
Port	Shows the port number the entry is for.
VLAN ID	Shows the VLAN applied to the port.
MAC Address	Shows the MAC address of the device which is used as a reliable source for network access.
Type	Shows how the entry was created.

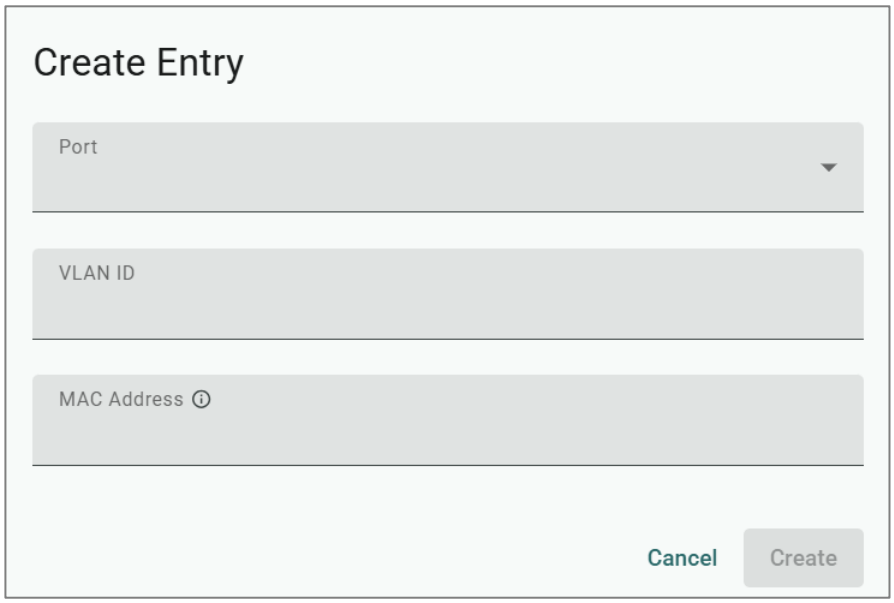
UI Setting	Description
Effective	Shows whether the entry is effective. **Note** If an entry is not effective, it may have an invalid interface set for it.

Static Port Lock - Create Entry

Menu Path: Security > Network Security > Port Security - Static Port Lock

Clicking **Create** 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 entry.



UI Setting	Description	Valid Range	Default Value
Port	Select the port to add an entry for.	Drop-down list of ports	N/A
VLAN ID	Specify the VLAN ID to use with the port.	Valid VLAN ID	N/A

UI Setting	Description	Valid Range	Default Value
MAC Address	Specify the MAC address of the device that will be used as the reliable source for network access.	Valid unicast 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 page will only appear when Port Security Mode is set to MAC Sticky.

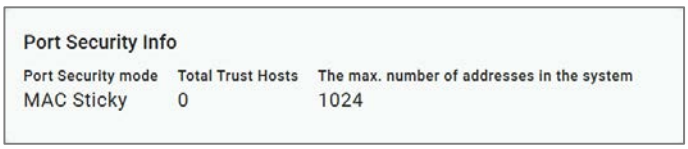
Note

MAC Sticky entries are not shown in the MAC address table; they are only shown on the Unable to render include or excerpt-include. Cycle detected. page.

Limitations

You can create up to 1024 MAC Sticky entries.

MAC Sticky - Port Security Info



UI Setting	Description
Port Security mode	Shows the port security mode being used.
Total Trust Hosts	Shows the number of trusted hosts allowed to access the network.
The max. number of addresses in the system	Show the maximum number of MAC addresses allowed to be learned or specified for port security.

MAC Sticky - Port List



UI Setting	Description
Port	Shows the port number the entry is for.

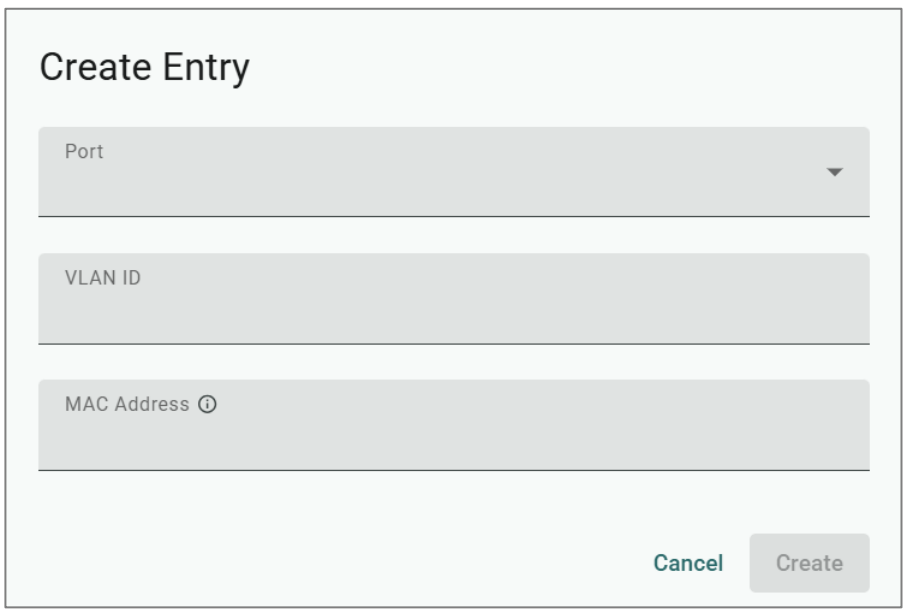
UI Setting	Description
VLAN ID	Shows the VLAN applied to the port.
MAC Address	Shows the MAC address of the device which is used as a reliable source for network access.
Type	Shows how the entry was created.
Effective	Shows whether the entry is effective. **Note** If an entry is not effective, it may have an invalid interface set for it.

MAC Sticky - Create Entry

Menu Path: Security > Network Security > Port Security - MAC Sticky

Clicking **Create** 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 entry.



UI Setting	Description	Valid Range	Default Value
Port	Select the port to add an entry for.	Drop-down list of ports	N/A
VLAN ID	Specify the VLAN ID to use with the port.	Valid VLAN ID	N/A
MAC Address	Specify the MAC address of the device that will be used as the reliable source for network access.	Valid unicast 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.



UI Setting	Description
Port	Shows the port number the entry is for.
Broadcast	Shows whether traffic storm control is enabled for broadcast packets for the port.
Multicast	Shows whether traffic storm control is enabled for multicast packets for the port.

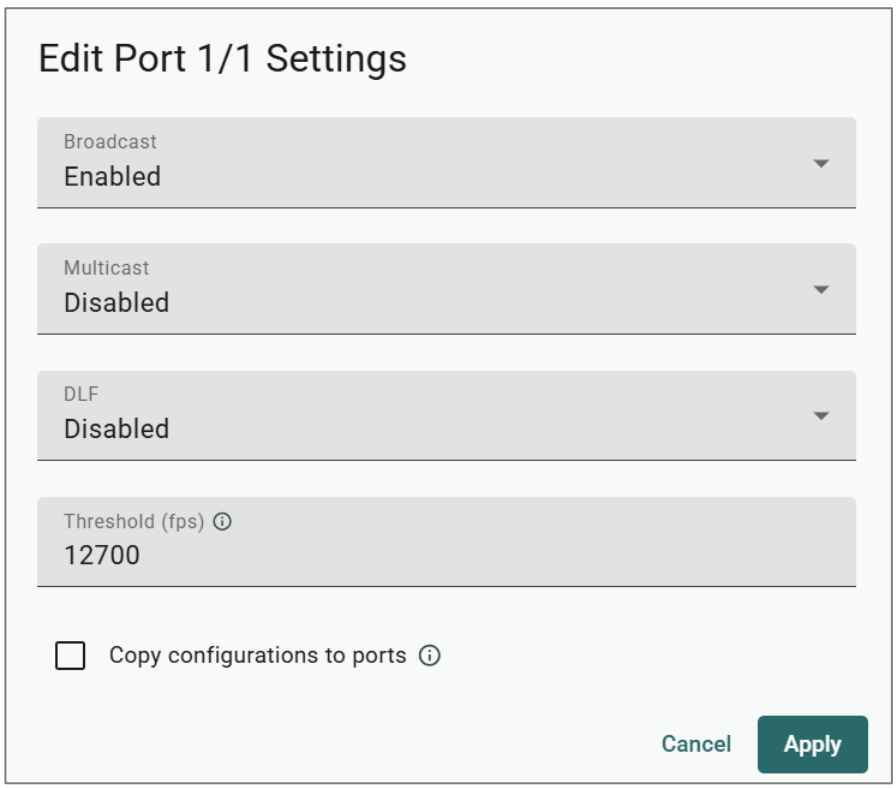
UI Setting	Description
DLF	Shows whether traffic storm control is enabled for DLF packets for the port.
Threshold	Shows the traffic storm threshold value in frames per second for the port.

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.



UI Setting	Description	Valid Range	Default Value
Broadcast	Enable or disable traffic storm control for broadcast packets for the port.	Enabled / Disabled	Disabled
Multicast	Enable or disable traffic storm control for multicast packets for the port.	Enabled / Disabled	Disabled
DLF	Enable or disable traffic storm control for DLF packets for the port.	Enabled / Disabled	Disabled
Threshold	Specify the threshold in frames per second to reach before detecting a traffic storm for the port.	625 to 14881000	12700 fps
Copy configurations to ports	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 control lists.

Access Control List



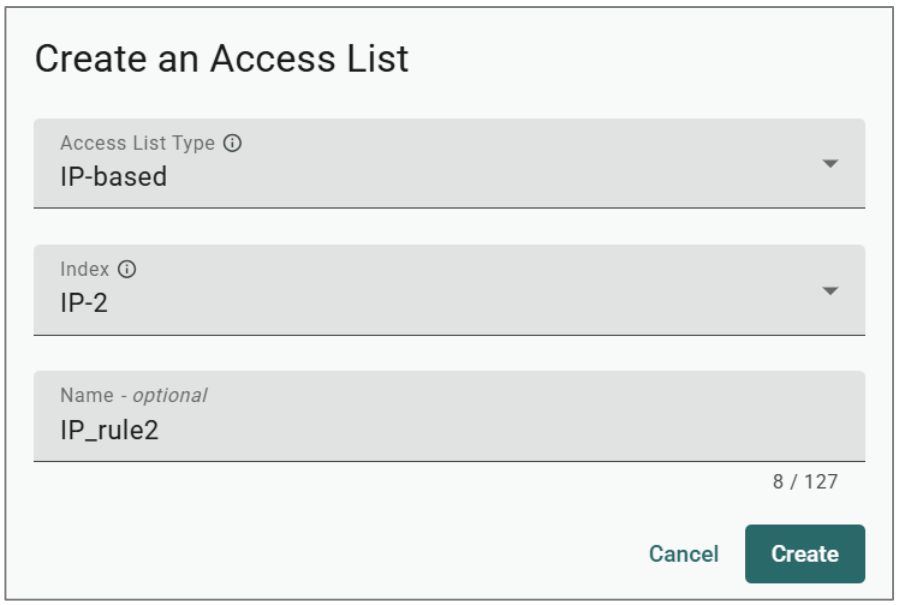
UI Setting	Description
Index	Shows the access list type and its index value.
Name	Shows the name of the access list.

Create an Access List

Menu Path: Security > Network Security > Access Control List - Settings

Clicking **Create** 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.



UI Setting	Description	Valid Range	Default Value
Access List Type	Specify the access list type to determine how it should control access.	IP-based / MAC-based	N/A
Index	Specify an index value for the access list. **Note** Priority is determined by two factors: index value and address type. Lower index values indicate higher priority. In cases where entries share the same index, MAC addresses take precedence over IP addresses.	Drop-down list of index values	N/A
Name	Specify a name for the access list.	0 to 127 characters	N/A

ACL Table Settings

You can switch to another ACL table by clicking on its name.



UI Setting	Description	Valid Range	Default Value
Active Interface Type	Specify the active interface type for the ACL.	Port-based / VLAN-based	Port-based
Active Ingress Ports	Specify the active ingress ports for the ACL.	Drop-down list of ports	N/A
Active Egress Ports	Specify the active egress ports for the ACL.	Drop-down list of ports	N/A

ACL Rule List (MAC-based)

If the currently displayed ACL table is **MAC-based**, the following table will appear.



UI Setting	Description
Index	Shows the index number for the ACL rule.
ACL Rule	Shows whether the ACL rule is enabled.

UI Setting	Description
Rule Type	Shows the rule type.
EtherType	Shows the EtherType for the ACL rule.
Source	Shows the source MAC address with mask for the ACL rule.
Destination	Shows the destination MAC address with mask for the ACL rule.
VLAN ID	Shows the VLAN ID for the ACL rule.
CoS	Shows the CoS value used to prioritize packets for the ACL rule.
Action	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 (IP-based)

If the currently displayed ACL table is **IP-based**, the following table will appear.



UI Setting	Description
Index	Shows the index number for the ACL rule.
ACL Rule	Shows whether the ACL rule is enabled.
Rule Type	Shows the rule type.
Protocol	Show the protocol used for the ACL rule.
Source	Shows the source IP address with subnet mask for the ACL rule.
Destination	Shows the destination IP address with subnet mask for the ACL rule.
DSCP	Shows the DSCP value used to prioritize packets for the ACL rule.
Optional Parameter	Show the relevant parameters for the selected protocol.

UI Setting	Description
Action	Show whether the redirect action or DSCP remark are enabled. If enabled, their respective configuration settings will be shown.

ACL Rule List - Create Rule

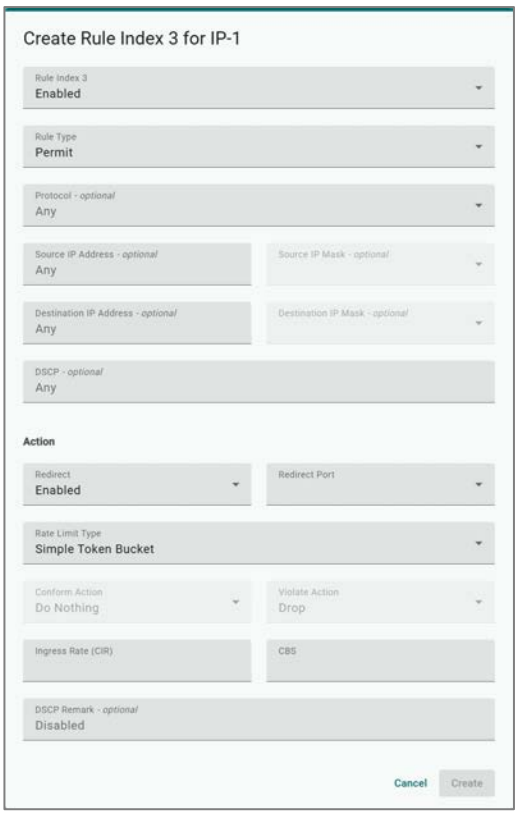
Menu Path: Security > Network Security > Access Control List - Settings

Clicking **Create** for an ACL table 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.

ACL Rule List - Create Rule (IP-based)

If the currently displayed ACL table is **IP-based**, the following table will appear.



UI Setting	Description	Valid Range	Default Value
Rule Index	Enable or disable the rule.	Enabled / Disabled	Enabled
Rule Type	Specify the rule type.	Permit / Deny	N/A
Protocol	Specify the protocol for the ACL rule.	TCP / UDP / ICMP / IGMP / OSPF / User-defined	Any
ICMP Type **(If Protocol is ICMP)**	Specify the ICMP type for the rule. If this is blank, any type will apply.	0 to 255	Any
ICMP Code **(If Protocol is ICMP)**	Specify the ICMP code for the rule. If this is blank, any code will apply.	0 to 15	Any
IGMP Type **(If Protocol is IGMP)**	Specify the IGMP type for the rule. If this is blank, any type will apply.	0 to 255	Any
Protocol Number **(If Protocol is User-defined)**	Specify the protocol number for this rule.	0 to 255	N/A
Source IP Address	Specify the source IP address.	Valid IP address	Any
Source IP Mask	Specify the source IP subnet mask.	Drop-down list of subnet masks	N/A
Destination IP Address	Specify the destination IP address.	Valid IP address	Any
Destination IP Mask	Specify the destination IP subnet mask.	Drop-down list of subnet masks	N/A
DSCP	Specify a DSCP value to prioritize packets for the ACL rule.	0 to 63	Any

Action

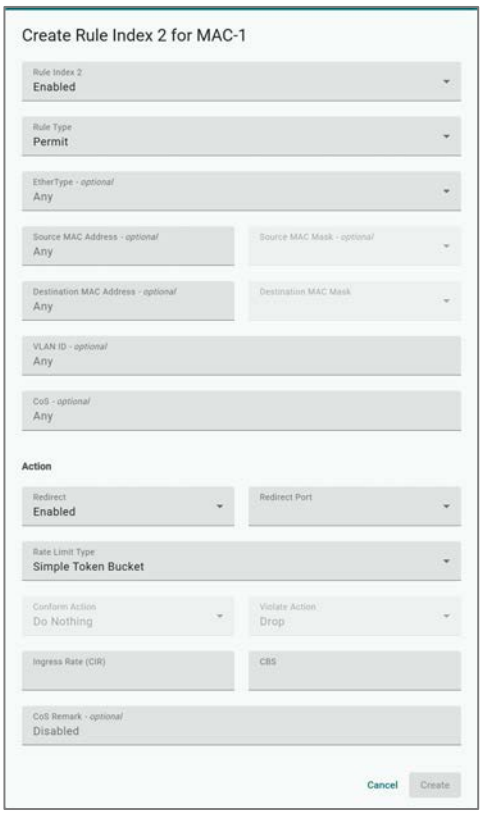
These settings will appear if **Rule Type** is **Permit.**

UI Setting	Description	Valid Range	Default Value
Redirect	Enable or disable redirects.	Enabled / Disabled	Disabled

UI Setting	Description	Valid Range	Default Value
Redirect port **(If Redirect is Enabled)**	Specify the port to redirect packets to.		N/A
Rate Limit Type **(Only in Advanced Mode)**	Specify whether to enable rate limiting. Moxa switches provide Simple Token Bucket as a rate limit algorithm.	None / Simple Token Bucket	None
Conform Action **(Only in Advanced Mode, if Rate Limit Type is Simple Token Bucket)**	Shows the action to take for packets within the allowed average rate (CIR) and burst tolerance (CBS). This is fixed to Do Nothing.	Do Nothing	Do Nothing
Violate Action **(Only in Advanced Mode, if Rate Limit Type is Simple Token Bucket)**	Shows the action to take for packets that exceed the allowed average rate (CIR) and burst tolerance (CBS). This is fixed to Drop.	Drop	Drop
Ingress Rate(CIR) **(Only in Advanced Mode, if Rate Limit Type is Simple Token Bucket)**	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.	1 to 1000	None
CBS **(Only in Advanced Mode, if Rate Limit Type is Simple Token Bucket)**	Specify the CBS (Committed Burst Size) 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.	10 to 10240	None
DSCP Remark	Enable adding a DSCP remark by specifying a DSCP Remark value. To disable it, leave this blank.	0 to 63	Disabled

ACL Rule List - Create Rule (MAC-based)

If the displayed ACL table is **MAC-based**, the following dialog will appear.



UI Setting	Description	Valid Range	Default Value
Rule Index	Enable or disable the rule.	Enabled / Disabled	Enabled
Rule Type	Specify the rule type.	Permit / Deny	N/A
EtherType	Specify the EtherType for the ACL rule.	GOOSE / SMV / User-defined	Any
Source MAC Address	Specify a source MAC address.	Valid MAC address	Any
Source MAC Mask	Select a source MAC mask.	Drop-down list of MAC masks	N/A
Destination MAC Address	Specify a destination MAC address.	Valid MAC address	Any
Destination MAC Mask	Specify a destination MAC mask.	Drop-down list of MAC masks	N/A
VLAN ID	Specify the VLAN ID for the ACL rule.	1 to 4094	Any

UI Setting	Description	Valid Range	Default Value
CoS	Specify a CoS value to prioritize packets for the ACL rule.	0 to 7	Any

Action

These settings will appear if **Rule Type** is **Permit.**

UI Setting	Description	Valid Range	Default Value
Redirect	Enable or disable redirects.	Enabled / Disabled	Disabled
Redirect port **(If Redirect is Enabled)**	Specify the port to redirect packets to.		N/A
Rate Limit Type **(Only in Advanced Mode)**	Specify whether to enable rate limiting. Moxa switches provide Simple Token Bucket as a rate limit algorithm.	None / Simple Token Bucket	None
Conform Action **(Only in Advanced Mode, if Rate Limit Type is Simple Token Bucket)**	Shows the action to take for packets within the allowed average rate (CIR) and burst tolerance (CBS). This is fixed to Do Nothing.	Do Nothing	Do Nothing
Violate Action **(Only in Advanced Mode, if Rate Limit Type is Simple Token Bucket)**	Shows the action to take for packets that exceed the allowed average rate (CIR) and burst tolerance (CBS). This is fixed to Drop.	Drop	Drop
Ingress Rate(CIR) **(Only in Advanced Mode, if Rate Limit Type is Simple Token Bucket)**	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.	1 to 1000	None
CBS **(Only in Advanced Mode, if Rate Limit Type is Simple Token Bucket)**	Specify the CBS (Committed Burst Size) 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.	10 to 10240	None
DSCP Remark	Enable adding a DSCP remark by specifying a DSCP Remark value. To disable it, leave this blank.	0 to 63	Disabled

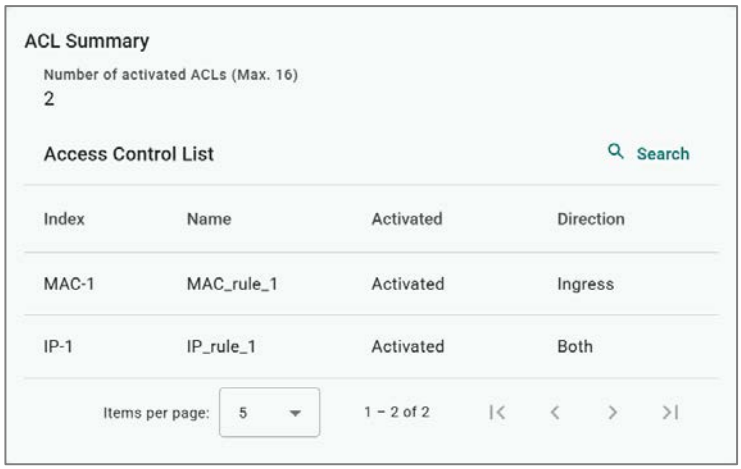
Access Control List - Status

Menu Path: Security > Network Security > Access Control List - Status

This page lets you view ACL status information for your device.

ACL Summary

When **View by ACL** is selected from the drop-down list, this information will appear.



UI Setting	Description
Number of activated ACLs (Max. 16)	Shows the number of activated ACLs.
Index	Shows the ACL type and its index value.
Name	Shows the name of the ACL.
Activated	Shows whether the ACL is enabled.
Direction	Shows the direction of the ACL.

ACL Rule Status (by ACL, IP-based)

When **View by ACL** is selected from the drop-down list and the selected ACL is **IP-based**, the following table will appear.

You can view ACL rules for a different ACL by clicking on the ACL's name.

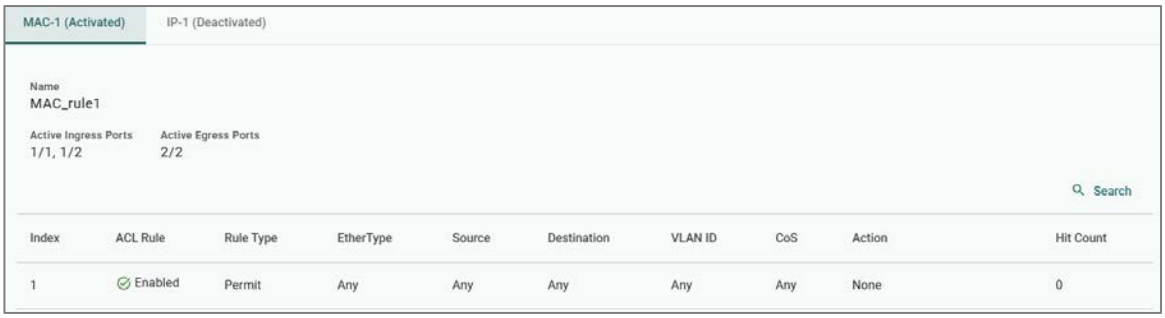


UI Setting	Description
Name	Shows the name of the access list.
Active Ingress Portss	Shows the active ingress ports configured for the ACL.
Active Egress Port	Shows the active egress ports configured for the ACL.
Index	Shows the index of the ACL rule.
ACL Rule	Shows whether the ACL rule is enabled.
Rule Type	Shows the rule type.
Protocol	Shows the protocol used for the ACL rule.
Source	Shows the source IP address with its subnet mask.
Destination	Shows the destination IP address with its subnet mask.
DSCP	Shows the DSCP value specified to differentiate the prioritization of IP packets.
Optional Parameter	Shows the relevant parameters for the selected protocol.
Action	Shows the redirect actions to take for this rule.
Hit Count	Shows the hit count of the ACL rule.

ACL Rule Status (by ACL, MAC-based)

When **View by ACL** is selected from the drop-down list and the selected ACL is **MAC-based**, the following table will appear.

You can view ACL rules for a different ACL by clicking on the ACL's name.

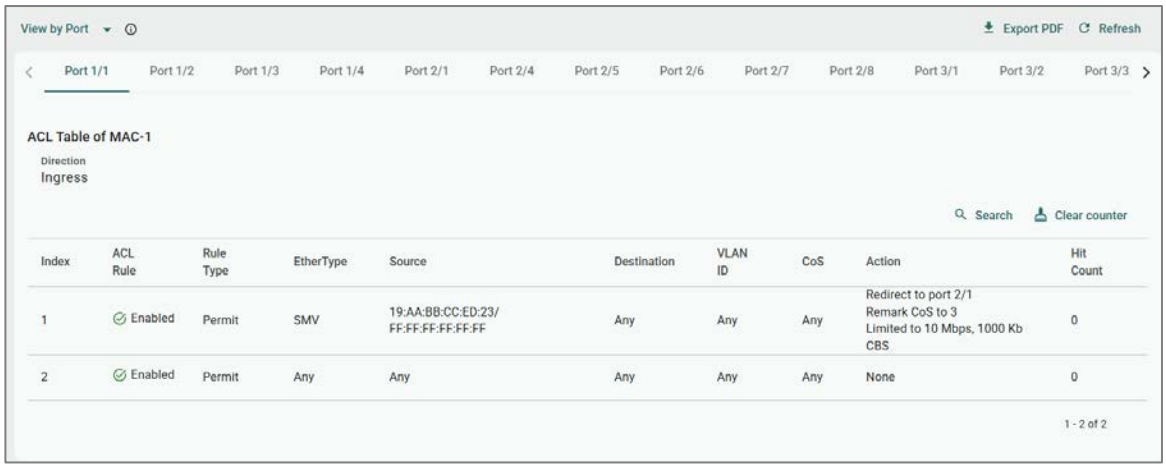


UI Setting	Description
Name	Shows the name of the access list.
Active Ingress Ports	Shows the active ingress ports configured for the ACL.
Active Egress Ports	Shows the active egress ports configured for the ACL.
Index	Shows the index of the ACL rule.
ACL Rule	Shows whether the ACL rule is enabled.
Rule Type	Shows the rule type.
EtherType	Shows the EtherType used for the ACL rule.
Source	Shows the source MAC address with its mask.
Destination	Shows the destination MAC address with its mask.
VLAN ID	Shows the VLAN ID.
CoS	Shows the CoS value specified to differentiate the prioritization of packets.
Action	Shows the redirect actions to take for this rule.
Hit Count	Shows the hit count of the ACL rule.

ACL Rule Status (by Port)

When **View by Port** is selected from the drop-down list, the following information will appear.

You can view ACL rules for a specific port by clicking on the port's name.



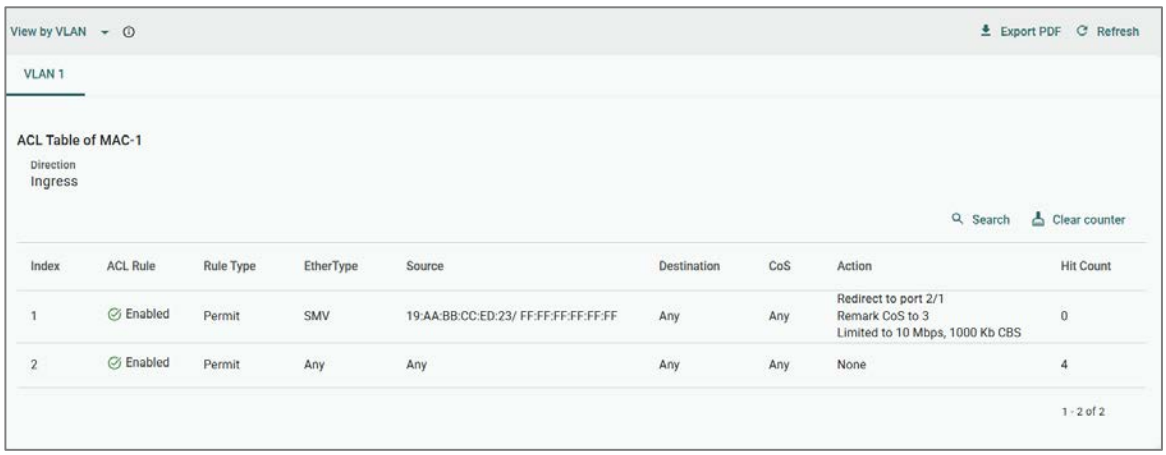
UI Setting	Description
Direction	Shows the direction of the relevant ACL for this port.
Index	Shows the index of the ACL rule.
ACL Rule	Shows whether the ACL rule is enabled.
Rule Type	Shows the rule type.
EtherType **(If relevant ACL is MAC-based)**	Shows the EtherType used for the ACL rule.
Protocol **(If relevant ACL is IP-based)**	Shows the Protocol used for the ACL rule.
Source	Shows the source IP or MAC address with its mask.
Destination	Shows the destination IP or MAC address with its mask.

UI Setting	Description
VLAN ID **(If relevant ACL is MAC-based)**	Shows the VLAN ID.
CoS **(If relevant ACL is MAC-based)**	Shows the CoS value specified to differentiate the prioritization of packets.
DSCP **(If relevant ACL is IP-based)**	Shows the DSCP value specified to differentiate the prioritization of packets.
Optional Parameter **(If relevant ACL is IP-based)**	Shows the relevant parameters for the selected EtherType/Protocol.
Action	Shows the actions to take for the ACL rule.
Hit Count	Shows the hit count of the ACL rule.

ACL Rule Status (by VLAN)

When **View by VLAN** is selected from the drop-down list, the following information will appear.

You can view ACL rules for a specific VLAN by clicking on the VLAN's name.



UI Setting	Description
Direction	Shows the direction of the relevant ACL for this VLAN.
Index	Shows the index of the ACL rule.
ACL Rule	Shows whether the ACL rule is enabled.
Rule Type	Shows the rule type.
EtherType **(If relevant ACL is MAC-based)**	Shows the EtherType used for the ACL rule.
Protocol **(If relevant ACL is IP-based)**	Shows the Protocol used for the ACL rule.
Source	Shows the source IP or MAC address with its mask.
Destination	Shows the destination IP or MAC address with its mask.
VLAN ID **(If relevant ACL is MAC-based)**	Shows the VLAN ID.
CoS **(If relevant ACL is MAC-based)**	Shows the CoS value specified to differentiate the prioritization of packets.
DSCP **(If relevant ACL is IP-based)**	Shows the DSCP value specified to differentiate the prioritization of packets.
Optional Parameter **(If relevant ACL is IP-based)**	Shows the relevant parameters for the selected EtherType/Protocol.
Action	Shows the actions to take for the ACL rule.
Hit Count	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

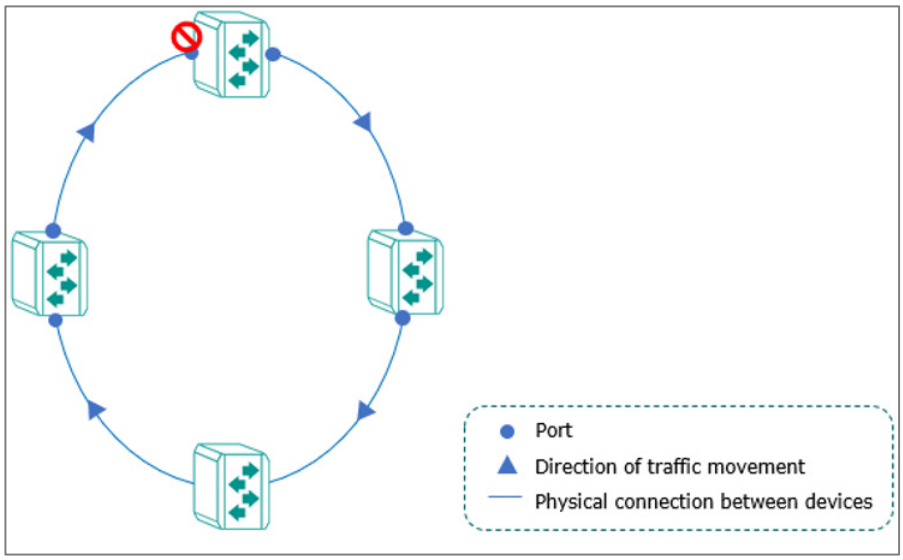
redundant protocols, when redundant protocols are not configured, or if the redundant protocol fails.

> **Note**
>
> This feature supports weaker authentication or encryption, and may not be secure over untrusted networks. Take appropriate security precautions.

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:

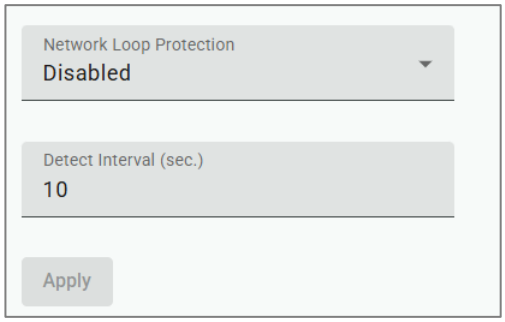
- Settings
- Status

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



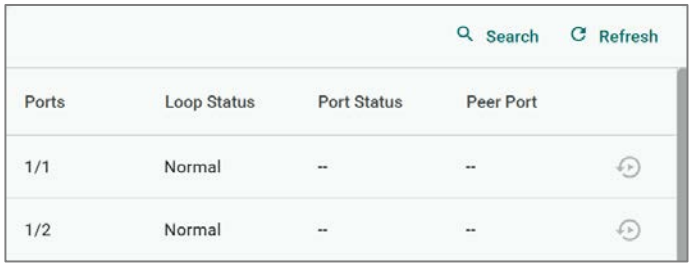
UI Setting	Description	Valid Range	Default Value
Network Loop Protection	Enable or disable the network loop protection.	Enabled / Disabled	Disabled
Detect Interval	Specify the detect interval in seconds.	1 to 30	10

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



UI Setting	Description
Ports	Shows the port number the entry is for.
Loop Status	Shows the loop status of the port. • **Normal**: The port is not looping. • **Looping**: The port is looping.
Port Status	Shows the port status of the port. • **Disabled**: The port is disabled due to a port shutdown or detected loop.
Peer Port	Shows the port where the looping frames are from when detecting a loop.

About Binding Databases

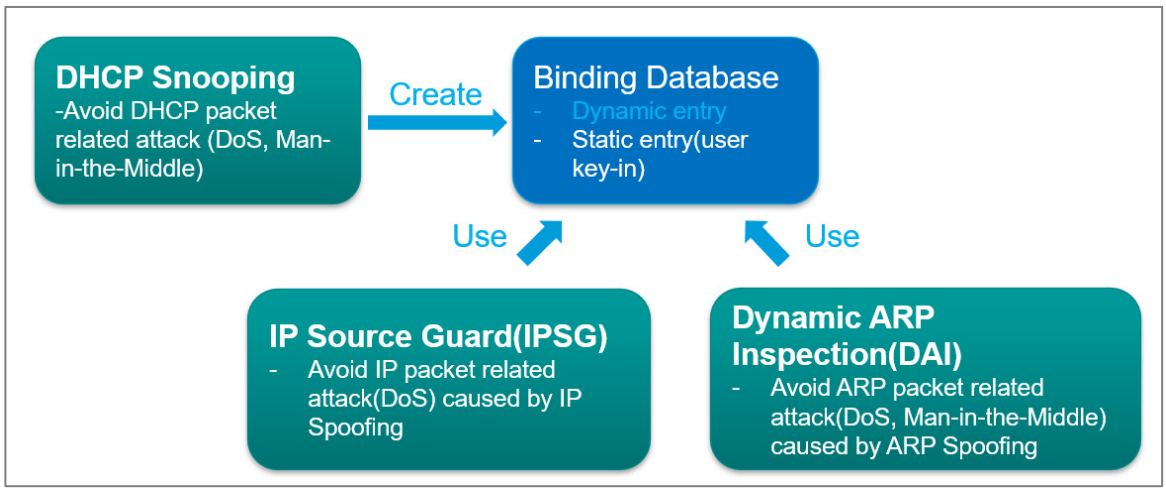
A binding database acts as an allowlist for IP Source Guard and Dynamic ARP Inspection to help protect against unauthorized traffic.

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 256 binding database entries, including dynamic and static entries. Entries will stop being generated or being user-addable when the this limit is reached. More entries can only be added when existing entries are released, bringing the total number below 256.

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 Database Static Entry List

This list shows the user-configured static entries for the binding database. These entries can be used as an allowlist base for IP Source Guard and Dynamic IP Inspection.



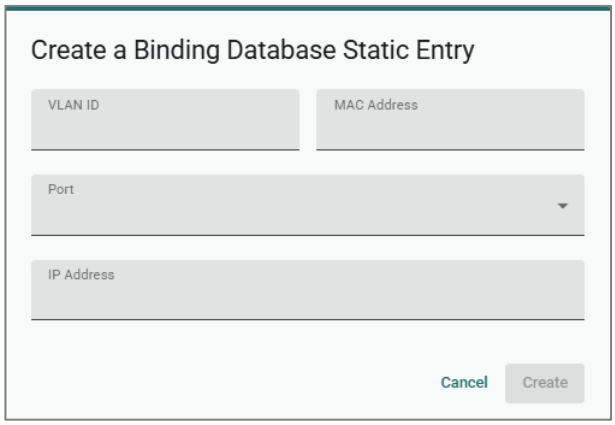
UI Setting	Description
VLAN ID	Shows the VLAN ID for the static entry.
MAC Address	Shows the MAC address for the static entry.
Port	Shows the port for the static entry.
IP Address	Shows the IP address for the static entry.

Create a Binding Database Static Entry

Menu Path: Security > Network Security > Binding Database - Binding Settings

Clicking **Create** on the **Security > Network Security > Binding Database - Binding Settings** page will open this dialog box. This dialog lets you add 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.



UI Setting	Description	Valid Range	Default Value
VLAN ID	Specify the VLAN ID to allowlist for the static entry.	1 to 4094	N/A
MAC Address	Specify the MAC address to allowlist for the static entry.	Valid MAC address	N/A
Port	Specify the port to allowlist for the static entry.	Drop-down list of ports	N/A
IP Address	Specify the IP address to allowlist for the static entry.	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



UI Setting	Description
Type	Shows the type of the entry. • **DHCP**: This is a dynamically learned entry. • **Static**: This is a user-configured entry.
VLAN ID	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.
MAC Address	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.
Port	Shows the untrusted port for a successful DHCP packet transaction, or the specified port for a user-created static entry.
IP Address	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.
Lease Time	Shows the lease time for the entry to be active. The lease time is infinite for user-created static entries.
Active	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

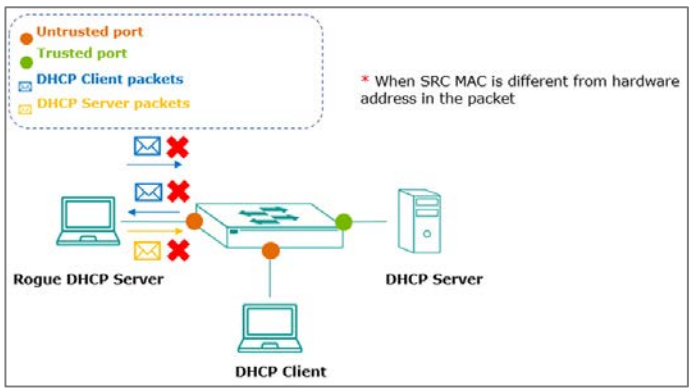
device, and then the feature will act like a firewall to validate DHCP messages received from untrusted sources and filter out invalid messages to exclude rogue DHCP servers and remove malicious DHCP traffic. This helps guarantee that clients obtain a legal address from the DHCP server you designate.

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.

Configuring DHCP Snooping on the Device

Enable DHCP Snooping on the device to set up DHCP packet filtering to avoid DHCP-related attacks and create allowlist entries in the Binding Database from successful DHCP transactions through untrusted ports. These allowlist entries can then be used for IP Source Guard and Dynamic ARP Inspection.

To configure DHCP Snooping on the device:

1. In **Security > Network Security > DHCP Snooping**, enable DHCP Snooping globally for a specific VLAN.
2. In **Security > Network Security > DHCP Snooping**, select the **Edit (✎)** icon for individual ports to configure them as Trusted or Untrusted.Typically, configure ports connected to an untrusted source—such as hosts—as Untrusted ports. Ports connected to a trusted source—such as a DHCP server—can be configured as Trusted.
3. When finished, click **APPLY** to save your changes.

> ✎ **Note**
>
> The port status cannot be changed to Trusted if Dynamic ARP Inspection or IP Source Guard is activated for the port.

Results:

Trusted Ports	Untrusted Ports
Pass all DHCP packets	1. Pass ingress DHCP client packets and egress DHCP server packets to complete normal DHCP transactions. 2. Drop egress DHCP client packets and ingress DHCP server packets to avoid the rogue DHCP server attacks. 3. Drop DHCP client type packets with a different source MAC address and hardware address to avoid malicious DHCP client attacks.

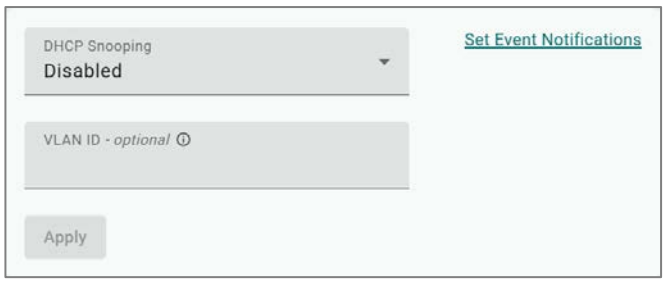
Enabling DHCP Snooping will also set up Binding Database entries, which will act as an allowlist for IP Source Guard and Dynamic ARP Inspection.

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
DHCP Snooping	Enable or disable DHCP snooping.	Enabled / Disabled	Disabled
VLAN ID	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



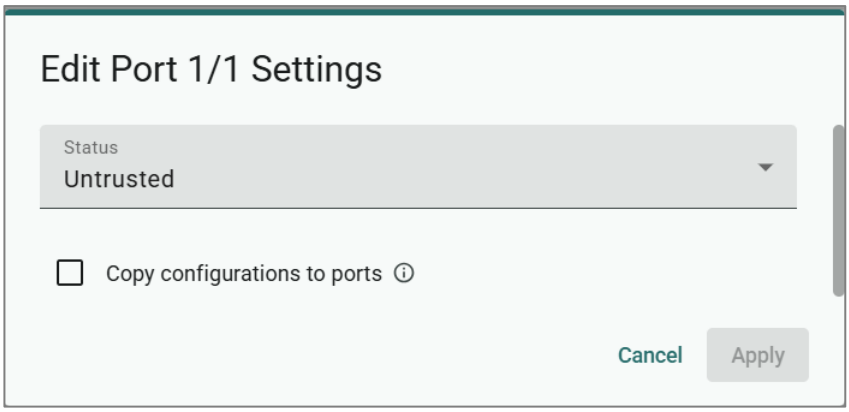
UI Setting	Description
Port	Shows the port number the entry is for.
Status	Shows whether the port is trusted or untrusted.

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.



UI Setting	Description	Valid Range	Default Value
Status	Specify the port as untrusted or trusted.	Untrusted / Trusted	Untrusted
Copy configurations to ports	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.

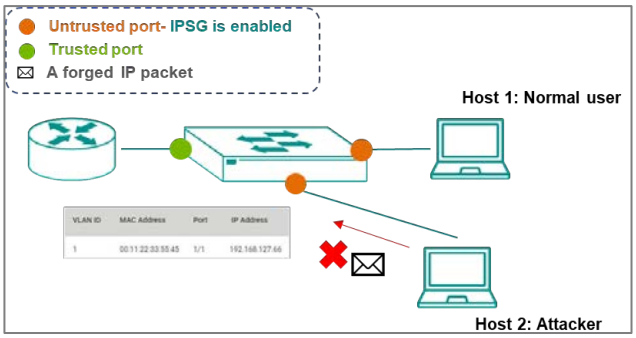
IP Source Guard In Depth

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.

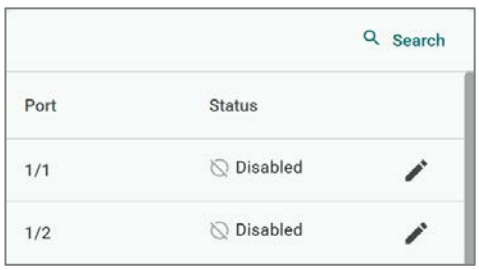


IP Source Guard

Menu Path: Security > Network Security > IP Source Guard

This page lets you enable or disable IP Source Guard for each port.

IP Source Guard Port List



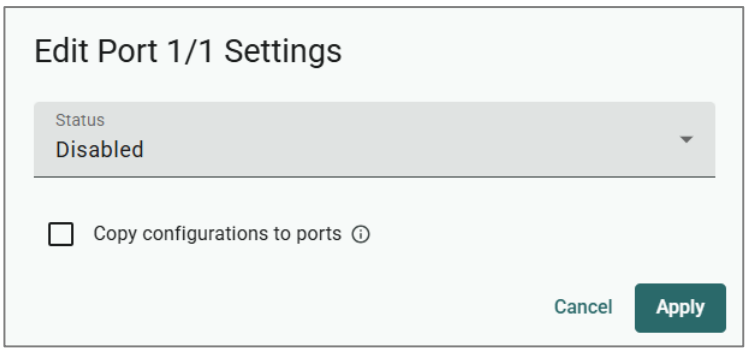
UI Setting	Description
Port	Shows the port number the entry is for.
Status	Shows whether IP Source Guard is enabled for the port.

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.



UI Setting	Description	Valid Range	Default Value
Status	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. **✎ Note** IP Source Guard can only be enabled on ports specified as untrusted in DHCP snooping.	Enabled / Disabled	Disabled
Copy configurations to ports	Select the ports you want to copy this configuration to.	Drop-down list of ports	N/A

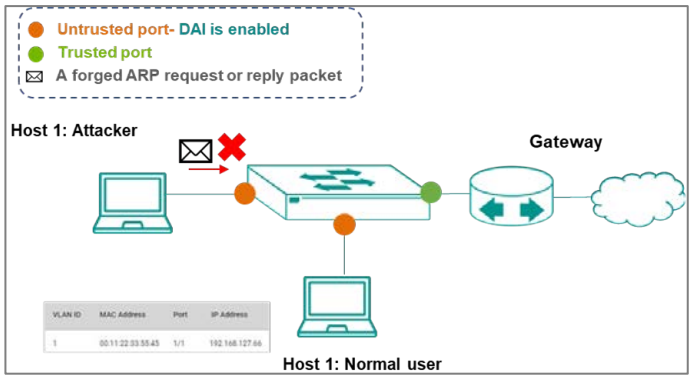
About Dynamic ARP Inspection

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.

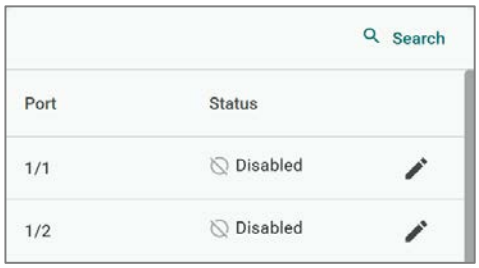


Dynamic ARP Inspection

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



UI Setting	Description
Port	Shows the port number the entry is for.

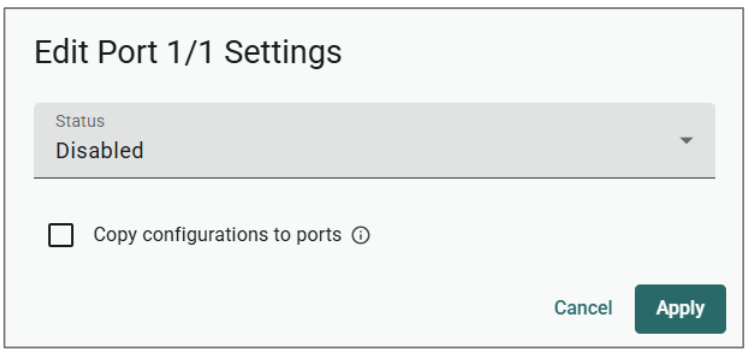
UI Setting	Description
Status	Shows whether Dynamic ARP Inspection is enabled for the port. **Note** Dynamic ARP Inspection can only be enabled on ports specified as untrusted in DHCP snooping.

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.



UI Setting	Description	Valid Range	Default Value
Status	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. **Note** Dynamic ARP Inspection can only be enabled on ports specified as untrusted in DHCP snooping.	Enabled / Disabled	Disabled
Copy configurations to ports	Select the ports you want to copy this configuration to.	Drop-down list of ports	N/A

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

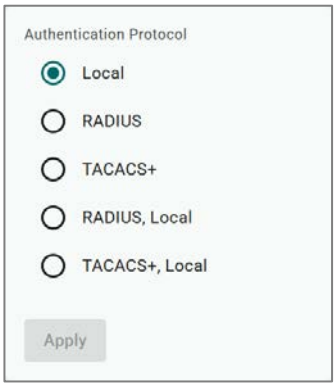
The account privilege level will be granted based on the service type setting for the user for RADIUS authentication, and the privilege level for the user for TACACS+ authentication.

RADIUS Service Type

- 6: Administrator
- 3: Supervisor
- All other values (1, 2, 4, 5, 7, 8, 9, 10, 11): User

TACACS+ Privilege Level

- 15: Administrator
- 12: Supervisor
- 1: User



UI Setting	Description	Valid Range	Default Value
Authentication Protocol	Select the login authentication protocol to use for your device. • **Local:** Only the local database will be checked for login authentication. • **RADIUS:** Only the RADIUS database will be checked for login authentication. • **TACACS+**: Only the TACACS+ database will be checked for login authentication. • **RADIUS, Local**: The RADIUS database will be checked first for login authentication. If checking the RADIUS database fails, then the local database will be checked. • **TACACS+, Local**: The TACACS+ database will be checked first for login authentication. If checking the TACACS+ database fails, then the local database will be checked.	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.

Note

This feature supports weaker authentication or encryption, and may not be secure over untrusted networks. Take appropriate security precautions.

RADIUS

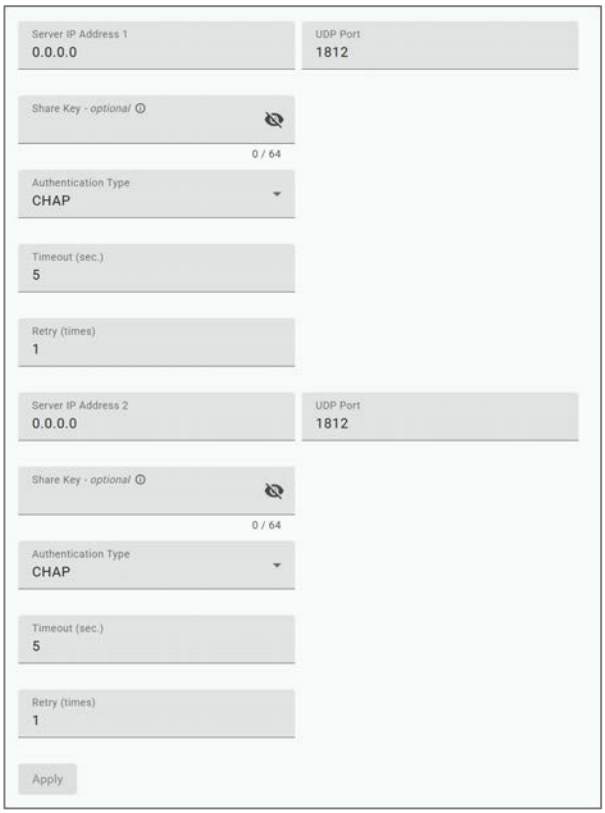
Menu Path: Security > Authentication > RADIUS

This page lets you configure the RADIUS settings for your device.

RADIUS Server Settings

Note

After leaving this page or refreshing, the Share Key fields will automatically be cleared to enhance security.



UI Setting	Description	Valid Range	Default Value
Server Address 1 / 2	Specify the address of the first/second RADIUS server.	Valid IP address	0.0.0.0
UDP Port	Specify the UDP port for the RADIUS server.	1 to 65535	1812
Share Key	Specify the share key for server authentication verification.	0 to 64 characters	N/A
Authentication Type	Select the authentication type to use for the RADIUS server.	PAP / CHAP / MS-CHAPv1 / MS-CHAPv2	CHAP

UI Setting	Description	Valid Range	Default Value
Timeout (sec.)	Specify how long in seconds to wait for a response from the RADIUS server before timing out.	5 to 180	5
Retry (sec.)	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.

> **Note**
>
> This feature supports weaker authentication or encryption, and may not be secure over untrusted networks. Take appropriate security precautions.

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.

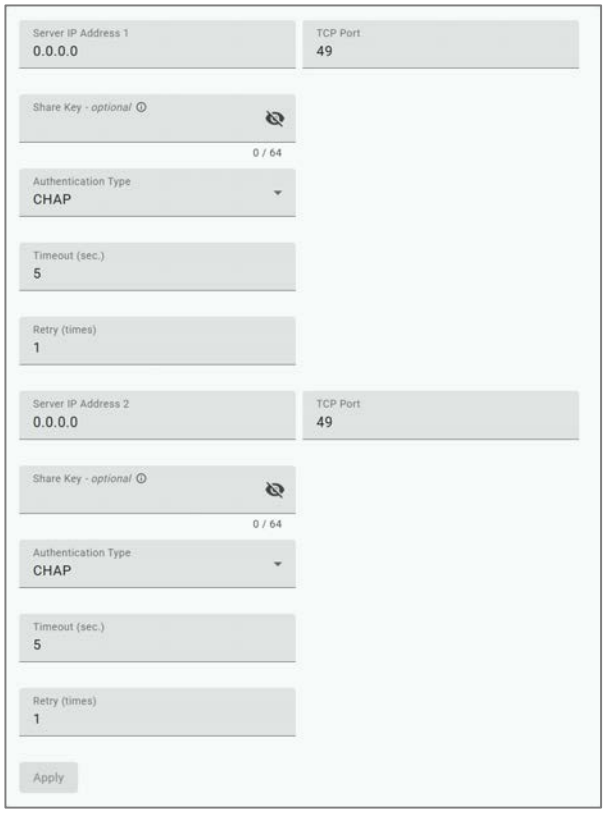
Note

Users created with the TACACS+ server will be granted Admin privileges.

TACACS+ Server Settings

Note

After leaving this page or refreshing, the Share Key fields will automatically be cleared to enhance security.



UI Setting	Description	Valid Range	Default Value
Server Address 1 / 2	Specify the address of the first/second TACACS+ server.	Valid IP address	0.0.0.0
TCP Port	Specify the TCP port for the TACACS+ server.	1 to 65535	49

UI Setting	Description	Valid Range	Default Value
Share Key	Specify the share key for server authentication verification.	0 to 64 characters	N/A
Authentication Type	Select the authentication type to use for the TACACS+ server.	ASCII / PAP / CHAP	CHAP
Timeout (sec.)	Specify how long in seconds to wait for a response from the TACACS+ server before timing out.	5 to 180	5
Retry	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 User Accounts for more information on user accounts.

Settings	Admin	Supervisor	User
System Status			
Resource Utilization	R	R	R
Fiber Check	R/W	R/W	R
Module Information	R	R	R
Network Status			
Network Statistics	R	R	R
LLDP	R/W	R/W	R
ARP Table	R	R	R
Tools			
Port and VLAN Mirroring	R/W	R/W	R

Settings	Admin	Supervisor	User
Ping	R/W	R/W	R/W
Event Logs and Notifications			
Event Logs	R/W	R/W	R
Event Notifications	R/W	R/W	R
Syslog	R/W	R/W	-
SNMP Trap / Inform	R/W	-	-
Email Settings	R/W	R	R
Relay Alarm	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 current usage and usage over time for:

- **CPU Utilization**
- **Memory Utilization**
- **Power Utilization**

Note

Power utilization monitoring is only supported for MDS devices.

Resource Utilization

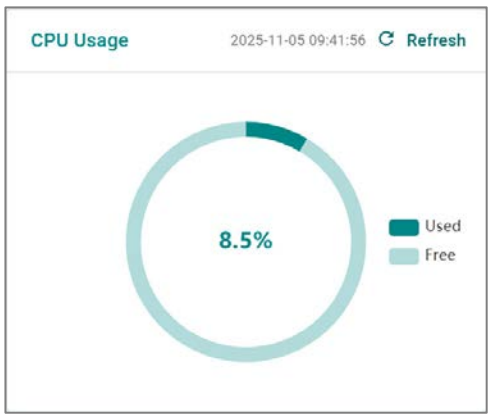
Menu Path: Diagnostics > System Status > Resource Utilization

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.



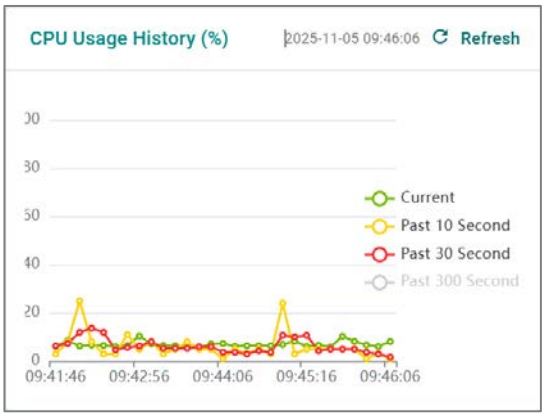
UI Setting	Description
CPU Usage	Displays the current utilization of the CPU.

CPU Usage History (%)

The device's CPU usage will be shown as a percentage based on a time interval. For example, a point on the **Past 10 Second** line shows the average CPU usage for the past 10 seconds at that time.

Click the **Refresh (↻)** icon to manually add the current value to the chart.

Click the names on the right side to toggle display of that data.

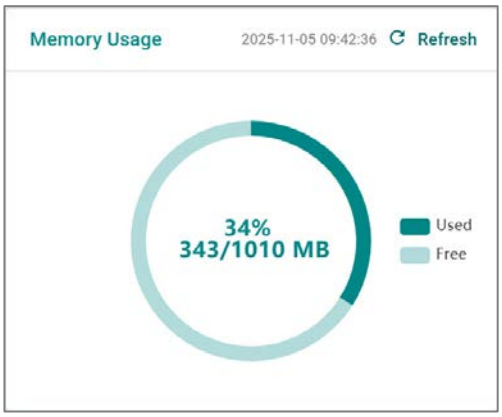


UI Setting	Description
CPU Usage History (%)	Displays the device's CPU usage over time.

Memory Usage

This display shows the device's memory usage.

Click the **Refresh (↻)** icon to refresh the graph.

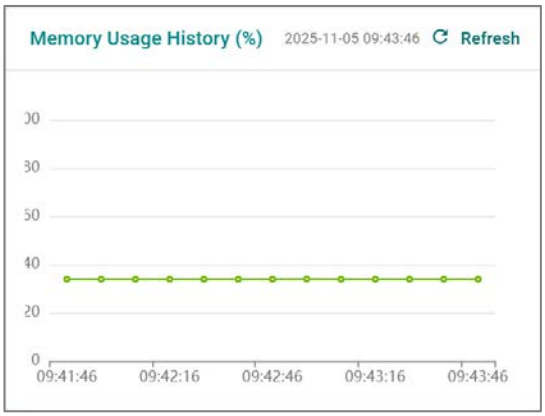


UI Setting	Description
Memory Usage	Displays the memory utilization status.

Memory Usage History

The device's memory usage will be shown as a percentage over time.

Click the **Refresh (↻)** icon to manually add the current value to the chart.



UI Setting	Description
Memory Usage History (%)	Displays the device's memory usage over time.

Power Consumption

This display shows the device's current power consumption in watts.

Click the **Refresh (↻)** icon to refresh the value.

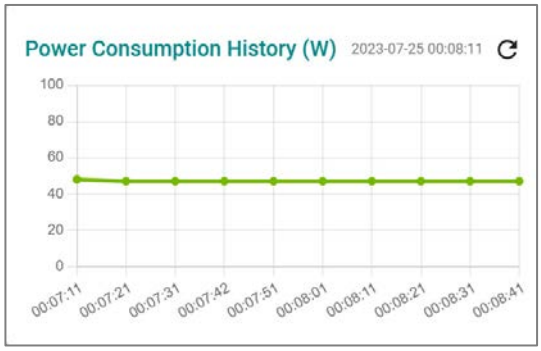


UI Setting	Description
Power Consumption	Displays the current power consumption of the device in watts.

Power Consumption History

This shows the device's power consumption over time.

Click the **Refresh (↻)** icon to manually add the current value to the chart.



UI Setting	Description
Power History	Displays the device's power consumption in watts over time.

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.

Configuring Fiber Check Thresholds

Configure events to trigger when fiber modules reach temperature and power thresholds.

This feature:

- Requires Moxa SFP modules installed
- Only supports Moxa SFP and fixed type (multi-mode SC/ST and single-mode SC) modules.

1. Sign in to the device with administrator credentials.
2. Go to **Diagnostics** > **System Status** > **Fiber Check**, and then select **Threshold Settings**.
3. Select **[Edit]** corresponding to the port to edit.

   Edit Port Settings appears.
4. Configure all of the following:

Option	Value
Mode	• **Auto**: Sets threshold values automatically. • **User-defined**: Configure threshold values manually.
Temperature Threshold	For **Mode User-defined**: Configure a maximum temperature to trigger and event.
Temperature Threshold	For **Mode User-defined**: Choose the unit for the temperature threshold: • **°C** • **°F**

Option	Value
Tx Power Threshold Low (dBm)	For **Mode User-defined**: Specify a minimum threshold for transmit power, below which an event triggers.
Tx Power Threshold High (dBm)	For **Mode User-defined**: Specify a maximum threshold for transmit power, above which an event triggers.
Rx Power Threshold Low (dBm)	For **Mode User-defined**: Specify a minimum threshold for received power, below which an event triggers.
Rx Power Threshold High (dBm)	For **Mode User-defined**: Specify a maximum threshold for received power, above which an event triggers.
Copy configuration to ports	Duplicate and apply this configuration to other ports.

5. Select **Apply** to save your changes.

Fiber Check warning events will trigger. You can now configure notifications based on these events.

To configure notifications for **Fiber Check warning** events events, go to **Event Logs and Notification** > **Event Notifications** > **Event Logs** > **Port**, find **Fiber Check warning**, and select **[Edit]**. You can then configure notifications.

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

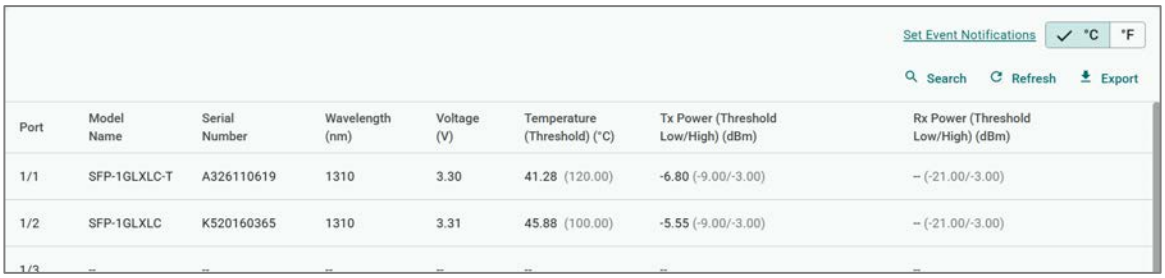
- Threshold Settings

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



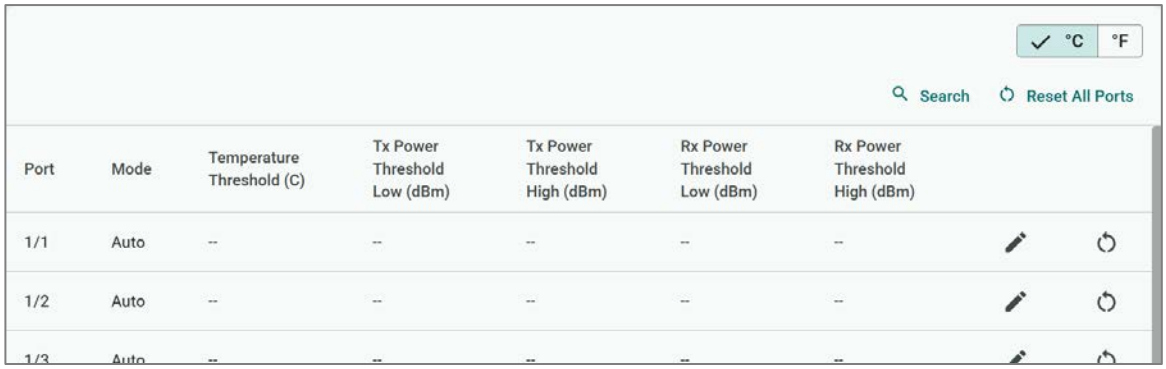
UI Setting	Description
Port	Shows the port the entry is for.
Model Name	Shows the model name of the port.
Serial Number	Shows the serial number of the port.
Wavelength	Shows the wavelength in nm of the port.
Voltage	Shows the voltage in V of the port.
Temperature Threshold	Shows the current temperature 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.
Tx Power (Threshold Low/High) (dBm)	Shows the current Tx power in dBm of the port, and the low and high thresholds for Tx power in parentheses ( ).
Rx Power (Threshold Low/High) (dBm)	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



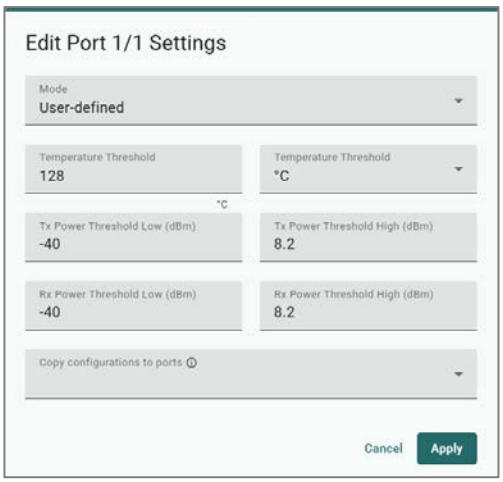
UI Setting	Description
Port	Shows the port the entry is for.
Mode	Shows whether the port is using Auto or User Defined threshold settings.
Temperature Threshold	Shows the temperature threshold for the port. An event will be triggered if the temperature goes above this threshold. You can change between °C and °F temperatures by using the buttons at the top of the table.
Tx Power Threshold Low (dBm)	Shows the low threshold for Tx power in dBm. An event will be triggered if Tx power goes below this threshold.
Tx Power Threshold High (dBm)	Shows the high threshold for Tx power in dBm. An event will be triggered if Tx power goes above this threshold.
Rx Power Threshold Low (dBm)	Shows the low threshold for Rx power in dBm. An event will be triggered if Rx power goes below this threshold.
Rx Power Threshold High (dBm)	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.



UI Setting	Description	Valid Range	Default Value
Mode	Specify how fiber check threshold values should be set. • **Auto:** Threshold values will be automatically specified. Refer to Fiber Check Threshold Values for Auto Mode for more information. • **User Defined**: Threshold values are manually specified.	Auto / User Defined	Auto
Temperature Threshold	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 drop-down menu to the right.	In °C: -128 to 128 In °F: -198.4 to 262.4	In °C: 128 In °F: 262.4
Tx Power Threshold Low (dBm)	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
Tx Power Threshold High (dBm)	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

UI Setting	Description	Valid Range	Default Value
Rx Power Threshold Low (dBm)	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
Rx Power Threshold High (dBm)	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
Copy configurations to ports	Select the ports you want to copy this configuration to.	Drop-down list of ports	N/A

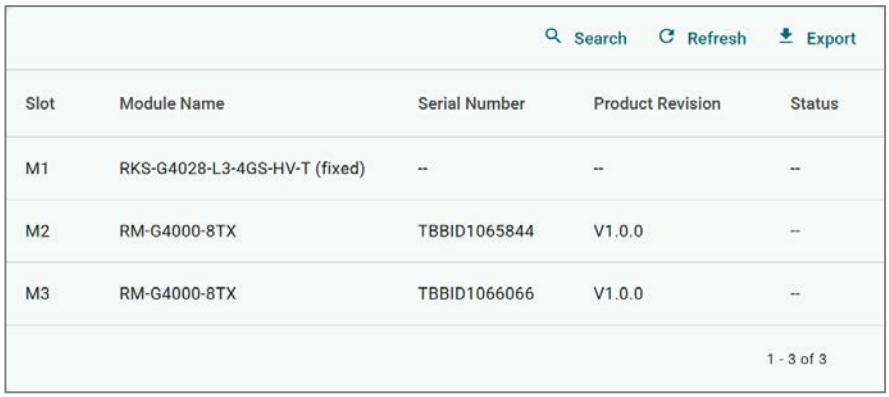
Module Information

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



UI Setting	Description
Slot	Shows the slot the module is installed in.
Module Name	Shows the name of the module this entry is for.

UI Setting	Description
Serial Number	Shows the serial number of the module.
Product Revision	Shows the product revision of the module.
Status	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.

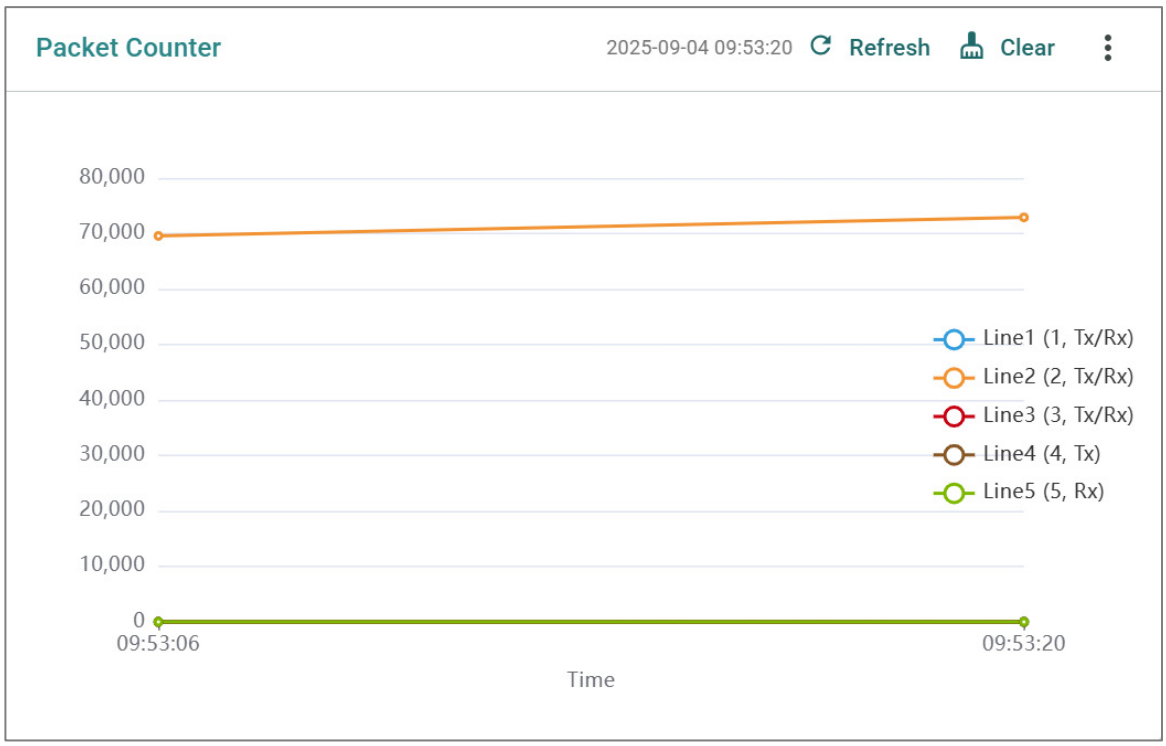
Network Status Display

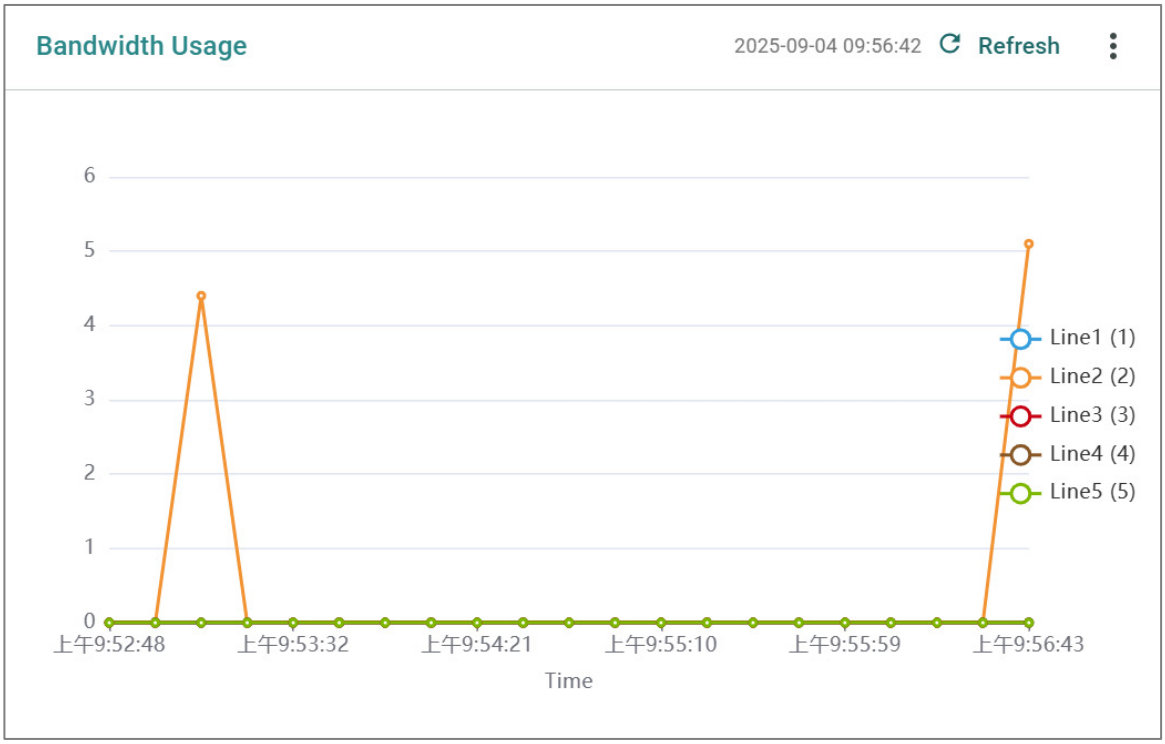
Click the **Options (⋮)** icon and select **Display Settings** to switch between **Packet Counter** and **Bandwidth Utilization** views and configure them.

- **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.

Click the **Refresh (↻)** icon to refresh the graph.

Click the **Clear (🧹)** icon to clear all graph data.

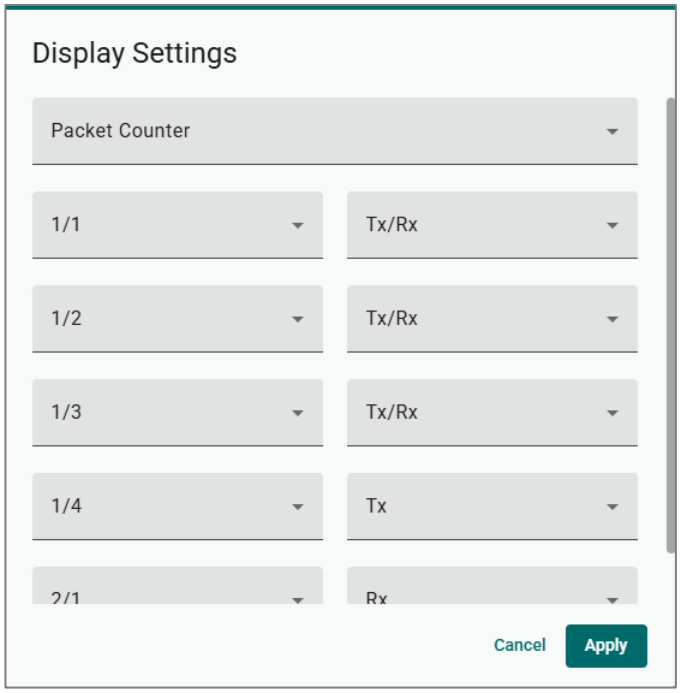


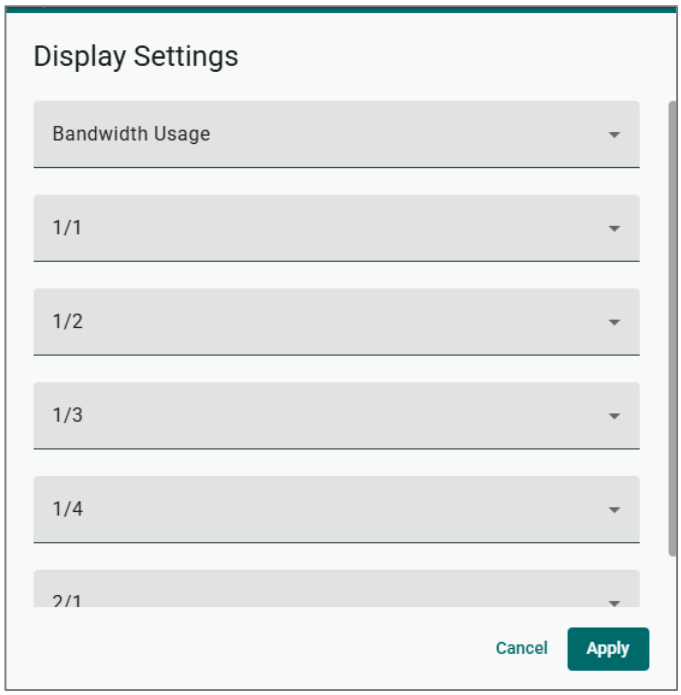


UI Setting	Description
Refresh ( )	Updates statistics immediately without waiting for the refresh interval.
Clear **(For Packet Counter display only)**	Clears the display and resets display settings back to defaults.
Options ( )	Opens a drop-down menu with additional options. • **Display Settings**: Opens **Display Settings**, which allows you to switch between **Packet Counter** and **Bandwidth Usage** view, and add lines based on user-defined criteria. • **Compare Data**: Compare data by selecting a benchmark line and time and a comparison line and time. This is only available for the **Packet Counter** view.

Display Settings

If you click the **Options ( )** icon on the **Diagnostics > System Status > Resource Utilization** page and select **Display Settings**, this dialog will appear.


Display Settings
Packet Counter
1/1
Tx/Rx
1/2
Tx/Rx
1/3
Tx/Rx
1/4
Tx
2/1
Rx
Cancel
Apply


Display Settings
Bandwidth Usage
1/1
1/2
1/3
1/4
2/1
Cancel
Apply

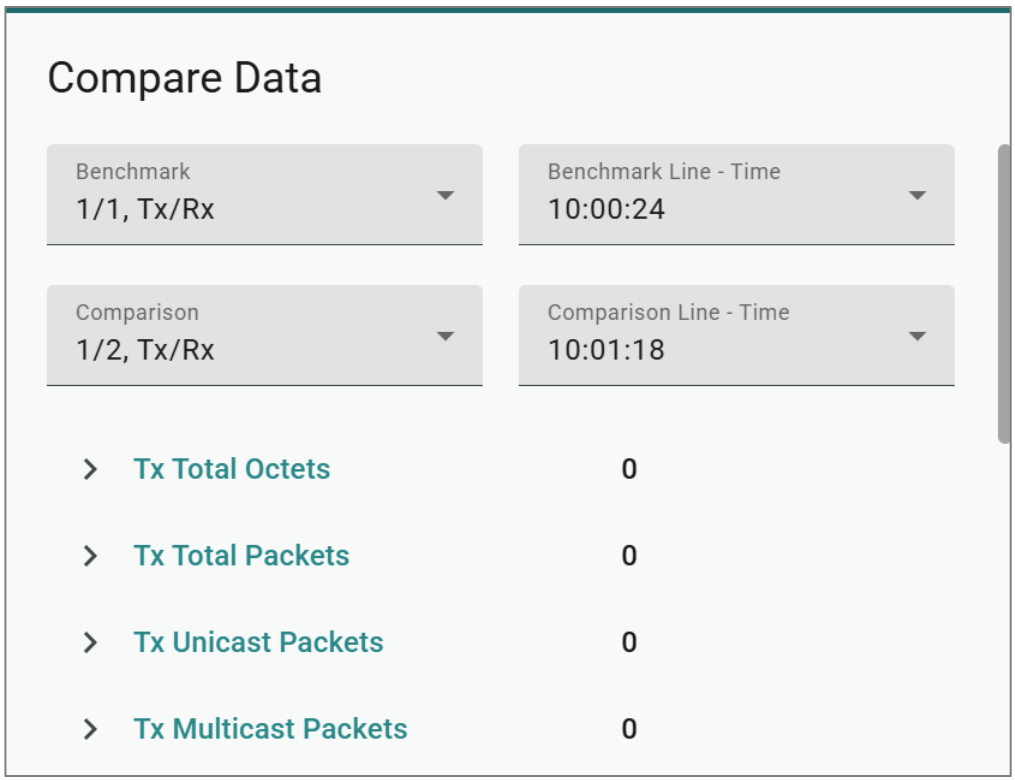
UI Setting	Description	Valid Range	Default Value
Display Mode	Select whether to show the **Packet Counter** or the **Bandwidth Usage** display.	Packet Counter / Bandwidth Usage	Packet Counter
Line 1-5 Sniffer **(If Display Mode is Packet Counter)**	Select which type of traffic to monitor for the line. • **Tx/Rx**: Monitor both transmit and receive traffic. • **Tx**: Only monitor transmit traffic. • **Rx**: Only monitor receive traffic.	Tx/Rx / Tx / Rx	Line 1: Tx/Rx Line 2: Tx/Rx Line 3: Tx/Rx Line 4: Tx Line 5: Rx
Line 1-5 Monitoring Port **(If Display Mode is Bandwidth Usage)**	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

Compare Data Settings

If you click the **Options (⋮)** icon on the **Diagnostics > System Status > Resource Utilization** page for the **Packet Counter** display and select **Compare Data**, 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.



UI Setting	Description	Valid Range	Default Value
Benchmark	Specify which line to use as the benchmark.	Drop-down list of monitored port and sniffer combinations	N/A
Benchmark Line - Time	Select a timestamp to determine which benchmark data to use.	Drop-down list of timestamps	N/A
Comparison	Specify which line to use as the comparison.	Drop-down list of monitored port and sniffer combinations	N/A
Comparison Line - Time	Select a timestamp to determine which comparison data to use.	Drop-down list of timestamps	N/A

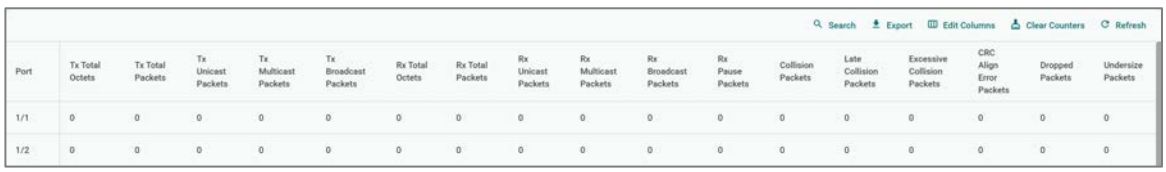
Network Statistics Table

This table shows various packet statistics for each port.

The table shows the total number of octets and packets since the last boot for the following items:

- Tx Total Octets
- Tx Total Packets

- Tx Unicast Packets
- Tx Multicast Packets
- Tx Broadcast Packets
- Rx Total Octets
- Rx Total Packets
- Rx Unicast Packets
- Rx Multicast Packets
- Rx Broadcast Packets
- Rx Pause Packets
- Collision Packets
- Late Collision Packets
- Excessive Collision Packets
- CRC Align Error Packets
- Dropped Packets
- Undersize Packets

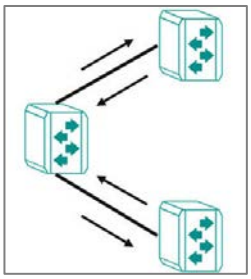


About LLDP

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.



Note

This feature supports weaker authentication or encryption, and may not be secure over untrusted networks. Take appropriate security precautions.

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.

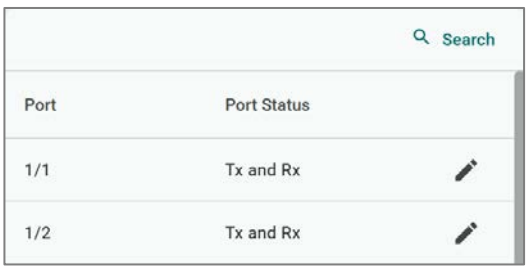
LLDP - Settings



UI Setting	Description	Valid Range	Default Value
LLDP	Enable or disable Link Layer Discovery Protocol (LLDP).	Enabled / Disabled	Enabled
LLDP Version	Shows the LLDP version.	v1(2005)	v1(2005)
Transmit Interval (sec.)	Specify how long in seconds the interval will be in between sending LLDP messages.	5 to 32768	30
Notification Interval (sec.)	Specify how long in seconds the interval will be in between sending notifications.	5 to 3600	5
Tx Delay (sec.)	Specify how long in seconds the interval will be in between successive LLDP frame transmissions initiated by changes.	1 to 8192	2
Reinitialization Delay (sec.)	Specify how long in seconds the delay will be before reinitializing an LLDP packet transmission.	1 to 10	2
Holdtime Multiplier (sec.)	Specify how long in seconds the receiving device will hold an LLDP packet before discarding it.	2 to 10	4

UI Setting	Description	Valid Range	Default Value
Chassis ID Subtype	Specify the Chassis ID subtype of the device.	Chassis-Component / If-Alias / Port-Component / MAC-Address / Network-Address / If-Name / Local	MAC-Address
Chassis ID **(If Chassis ID Subtype is Chassis-Component, Port-Component, or Local)**	Specify the Chassis ID. **Note** The MAC address of the default VLAN is often used for the Chassis ID.	1 to 255 characters	N/A

LLDP Port List



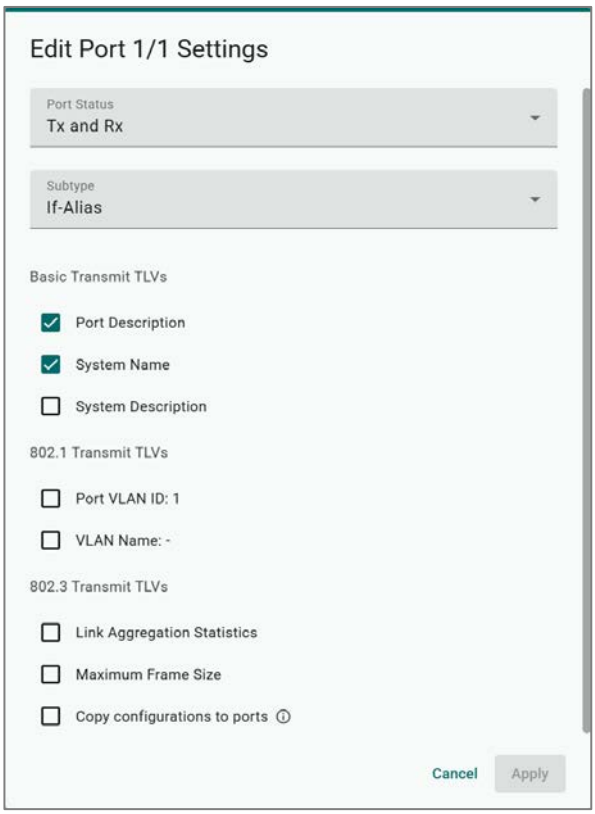
UI Setting	Description
Port	Shows the port number the entry is for.
Port Status	Show the status of what data is being transmitted for the port.

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
Port Status	Specify the port status for transmitting data.	Tx and Rx / Tx Only / Rx Only	Tx and Rx
Subtype	Specify the Chassis ID subtype for the port.	Chassis-Component / If-Alias / Port-Component / MAC-Address / Network-Address / If-Name / Local	If-Alias
Port Component Description **(If Subtype is Port-Component or Local)**	Specify a port component description (optional).	0 to 255 characters	N/A
Basic Transmit TLVs	Select the basic information to use for the TLV. You can select multiple options.	Port Description / System Name / System Description	Port Description, System Name
802.1 Transmit TLVs	Select the 802.1 information to use for the TLV. You can select multiple options.	Port VLAN ID / VLAN Name	N/A

UI Setting	Description	Valid Range	Default Value
802.3 Transmit TLVs	Select the 802.3 information to use for the TLV. You can select multiple options.	Link Aggregation Statistics / Maximum Frame Size	N/A
Copy configurations to ports	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

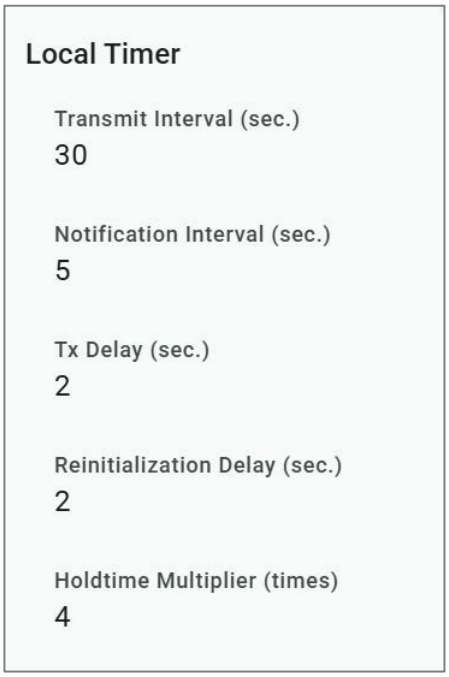
This page lets you see the status of LLDP on your device.

Local Information



UI Setting	Description
LLDP	Shows whether LLDP is enabled.
LLDP Version	Shows the LLDP version.
Chassis ID Subtype	Shows the chassis ID subtype.
Chassis ID	Shows the chassis ID.
System Capability	Shows the system capability.
Interface ID / Management Address	Shows the interface ID and the management IP address.

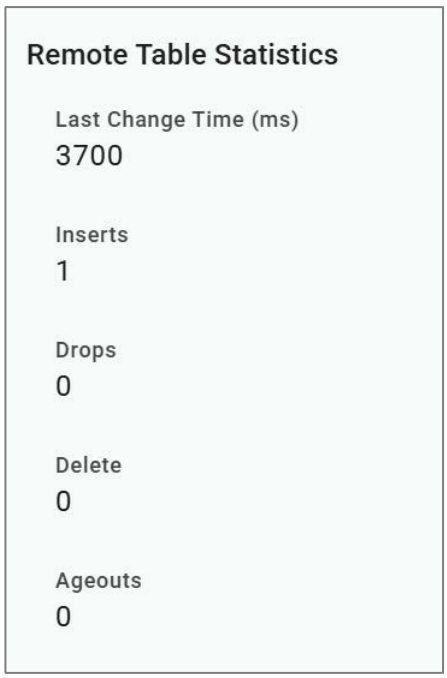
Local Timer



UI Setting	Description
Transmit Interval	Shows the interval between regular LLDP packet transmissions.
Notification Interval	Shows the interval between sending notifications.

UI Setting	Description
Tx Delay	Shows the delay period between successive LLDP frame transmissions initiated by changes.
Reinitialization Delay	Shows the delay an LLDP port waits before reinitializing an LLDP packet transmission.
Holdtime Multiplier	Shows the amount of time that the receiving device will hold an LLDP packet before discarding it.

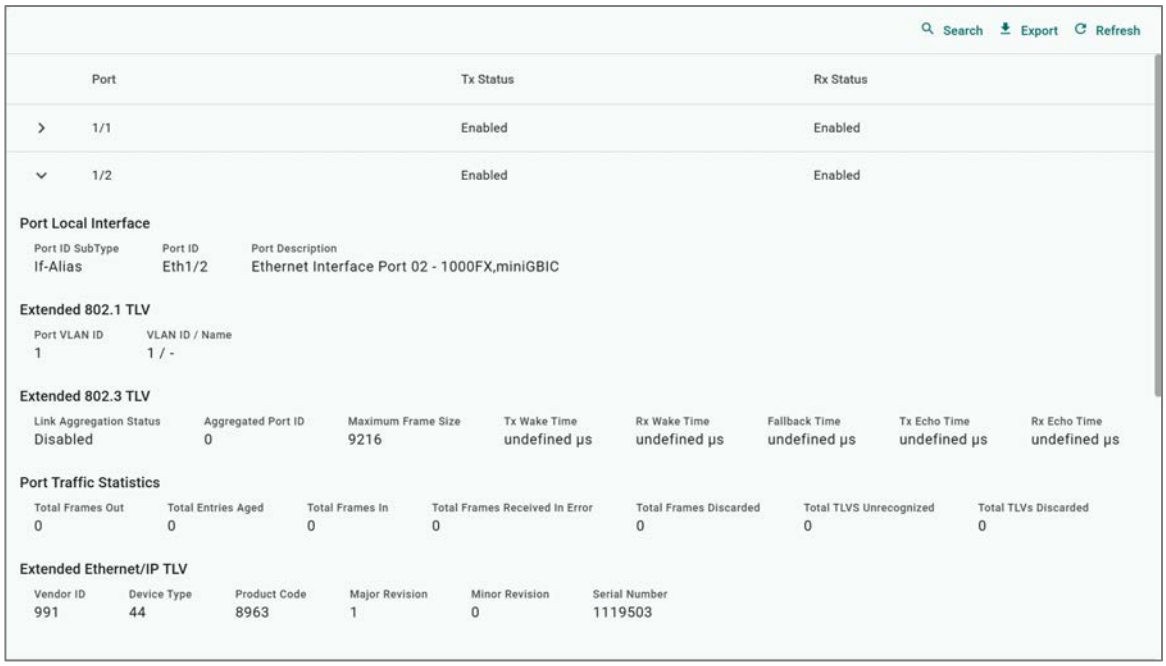
Remote Table Statistics



UI Setting	Description
Last Change Time (ms)	Shows how long ago in milliseconds the remote table was last changed.
Inserts	Shows how many inserts have occurred since the last change.
Drops	Shows how many drops have occurred since the last change.
Delete	Shows how many deletes have occurred since the last change.
Ageouts	Shows how many ageouts have occurred since the last change.

LLDP Port Status

To view the detailed LLDP status for a specific port, click the **detailed information (›)** icon for the port.



UI Setting	Description
Port	Shows the port number the entry is for.
Tx Status	Shows whether LLDP is enabled for transmit traffic.
Rx Status	Shows whether LLDP is enabled for receive traffic.

menu reference LLDP - Neighbor Status

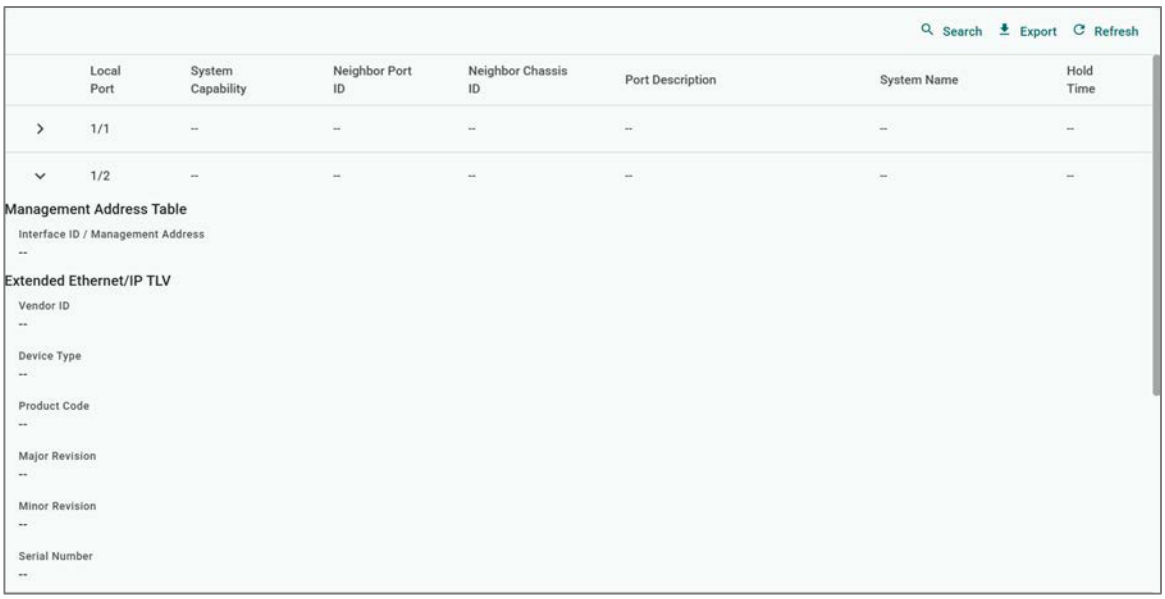
LLDP - Neighbor Status

Menu Path: Diagnostics > Network Status > LLDP - Neighbor Status

This page lets you see the neighbor status of LLDP.

Neighbor Status Port List

To view the detailed status for a specific port, click the **detailed information (›)** icon for the port.



UI Setting	Description
Local Port	Shows the number of the port connected to the neighbor.
System Capability	Shows the system capability of the neighbor.
Neighbor Port ID	Shows the neighbor's port ID for the interface this device is connected to.
Neighbor Chassis ID	Shows the unique ID (typically the MAC address) used to identify the neighbor device.
Port Description	Shows the neighbor's port description for the interface this device is connected to.
System Name	Shows the hostname of the neighbor device.
Hold Time	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

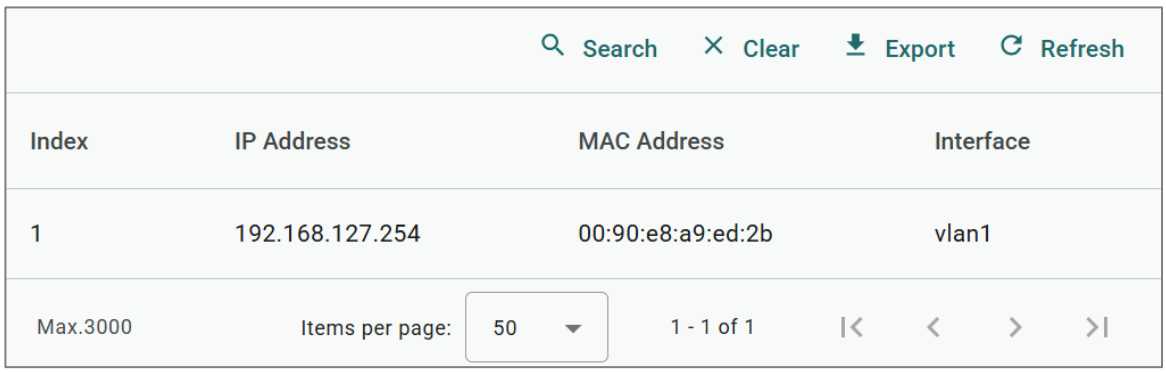
Menu Path: Diagnostics > Network Status > ARP Table

This page lets you see the device's Address Resolution Protocol (ARP) table.

Limitations

The ARP table can hold up to 3000 entries.

ARP Table



UI Setting	Description
Index	Shows the index of the device entry.
IP Address	Shows the IP address used for the device.
MAC Address	Shows the MAC address of the device.
Interface	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 and VLAN Mirroring

Port and VLAN mirroring is used to monitor data being transmitted through specific ports or VLANs. This is done by setting up mirror ports to receive the same data being transmitted to, from, or both to and from the ports or VLANs being monitored. Using mirror ports allows network administrators to sniff the observed ports or VLANs to keep tabs on network activity. This feature is commonly used for network analysis, performance monitoring, or troubleshooting.

Use cases include:

- Monitoring traffic for a specific port or VLAN
- Capturing packets for analysis with tools like Wireshark
- Troubleshooting network issues
- Detecting and analyzing suspicious activities

Port Mirroring In Depth

There are two ways to use Port Mirroring on this device:

- **SPAN (Switched Port Analyzer):** Mirrors data from monitored ports or VLANs to multiple terminal ports on the same switch.
- **RSPAN (Remote Switched Port Analyzer):** Mirrors data from monitored ports or VLANs on one switch to multiple terminal ports on other switches.

Note

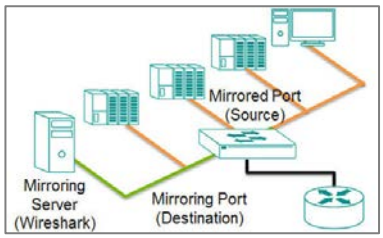
Whether Port Mirroring and VLAN Mirroring can be enabled at the same time depends on the product model.

- RKS-(G)4000 Series: Port Mirroring and VLAN Mirroring can not be enabled at the same time

SPAN Port Mirroring

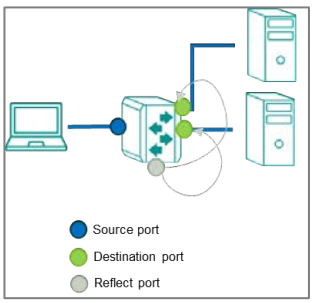
SPAN can be configured to copy packets from various ports to a single port or multiple ports so users can check if there are problems occurring in these ports.

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 packets for issues. This is useful for troubleshooting or monitoring network data transmissions for debugging or security purposes.



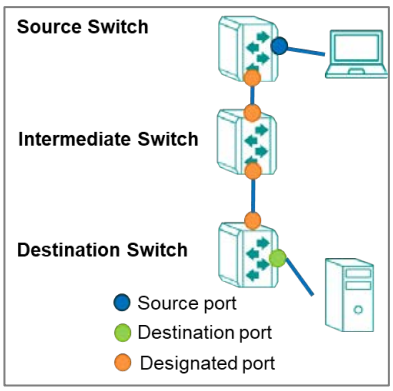
Ingress, egress, or both ingress and egress traffic can be mirrored to one or more destination ports.

If you want to mirror traffic to multiple destination ports, then a reflect port needs to be assigned and the destination ports need to be in the same VLAN as the reflect port.



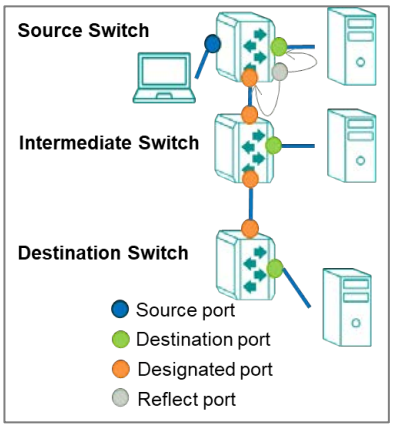
RSPAN Port Mirroring

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 the source switch, intermediate switch(es), and destination switch(es) need to be in the same VLAN as the reflect port.



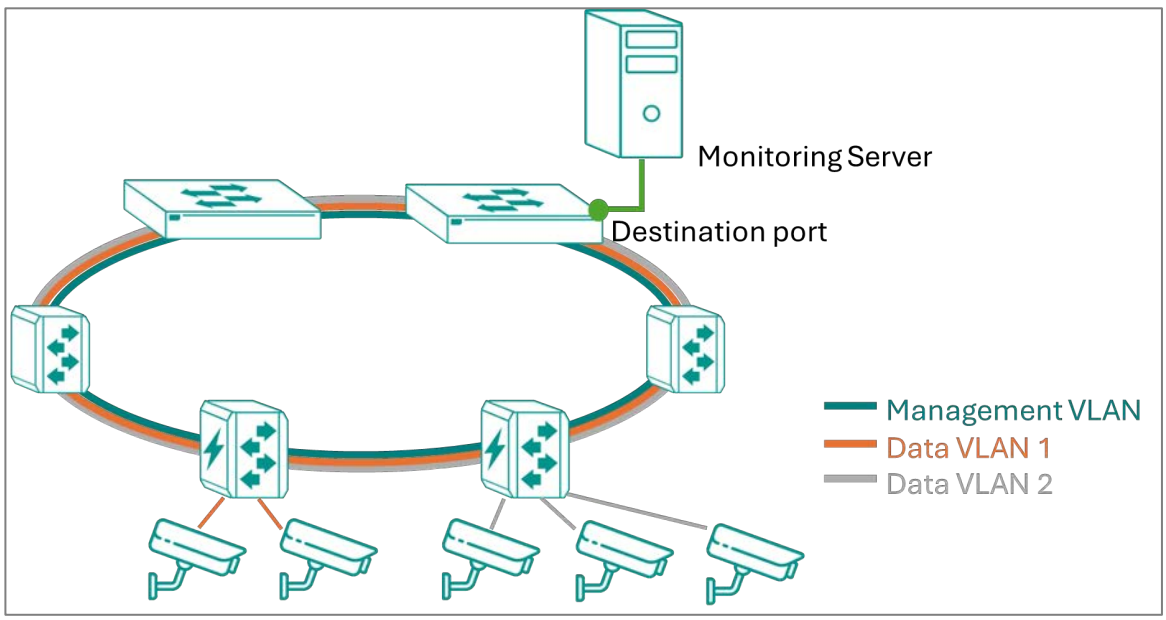
- You can set source ports to be from one or more RSPAN source switches. If one of the destination ports is on a source switch, a reflect port needs to be assigned.

- 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.

SPAN and RSPAN - VLAN Mirroring

VLAN Mirroring for SPAN and RSPAN can be configured to copy packets from various VLANs to a single port or multiple ports in the same switch (SPAN) or in different switches (RSPAN), so that users can check if there are problems occurring in these VLANs.

For example, with RSPAN VLAN mirroring as in the following figure, you can select Data VLAN 1 or 2 as a source VLAN, then packets transmitted through the ports within the selected source VLANs will be copied (mirrored) through intermediate switches in the ring to a single mirroring port (marked in green). These packets will be sent to a monitoring computer where software is used to check packets for issues. This is useful for troubleshooting or monitoring network data transmissions for debugging or security purposes.



- You can set source VLANs 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 (must be different from source VLANs and management VLANs) 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.

Enabling Mirroring

1. Sign in to the device with administrator credentials.
2. Go to **Diagnostics** > **Tools** > **Port and VLAN Mirroring**, and then click **General**.
3. Set **Port and VLAN Mirroring** to **Enabled** and then select **Apply**.

Mirroring is now active.

Configuring Port Mirroring with Single-port SPAN

Mirror one port to one other port on the same switch.

1. Sign in to the device with administrator credentials.
2. Go to **Diagnostics** > **Tools** > **Port and VLAN Mirroring**, and then select **SPAN**.
3. Next to **SPAN Session**, select **Create**.

   Create SPAN Session appears.
4. Configure the following:

Option	Value
Session ID	Specify a unique session ID.
Source Type	**Ports**
Tx Source Ports	Mirrors specified egress traffic.

Option	Value
Rx Source Ports	Mirrors specified egress traffic.
Reflect Port Mode	**Disabled** for single-destination mirroring.
Destination Port	Specify the port to receive mirrored traffic.

Note

- Specify at least one item in Tx Source Ports or Rx Source Ports.
- The following must be unique among all sessions:
  - Tx Source Ports
  - Rx Source Ports
  - Destination Port

5. Select **Create**.

The session appears under **SPAN Session**.

Configuring VLAN Mirroring with Single-Port SPAN

Mirror one VLAN to one other port on the same switch.

Port Mirroring and VLAN Mirroring cannot be configured at the same time.

Only one VLAN Mirroring session can be active at a time.

1. Sign in to the device with administrator credentials.
2. Go to **Diagnostics** > **Tools** > **Port and VLAN Mirroring**, and then select **SPAN**.
3. Next to **SPAN Session**, select **Create**.

Create SPAN Session appears.

4. Configure the following:

Option	Value
Session ID	Specify a unique session ID.
Source Type	**VLANs**
Rx Source VLANs	Mirrors specified ingress traffic.

Option	Value
Reflect Port Mode	**Disabled** for single-destination mirroring.
Destination Port	Specify the port to receive mirrored traffic.

Note

The following must be unique among all sessions:

- Rx Source VLANs

5. Select **Create**.

The session appears under **SPAN Session**.

Configuring Port Mirroring with Multi-port SPAN

Mirror one port to multiple other ports on the same switch.

Note

This feature requires a Reflect Port, which has special requirements:

- Dedicated port
- For Layer 2 switches: Membership in management VLAN
- For Layer 3 switches: Membership in VLAN interfaces
- VLANs in Trunk or Hybrid Mode

Additionally, reflect ports with PVIDs from dynamically assigned VLANs are discouraged.

1. Sign in to the device with administrator credentials.
2. Go to **Diagnostics** > **Tools** > **Port and VLAN Mirroring**, and then select **SPAN**.
3. Next to **SPAN Session**, select **Create**.

   Create SPAN Session appears.

4. Configure the following:

Option	Value
Session ID	Specify a unique session ID.
Source Type	**Ports**

Option	Value
Tx Source Ports	Mirrors specified egress traffic.
Rx Source Ports	Specify the port to receive mirrored traffic.
Reflect Port Mode	**Enabled** for multi-destination mirroring.
Reflect Port	Select a port. Reflects or "bounces" traffic, often through an external network appliance. Required for multi-destination mirroring.

Info

- Specify at least one item in Tx Source Ports or Rx Source Ports.
- The following must be unique among all sessions:
  - Tx Source Ports
  - Rx Source Ports

5. Select **Create**.

The session appears under **SPAN Session**.

Configuring VLAN Mirroring with Multi-port SPAN

Mirror one or more VLANs to multiple other ports on the same switch.

Port Mirroring and VLAN Mirroring cannot be configured at the same time.

Only one VLAN Mirroring session can be active at a time.

Note

This feature requires a Reflect Port, which has special requirements:

- Dedicated port
- For Layer 2 switches: Membership in management VLAN
- For Layer 3 switches: Membership in VLAN interfaces
- VLANs in Trunk or Hybrid Mode

Additionally, reflect ports with PVIDs from dynamically assigned VLANs are discouraged.

1. Sign in to the device with administrator credentials.
2. Go to **Diagnostics** > **Tools** > **Port and VLAN Mirroring**, and then select **SPAN**.

3. Next to **SPAN Session**, select **Create**.

Create SPAN Session appears.

4. Configure the following:

Option	Value
Session ID	Specify a unique session ID.
Source Type	**VLANs**
Rx Source VLANs	Mirrors specified ingress traffic.
Reflect Port Mode	**Enabled** for multi-destination mirroring.
Reflect Port	Select a port. Reflects or "bounces" traffic, often through an external network appliance. Required for multi-destination mirroring.

Note

The following must be unique among all sessions:

- Rx Source VLANs

5. Select **Create**.

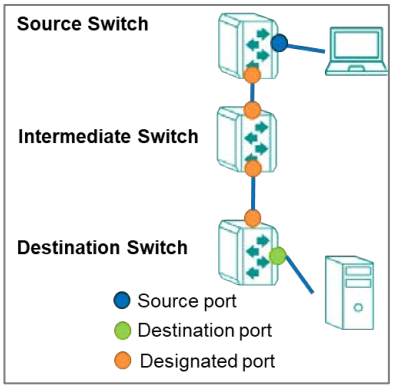
The session appears under **SPAN Session**.

Configuring Port Mirroring with Single-destination RSPAN

RSPAN topologies usually incorporate 3 or more switches between the source and destination ports.

When planning for RSPAN, a given RSPAN switch can only be a source or destination switch once across all RSPAN sessions. For example, Switch A can be a source switch for session 6, and a destination for session 7, but cannot be a source twice.

Intermediate switches can be intermediates for session 6 and 7, but cannot serve in any other roles.



1. Configure source switch.
2. Configure intermediate switch.
3. Configure destination switch.

The following sections outline how to configure RSPAN when the destination port is located on the destination switch.

Configuring a Source Switch for RSPAN Single-destination Port Mirroring

To monitor a port, create an RSPAN session with the source role and specify a Source Port.

> **Note**
>
> Make sure you have a dedicated RSPAN VLAN, with the following requirements:
>
> - Source, intermediate, and destination switches in the same session must use the same RSPAN VLAN.
> - RSPAN VLAN must be unique among all RSPAN sessions.
> - Do not use management VLANs (L2 switches) or VLAN interfaces (L3 switches) as the RSPAN VLAN.
> - Avoid using dynamic VLANs for the RSPAN VLAN.

1. Sign in to the device with administrator credentials.
2. Go to **Diagnostics** > **Tools** > **Port and VLAN Mirroring**, and then click **RSPAN**.
3. Next to **RSPAN Session**, select **Create**.

   The **Create RSPAN Session** screen appears.
4. Configure the following:

Option	Value
Session ID	Specify a unique session ID. The **Session ID** is a local setting, and does not need to match source, intermediate, and destination switches.
RSPAN Type	**Source** for RSPAN source switches.
Source Type	**Ports**
Tx Source Ports	Mirrors specified egress traffic.
Rx Source Ports	Mirrors specified ingress traffic.
Reflect Port Mode	**Disabled** for single-destination mirroring.
RSPAN VLAN ID	Choose a VLAN to carry the mirrored traffic.
Designated Port	Specify the port for mirrored traffic to exit the switch.

Note

- Specify at least one item in Tx Source Ports or Rx Source Ports.
- The following must be unique among all sessions:
  - Tx Source Ports
  - Rx Source Ports

5. Select **Create**.

The RSPAN session appears under **RSPAN Session**.

Configuring an Intermediate Switch for RSPAN Single-destination Port Mirroring

RSPAN intermediate switches relay mirrored port traffic from source to destination switches.

Note

Make sure you have a dedicated RSPAN VLAN, with the following requirements:

- Source, intermediate, and destination switches in the same session must use the same RSPAN VLAN.
- RSPAN VLAN must be unique among all RSPAN sessions.
- Do not use management VLANs (L2 switches) or VLAN interfaces (L3 switches) as the RSPAN VLAN.
- Avoid using dynamic VLANs for the RSPAN VLAN.

Assign the **RSPAN VLAN** to both the ingress and egress ports on the intermediate switch.

1. Sign in to the device with administrator credentials.
2. Go to **Diagnostics** > **Tools** > **Port and VLAN Mirroring**, and then click **RSPAN**.
3. Set **RSPAN Intermediate Role** to **Enabled**.

   RSPAN Intermediate VLAN ID options appear.
4. Configure the following:

Options	Value
RSPAN Intermediate 1st VLAN ID	Specify the VLAN ID that carries mirrored traffic.
RSPAN Intermediate 2nd VLAN ID	Specify the VLAN ID that carries mirrored traffic for an additional RSPAN session.

5. Select **Apply** to save changes.

Configuring a Destination Switch for RSPAN Single-destination Port Mirroring

RSPAN destination switches are the primary exit points for mirrored traffic.

Note

Make sure you have a dedicated RSPAN VLAN, with the following requirements:

- Source, intermediate, and destination switches in the same session must use the same RSPAN VLAN.
- RSPAN VLAN must be unique among all RSPAN sessions.
- Do not use management VLANs (L2 switches) or VLAN interfaces (L3 switches) as the RSPAN VLAN.
- Avoid using dynamic VLANs for the RSPAN VLAN.

1. Sign in to the device with administrator credentials.

2. Go to **Diagnostics** > **Tools** > **Port and VLAN Mirroring**, and then click **RSPAN**.
3. Next to **RSPAN Session**, select **Create**.

The **Create RSPAN Session** screen appears.

4. Configure the following:

Option	Value
Session ID	Specify a unique session ID. The **Session ID** is a local setting, and does not need to match source, intermediate, and destination switches.
RSPAN Type	**Destination** for RSPAN Destination Switches.
Source Type	**Ports**
RSPAN VLAN ID	Choose a VLAN to carry the mirrored traffic.
Destination Ports	Specify the destination port or ports for the mirrored traffic.

5. Select **Create**.

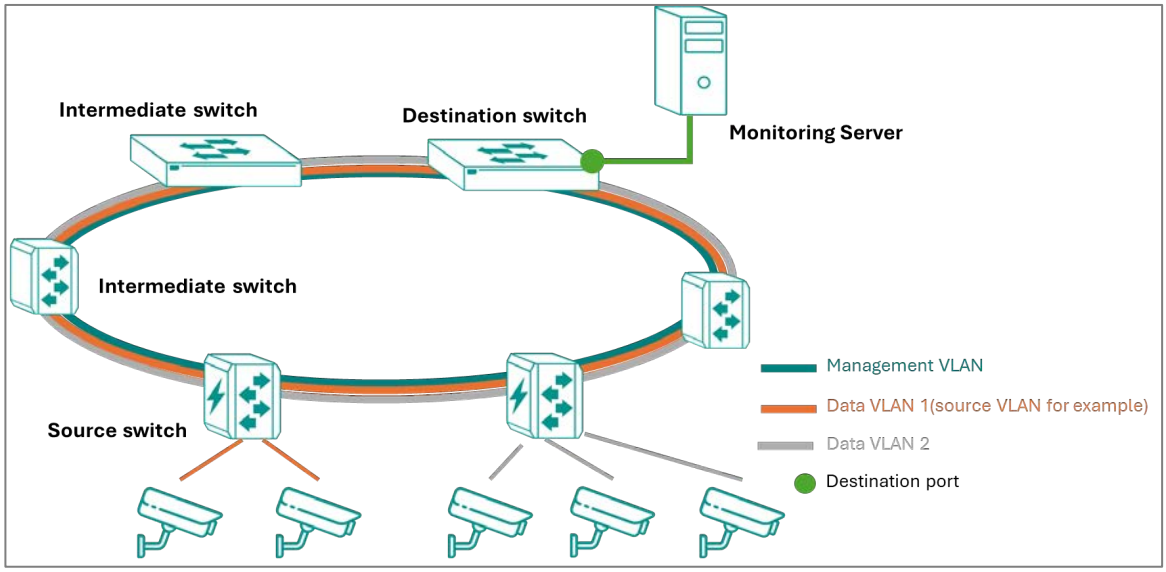
The RSPAN session appears under **RSPAN Session**.

Configuring VLAN Mirroring with Single-destination RSPAN

RSPAN topologies usually incorporate 3 or more switches between the source VLAN and destination port.

When planning for RSPAN, a given RSPAN switch can only be a source or destination switch once across all RSPAN sessions. For example, Switch A can be a source switch for session 6, and a destination for session 7, but cannot be a source twice.

Intermediate switches can be intermediates for session 6 and 7, but cannot serve in any other roles.



1. Configure Source Switch.
2. Configure intermediate switch.
3. Configure destination switch.

The following sections outline how to configure RSPAN when the destination VLAN is located on the destination switch.

Configuring a Source Switch for RSPAN Single-destination VLAN Mirroring

To monitor a VLAN, create an RSPAN session with the source role and specify a source VLAN.

Note

Make sure you have a dedicated RSPAN VLAN, with the following requirements:

- Source, intermediate, and destination switches in the same session must use the same RSPAN VLAN.
- RSPAN VLAN must be unique among all RSPAN sessions.
- Do not use management VLANs (L2 switches) or VLAN interfaces (L3 switches) as the RSPAN VLAN.
- Avoid using dynamic VLANs for the RSPAN VLAN.

1. Sign in to the device with administrator credentials.
2. Go to **Diagnostics** > **Tools** > **Port and VLAN Mirroring**, and then click **RSPAN**.
3. Next to **RSPAN Session**, select **Create**.

The **Create RSPAN Session** screen appears.

4. Configure the following:

Option	Value
Session ID	Specify a unique session ID. The **Session ID** is a local setting, and does not need to match source, intermediate, and destination switches.
RSPAN Type	**Source** for RSPAN source switches.
Source Type	**VLANs**
Source VLANs	Mirrors specified ingress traffic.
RSPAN VLAN ID	Choose a VLAN to carry the mirrored traffic.
Reflect Port Mode	**Disabled** for single-destination mirroring.
Designated Port	Specify the port for mirrored traffic to exit the switch.

Note

The following must be unique among all sessions:

- Source VLANs

5. Select **Create**.

The RSPAN session appears under **RSPAN Session**.

Specified **Destination Ports** are automatically added to the RSPAN VLAN.

Configuring an Intermediate Switch for RSPAN Single-destination VLAN Mirroring

RSPAN Intermediate switches relay mirrored VLAN traffic from the source switch to the destination switch.

Note

Make sure you have a dedicated RSPAN VLAN, with the following requirements:

- Source, intermediate, and destination switches in the same session must use the same RSPAN VLAN.
- RSPAN VLAN must be unique among all RSPAN sessions.
- Do not use management VLANs (L2 switches) or VLAN interfaces (L3 switches) as the RSPAN VLAN.
- Avoid using dynamic VLANs for the RSPAN VLAN.

Assign the **RSPAN VLAN** to both the ingress and egress ports on the intermediate switch.

1. Sign in to the device with administrator credentials.
2. Go to **Diagnostics** > **Tools** > **Port and VLAN Mirroring**, and then click **RSPAN**.
3. Set **RSPAN Intermediate Role** to **Enabled**.

   RSPAN Intermediate VLAN ID options appear.
4. Configure the following:

Options	Value
RSPAN Intermediate 1st VLAN ID	Specify the VLAN ID that carries mirrored traffic.
RSPAN Intermediate 2nd VLAN ID	Specify the VLAN ID that carries mirrored traffic for an additional RSPAN session.

5. Select **Apply** to save changes.

Configuring a Destination Switch for RSPAN Single-destination VLAN Mirroring

RSPAN destination switches are the primary exit points for mirrored traffic. Create an RSPAN session and specify a destination port.

Note

Make sure you have a dedicated RSPAN VLAN, with the following requirements:

- Source, intermediate, and destination switches in the same session must use the same RSPAN VLAN.
- RSPAN VLAN must be unique among all RSPAN sessions.
- Do not use management VLANs (L2 switches) or VLAN interfaces (L3 switches) as the RSPAN VLAN.
- Avoid using dynamic VLANs for the RSPAN VLAN.

1. Sign in to the device with administrator credentials.
2. Go to **Diagnostics** > **Tools** > **Port and VLAN Mirroring**, and then click **RSPAN**.
3. Next to **RSPAN Session**, select **Create**.

   The **Create RSPAN Session** screen appears.
4. Configure the following:

Option	Value
Session ID	Specify a unique session ID. The **Session ID** is a local setting, and does not need to match source, intermediate, and destination switches.
RSPAN Type	**Destination** for RSPAN Destination Switches.
RSPAN VLAN ID	Choose a VLAN to carry the mirrored traffic.
Destination Ports	Specify the destination port or ports for the mirrored traffic.

5. Select **Create**.

The RSPAN session appears under **RSPAN Session**.

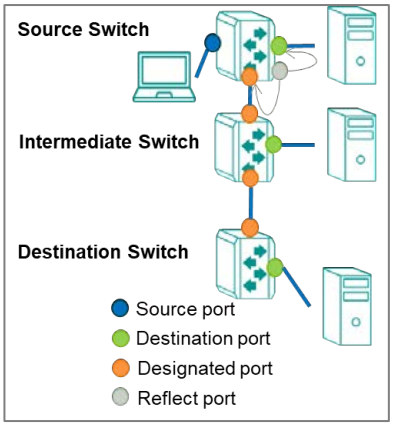
Configuring Port Mirroring with Multi-destination RSPAN

Port mirroring with multi-destination RSPAN uses the RPSAN VLAN and reflect port mode to support multiple destinations.

RSPAN topologies usually incorporate 3 or more switches between the source and destination ports.

When planning for RSPAN, a given RSPAN switch can only be a source or destination switch once across all RSPAN sessions. For example, Switch A can be a source switch for session 6, and a destination for session 7, but cannot be a source twice.

Intermediate switches can be intermediates for session 6 and 7, but cannot serve in any other roles.



1. Configure source switch.
2. Configure intermediate switch.
3. Configure destination switch.

The following sections outline how to configure RSPAN when the destination port is located on the destination switch.

Configuring a Source Switch for RSPAN Multi-destination Port Mirroring

To monitor a port and copy traffic to multiple destinations, create an RSPAN session with the source role, specify a source port, and configure **Reflect Port Mode**.

Note

Make sure you have a dedicated RSPAN VLAN, with the following requirements:

- Source, intermediate, and destination switches in the same session must use the same RSPAN VLAN.
- RSPAN VLAN must be unique among all RSPAN sessions.
- Do not use management VLANs (L2 switches) or VLAN interfaces (L3 switches) as the RSPAN VLAN.
- Avoid using dynamic VLANs for the RSPAN VLAN.

Note

This feature requires a Reflect Port, which has special requirements:

- Dedicated port
- For Layer 2 switches: Membership in management VLAN
- For Layer 3 switches: Membership in VLAN interfaces
- VLANs in Trunk or Hybrid Mode

Additionally, reflect ports with PVIDs from dynamically assigned VLANs are discouraged.

1. Sign in to the device with administrator credentials.
2. Go to **Diagnostics** > **Tools** > **Port and VLAN Mirroring**, and then click **RSPAN**.
3. Next to **RSPAN Session**, select **Create**.

   The **Create RSPAN Session** screen appears.
4. Configure the following:

Option	Value
Session ID	Specify a unique session ID. The **Session ID** is a local setting, and does not need to match source, intermediate, and destination switches.
RSPAN Type	**Source** for RSPAN source switches.
Source Type	**Ports**
Tx Source Ports	Mirrors specified egress traffic.
Rx Source Ports	Mirrors specified ingress traffic.
RSPAN VLAN ID	Choose a VLAN to carry the mirrored traffic.
Reflect Port Mode	**Enabled** for multi-destination mirroring. This is required if there are multiple destination ports.
Reflect Port	Select a port. Reflects or "bounces" traffic, often through an external network appliance. Required for multi-destination mirroring.

Note

- Specify at least one item in Tx Source Ports or Rx Source Ports.
- The following must be unique among all sessions:
  - Tx Source Ports
  - Rx Source Ports

5. Select **Create**.

The RSPAN session appears under **RSPAN Session**.

Specified **Destination Ports** are automatically added to the RSPAN VLAN.

Configuring an Intermediate Switch for RSPAN Multi-destination Port Mirroring

RSPAN intermediate switches relay mirrored port traffic from source to destination switches, and can mirror monitored traffic to local ports added to the RSPAN VLAN.

Note

Make sure you have a dedicated RSPAN VLAN, with the following requirements:

- Source, intermediate, and destination switches in the same session must use the same RSPAN VLAN.
- RSPAN VLAN must be unique among all RSPAN sessions.
- Do not use management VLANs (L2 switches) or VLAN interfaces (L3 switches) as the RSPAN VLAN.
- Avoid using dynamic VLANs for the RSPAN VLAN.

Assign the RSPAN VLAN to both the ingress and egress ports on the intermediate switch.

1. Sign in to the device with administrator credentials.
2. Go to **Diagnostics** > **Tools** > **Port and VLAN Mirroring**, and then click **RSPAN**.
3. Set **RSPAN Intermediate Role** to **Enabled**.

   RSPAN Intermediate VLAN ID options appear.
4. Configure the following:

Options	Value
RSPAN Intermediate 1st VLAN ID	Specify the VLAN ID that carries mirrored traffic.
RSPAN Intermediate 2nd VLAN ID	Specify the VLAN ID that carries mirrored traffic for an additional RSPAN session.

5. Select **Apply** to save changes.

Additional destination ports may be added to intermediate switches by adding them to the RSPAN VLAN.

Configuring a Destination Switch for RSPAN Multi-destination Port Mirroring

RSPAN destination switches are the primary exit points for mirrored port traffic. Multiple destination ports can be specified by adding local ports to the RSPAN VLAN.

> **Note**
>
> Make sure you have a dedicated RSPAN VLAN, with the following requirements:
>
> - Source, intermediate, and destination switches in the same session must use the same RSPAN VLAN.
> - RSPAN VLAN must be unique among all RSPAN sessions.
> - Do not use management VLANs (L2 switches) or VLAN interfaces (L3 switches) as the RSPAN VLAN.
> - Avoid using dynamic VLANs for the RSPAN VLAN.

1. Sign in to the device with administrator credentials.
2. Go to **Diagnostics** > **Tools** > **Port and VLAN Mirroring**, and then click **RSPAN**.
3. Next to **RSPAN Session**, select **Create**.

The **Create RSPAN Session** screen appears.

4. Configure the following:

Option	Value
Session ID	Specify a unique session ID. The **Session ID** is a local setting, and does not need to match source, intermediate, and destination switches.
RSPAN Type	**Destination** for RSPAN Destination Switches.
RSPAN VLAN ID	Choose a VLAN to carry the mirrored traffic.
Destination Ports	Specify the destination port or ports for the mirrored traffic. Specified **Destination Ports** are automatically added to the RSPAN VLAN.

5. Select **Create**.

The RSPAN session appears under **RSPAN Session**.

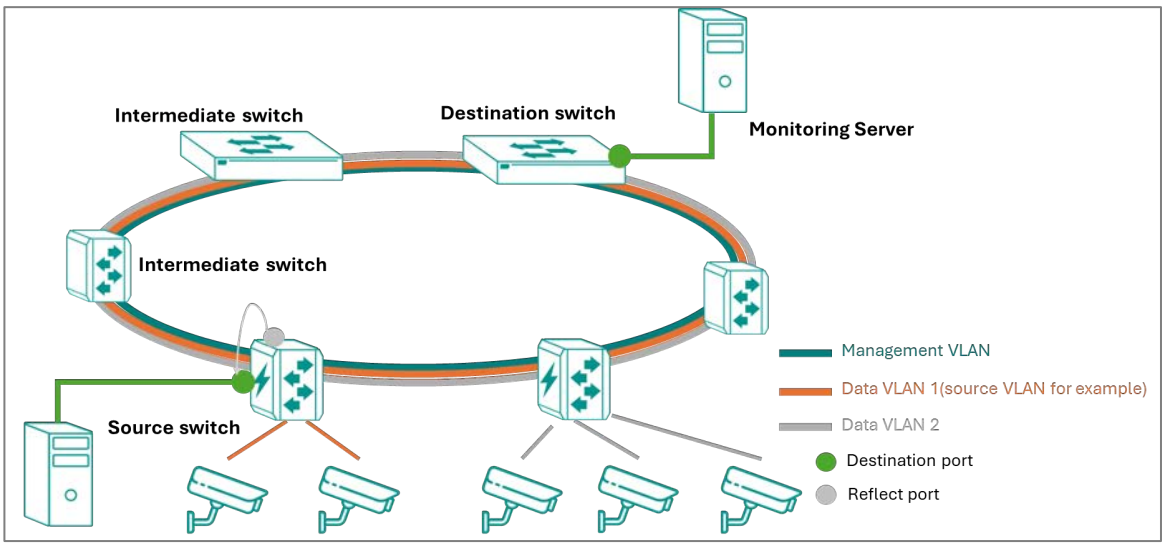
Configuring VLAN Mirroring with Multi-destination RSPAN

VLAN mirroring with multi-destination RSPAN uses the RPSAN VLAN and reflect port mode to support multiple destinations.

RSPAN topologies usually incorporate 3 or more switches between the source and destination.

When planning for RSPAN, a given RSPAN switch can only be a source or destination switch once across all RSPAN sessions. For example, Switch A can be a source switch for session 6, and a destination for session 7, but cannot be a source twice.

Intermediate switches can be intermediates for session 6 and 7, but cannot serve in any other roles.



1. Configure source switch.
2. Configure intermediate switch.
3. Configure destination switch.

The following sections outline how to configure RSPAN when the destination port is located on the destination switch.

Configuring a Source Switch for RSPAN Multi-destination VLAN Mirroring

To monitor a VLAN and copy traffic to multiple destinations, create an RSPAN session with the source role, specify a source VLAN, and configure **Reflect Port Mode**.

Note

Make sure you have a dedicated RSPAN VLAN, with the following requirements:

- Source, intermediate, and destination switches in the same session must use the same RSPAN VLAN.
- RSPAN VLAN must be unique among all RSPAN sessions.
- Do not use management VLANs (L2 switches) or VLAN interfaces (L3 switches) as the RSPAN VLAN.
- Avoid using dynamic VLANs for the RSPAN VLAN.

Note

This feature requires a Reflect Port, which has special requirements:

- Dedicated port
- For Layer 2 switches: Membership in management VLAN
- For Layer 3 switches: Membership in VLAN interfaces
- VLANs in Trunk or Hybrid Mode

Additionally, reflect ports with PVIDs from dynamically assigned VLANs are discouraged.

1. Sign in to the device with administrator credentials.
2. Go to **Diagnostics** > **Tools** > **Port and VLAN Mirroring**, and then click **RSPAN**.
3. Next to **RSPAN Session**, select **Create**.

The **Create RSPAN Session** screen appears.

4. Configure the following:Select **Create**.

Option	Value
Session ID	Specify a unique session ID. The **Session ID** is a local setting, and does not need to match source, intermediate, and destination switches.
RSPAN Type	**Source** for RSPAN source switches.
Source Type	**VLANs**
Source VLANs	Mirrors specified ingress traffic.
RSPAN VLAN ID	Choose a VLAN to carry the mirrored traffic.

Option	Value
Reflect Port Mode	**Enabled** for multi-destination mirroring. This is required if there are multiple destination ports.
Reflect Port	Select a port. Reflects or "bounces" traffic, often through an external network appliance. Required for multi-destination mirroring.

Note

The following must be unique among all sessions:

- Source VLANs

5. The RSPAN session appears under **RSPAN Session**.

Specified **Destination Ports** are automatically added to the RSPAN VLAN.

Configuring an Intermediate Switch for RSPAN Multi-destination VLAN Mirroring

RSPAN intermediate switches relay mirrored VLAN traffic from source switches to destination switches, and can mirror monitored traffic to local ports added to the RSPAN VLAN.

Note

Make sure you have a dedicated RSPAN VLAN, with the following requirements:

- Source, intermediate, and destination switches in the same session must use the same RSPAN VLAN.
- RSPAN VLAN must be unique among all RSPAN sessions.
- Do not use management VLANs (L2 switches) or VLAN interfaces (L3 switches) as the RSPAN VLAN.
- Avoid using dynamic VLANs for the RSPAN VLAN.

Assign the **RSPAN VLAN** to both the ingress and egress ports on the intermediate switch.

1. Sign in to the device with administrator credentials.
2. Go to **Diagnostics** > **Tools** > **Port and VLAN Mirroring**, and then click **RSPAN**.
3. Set **RSPAN Intermediate Role** to **Enabled**.

RSPAN Intermediate VLAN ID options appear.

4. Configure the following:

Options	Value
RSPAN Intermediate 1st VLAN ID	Specify the VLAN ID that carries mirrored traffic.
RSPAN Intermediate 2nd VLAN ID	Specify the VLAN ID that carries mirrored traffic for an additional RSPAN session.

5. Select **Apply** to save changes.

Additional destination ports may be added to intermediate switches by adding them to the RSPAN VLAN.

Configuring a Destination Switch for RSPAN Multi-destination VLAN Mirroring

RSPAN destination switches are the primary exit points for mirrored VLAN traffic. Multiple destination ports can be specified by adding local ports to the RSPAN VLAN.

Note

Make sure you have a dedicated RSPAN VLAN, with the following requirements:

- Source, intermediate, and destination switches in the same session must use the same RSPAN VLAN.
- RSPAN VLAN must be unique among all RSPAN sessions.
- Do not use management VLANs (L2 switches) or VLAN interfaces (L3 switches) as the RSPAN VLAN.
- Avoid using dynamic VLANs for the RSPAN VLAN.

1. Sign in to the device with administrator credentials.
2. Go to **Diagnostics** > **Tools** > **Port and VLAN Mirroring**, and then click **RSPAN**.
3. Next to **RSPAN Session**, select **Create**.

The **Create RSPAN Session** screen appears.

4. Configure the following:

Option	Value
Session ID	Specify a unique session ID. The **Session ID** is a local setting, and does not need to match source, intermediate, and destination switches.
RSPAN Type	**Destination** for RSPAN Destination Switches.
RSPAN VLAN ID	Choose a VLAN to carry the mirrored traffic.
Destination Ports	Specify the destination port or ports for the mirrored traffic. Specified **Destination Ports** are automatically added to the RSPAN VLAN.

5. Select **Create**.

The RSPAN session appears under **RSPAN Session**.

Port and VLAN Mirroring

Menu Path: Diagnostics > Tools > Port and VLAN Mirroring

This page lets you configure port and VLAN mirroring for your device.

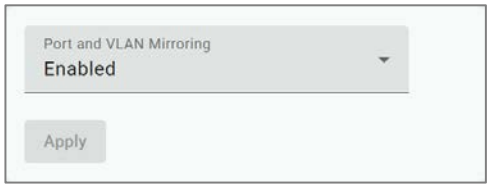
This page includes these tabs:

- General
- SPAN
- RSPAN

Port and VLAN Mirroring - General

Menu Path: Diagnostics > Tools > Port and VLAN Mirroring - General

This page lets you enable or disable port and VLAN mirroring for your device.



UI Setting	Description	Valid Range	Default Value
Port and VLAN Mirroring	Enable or disable port and VLAN mirroring to facilitate the creation of SPAN or RSPAN sessions.	Enabled / Disabled	Enabled

SPAN

Menu Path: Diagnostics > Tools > Port and VLAN Mirroring - SPAN

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

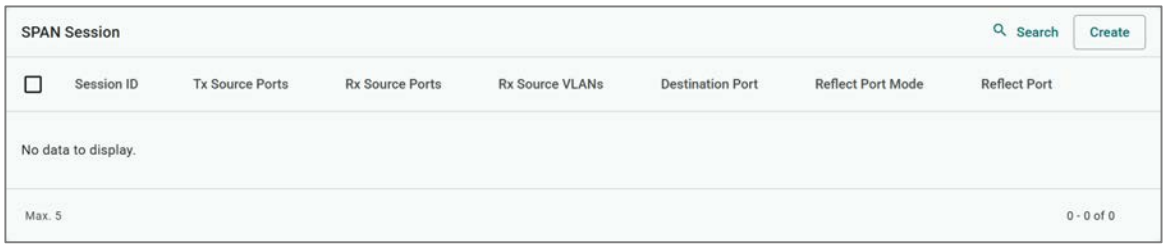
Limitations

You can create up to 5 SPAN entries.

Note

Port Mirroring and VLAN Mirroring cannot be active at the same time.

SPAN Session List



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.
Tx Source Ports	Shows the ports monitored for packets sent out.

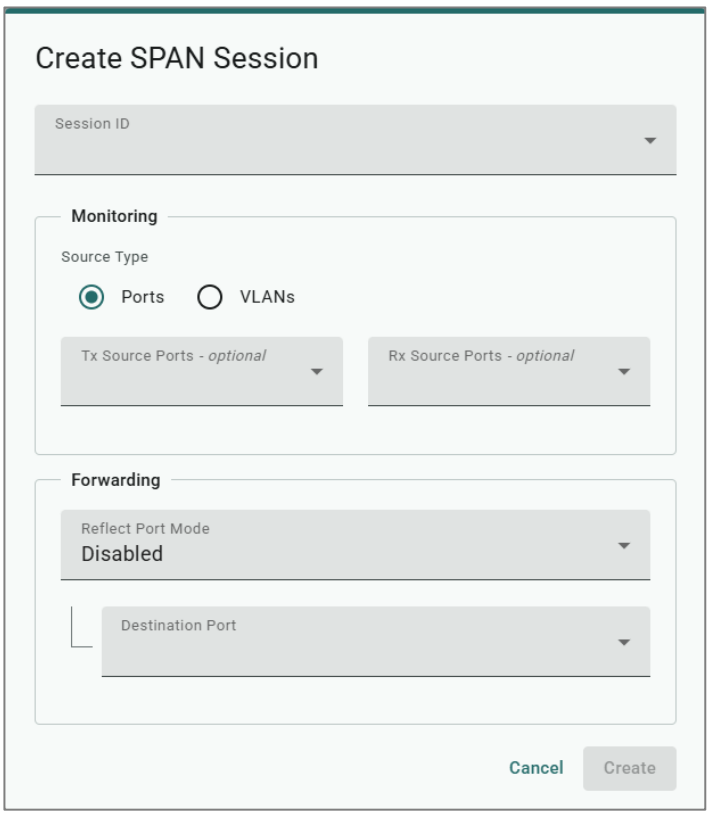
UI Setting	Description
Rx Source Ports	Shows the ports monitored for packets received.
Rx Source VLANs	Shows the VLANs monitored for packets received.
Destination Port	Shows the destination port for the session.
Reflect Port Mode	Shows whether Reflect Port Mode is enabled for the session.
Reflect Port	Shows the reflect port for the session.

Creating a SPAN Session

Menu Path: Diagnostics > Tools > Port and VLAN Mirroring - SPAN

Clicking **Create** on the **Diagnostics > Tools > Port and VLAN 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.



UI Setting	Description	Valid Range	Default Value
Session ID	Select the session ID to use for the session. **Note** SPAN and RSPAN share 7 sessions, SPAN uses 1 to 5, and RSPAN uses 6 and 7.	1 to 5	N/A
Source Type	Select the monitoring source type for the session. **Note** Port Mirroring and VLAN Mirroring cannot be configured at the same time. Only one VLAN Mirroring session can be active at any given time.	Ports / VLANs	Ports
Tx Source Ports **(If Source Type is Ports)**	Select ports to monitor for data packets being sent through them. **Note** Avoid selecting source ports that are in the same VLAN as the reflect port.	Drop-down list of ports	N/A
Rx Source Ports **(If Source Type is Ports)**	Select ports to monitor for data packets being received through them. **Note** Avoid selecting source ports that are in the same VLAN as the reflect port.	Drop-down list of ports	N/A
Rx Source VLANs **(If Source Type is VLANs)**	Select the VLAN(s) to monitor for data packets being received through them.	Drop-down list of VLANs	N/A
Reflect Port Mode	Enable or disable Reflect Port Mode. • **Enabled**: You can configure a reflect port to mirror packets to multiple destination ports. • **Disabled**: Packets will be mirrored to a single destination port.	Enabled / Disabled	N/A

UI Setting	Description	Valid Range	Default Value
Reflect Port **(If Reflect Port Mode is Enabled)**	Select the port to use as the reflect port for Reflect Port Mode to mirror packets to multiple destination ports. **Note** This port will be specifically reserved for reflect port use; please do not configure it for other uses. The reflect port must be a member of the management VLAN (for Layer 2 switches) or VLAN interfaces (for Layer 3 switches) to prevent looping. Select only Trunk or Hybrid mode VLAN ports to prevent dropping tagged frames. Using dynamically assigned VLANs as PVIDs of reflect ports is not recommended.	Drop-down list of ports	N/A
Destination Port **(If Reflect Port Mode is Disabled)**	Select the destination port to use for the session.	Drop-down list of ports	N/A

RSPAN

Menu Path: Diagnostics > Tools > Port and VLAN Mirroring - RSPAN

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

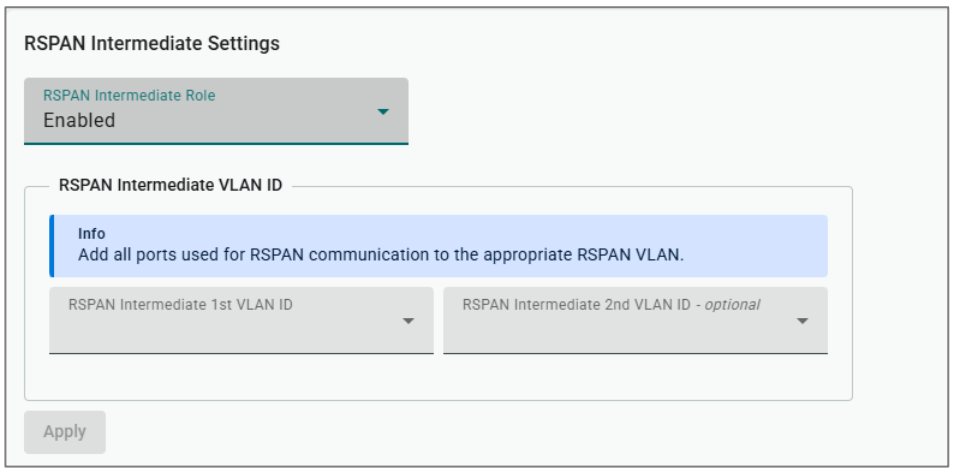
Limitations

You can create up to 2 RSPAN entries.

Note

Port Mirroring and VLAN Mirroring cannot be active at the same time.

RSPAN Intermediate Settings



UI Setting	Description	Valid Range	Default Value
RSPAN Intermediate Role	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
RSPAN Intermediate 1st/2nd VLAN ID	Specify the VLAN ID to use as the RSPAN intermediate VLAN ID. **Note** The management VLAN ID cannot be used as an RSPAN intermediate VLAN ID. Use of two RSPAN intermediate VLANs is supported as of firmware v5.0. If you downgrade your device's firmware to a version before v5.0, only the first VLAN ID will be reserved in the configuration.	Drop-down list of VLAN IDs	N/A

RSPAN Session List



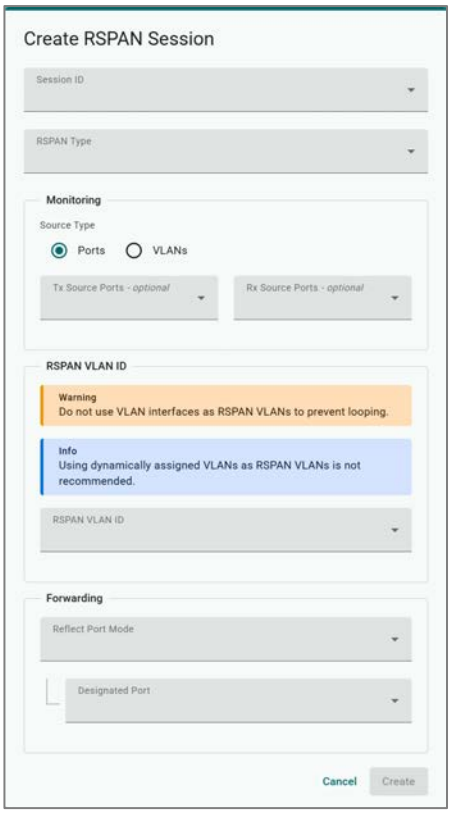
UI Setting	Description
Session ID	Shows the session ID the entry is for. **Note** SPAN and RSPAN share 7 sessions, SPAN uses 1 to 5, and RSPAN uses 6 and 7.
RSPAN Type	Shows **Source** if the device role is an RSPAN source switch. Shows **Destination** if the device role is an RSPAN destination switch.
RSPAN VLAN ID	Shows the VLAN ID used for the RSPAN.
Tx Source Ports	Shows the ports monitored for packets sent out.
Rx Source Ports	Shows the ports monitored for packets received.
Source VLANs	Shows the VLANs being monitored for packets received.
Destination Ports	Shows the destination ports for the session.
Designated Port	Shows the designated port for the session.
Reflect Port Mode	Shows whether Reflect Port Mode is enabled for the session.
Reflect Port	Shows the reflect port for the session.

Creating an RSPAN Session

Menu Path: Diagnostics > Tools > Port and VLAN Mirroring - RSPAN

Clicking **Create** on the **Diagnostics > Tools > Port and VLAN Mirroring - RSPAN** page will open this dialog box. This dialog lets you create an RSPAN mirroring session.

Click **Create** to save your changes and add the new session.



UI Setting	Description	Valid Range	Default Value
Session ID	Select the session ID to use for the session. **Note** SPAN and RSPAN share 7 sessions, SPAN uses 1 to 5, and RSPAN uses 6 and 7.	6 / 7	N/A

UI Setting	Description	Valid Range	Default Value
RSPAN Type	Select the RSPAN type to use for the session. • **Source:** The device will act as an RSPAN source switch. • **Destination**: The device will act as an RSPAN destination switch. If Reflect Port Mode is Enabled, the RSPAN Type will be fixed to Source.	Source / Destination	N/A
Source Type **(If RSPAN Type is Source)**	Select the monitoring source type for the session. **Note** Port Mirroring and VLAN Mirroring cannot be configured at the same time. Only one VLAN Mirroring session can be active at any given time.	Ports / VLANs	Ports
Tx Source Ports **(If RSPAN Type is Source and Source Type is Ports)**	Select the ports you want to monitor for packets being sent out. **Note** The duplication of source port(s) configured in different sessions is not allowed. The duplication of source ports and destination ports in different sessions is not allowed. Source ports must be not be RSPAN VLAN members.	Drop-down list of ports	N/A
Rx Source Ports **(If RSPAN Type is Source and Source Type is Ports)**	Select the ports you want to monitor for packets received. **Note** The duplication of source port(s) configured in different sessions is not allowed. The duplication of source port(s) and destination ports in different sessions is not allowed. Source ports must be not be RSPAN VLAN members.	Drop-down list of ports	N/A
Rx Source VLANs **(If RSPAN Type is Source and Source Type is VLANs)**	Select the VLAN(s) to monitor for data packets being received through them.	Drop-down list of VLANs	N/A

UI Setting	Description	Valid Range	Default Value
RSPAN VLAN ID	Select the VLAN ID to use as the RSPAN VLAN ID. Only existing VLAN IDs can be selected. **Note** Do not use Management VLANs (for Layer 2 switches) or VLAN interfaces (for Layer 3 switches) as RSPAN VLANs to prevent looping. Using dynamically assigned VLANs as RSPAN VLANs is not recommended. The VLAN cannot be duplicated in different RSPAN sessions.	Drop-down list of VLAN IDs	N/A
Reflect Port Mode	Enable or disable Reflect Port Mode. • **Enable**: You can configure a reflect port to mirror packets to destination ports in the source switch. • **Disable**: Packets will be mirrored to the designated port only. If RSPAN Type is Destination, the Reflect Port Mode will be fixed to Disabled.	Enabled / Disabled	N/A
Reflect Port **(If Reflect Port Mode is Enabled)**	Select the port to use as the reflect port for Reflect Port Mode to mirror packets to multiple designated ports. **Note** This port will be specifically reserved for reflect port use; please do not configure it for other uses. The reflect port must be a member of the management VLAN (for Layer 2 switches) or VLAN interfaces (for Layer 3 switches) to prevent looping. Select only Trunk or Hybrid mode VLAN ports to prevent dropping tagged frames. Using dynamically assigned VLANs as PVIDs of reflect ports is not recommended.	Drop-down list of ports	N/A
Designated Port **(If RSPAN Type is Source and Reflect Port Mode is Disabled)**	Select the designated port to use for the session.	Drop-down list of ports	N/A

UI Setting	Description	Valid Range	Default Value
Destination Ports **(If RSPAN Type is Destination)**	Select the destination ports to use for the session.	Drop-down list of ports	N/A

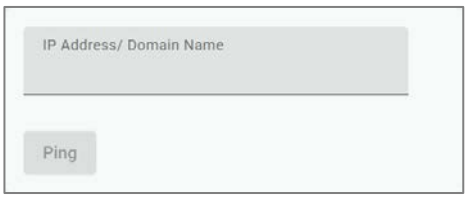
About Ping

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
IP Address/Domain Name	Specify the IP address or domain name you want to ping, then click the **Ping** button to ping the address and display the results.	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

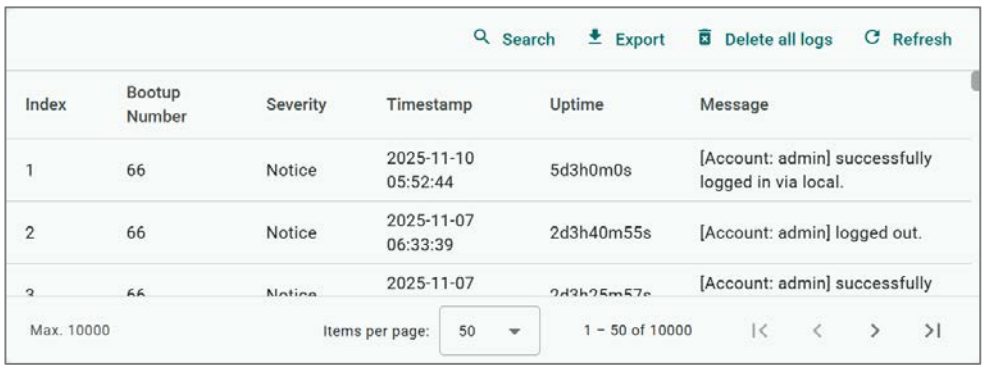
Menu Path: Diagnostics > Event Logs and Notifications > Event Logs - Event Logs

This page lets you view your device's event logs.

Limitations

The system log can record up to 10000 events.

- Click the **Export icon ( )** to export all logs to a file.
- Click the **Delete all logs icon ( )** to delete all logs.
- Click the **Refresh icon ( )** to refresh the logs.



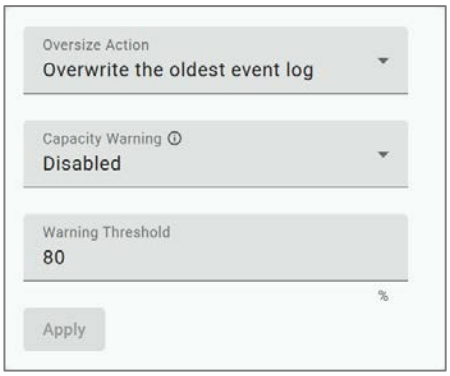
UI Setting	Description
Index	Shows the index of the event.
Bootup Number	Shows the total number of times the device has been powered on. The number increases by 1 every time the device is powered on.
Severity	Shows the severity categorization of the event.
Timestamp	Shows the time of the event, including the date, time, and UTC time zone adjustment.
Uptime	Shows the uptime of the device after it is powered on.
Message	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: **Login Success, Login Fail**, **User Logout**.

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



UI Setting	Description	Valid Range	Default Value
Oversize Action	Select the action to take when the event log reaches its maximum number of entries. • **Overwrite the oldest event log**: New events will overwrite the oldest events. • **Stop recording event logs**: No new events will be recorded. This will also disable port monitoring.	Overwrite the oldest event log / Stop recording event logs	Overwrite the oldest event log
Capacity Warning	Enable or disable capacity warnings. **Note** The registered action can be configured for individual events on the Event Notifications page.	Enabled / Disabled	Disabled
Warning Threshold	Set the warning threshold as a percentage. When **Capacity Warning** is enabled, a warning event log will be triggered when the event log reaches this threshold.	50 to 100	80

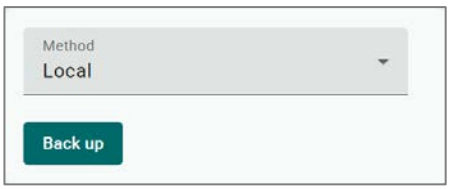
Event Logs - Backup

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.



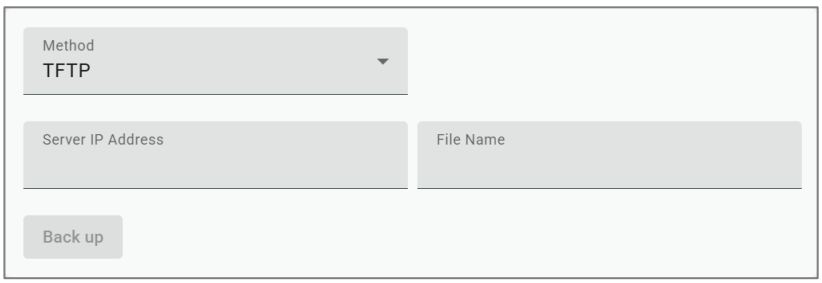
UI Setting	Description	Valid Range	Default Value
Method	Select a method for backing up event logs.	Local / TFTP / SFTP / USB / microSD	Local

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.

Note

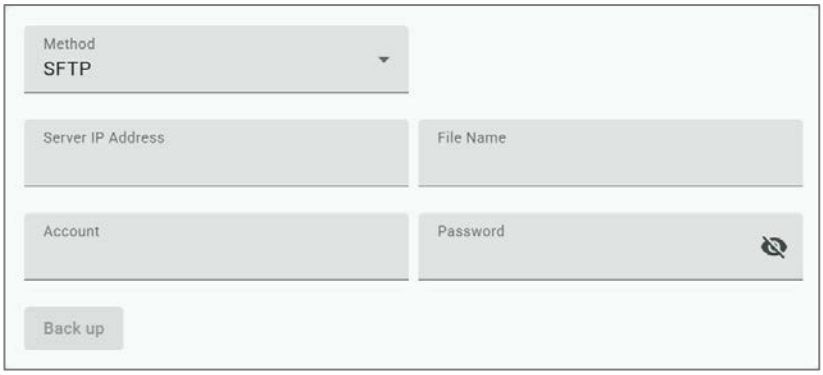
This feature supports weaker authentication or encryption, and may not be secure over untrusted networks. Take appropriate security precautions.



UI Setting	Description	Valid Range	Default Value
Method	Select a method for backing up event logs.	Local / TFTP / SFTP / USB / microSD	Local
Server IP Address	Specify the IP address of the TFTP server to upload the event logs to.	Valid IP address	N/A
File Name	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.

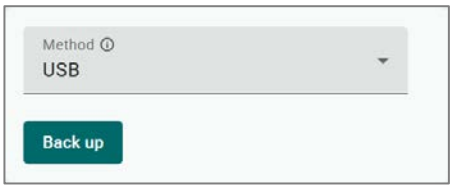


UI Setting	Description	Valid Range	Default Value
Method	Select a method for backing up event logs.	Local / TFTP / SFTP / USB / microSD	Local
Server IP Address	Specify the IP address of the SFTP server to upload the event logs to.	Valid IP address	N/A
File Name	Specify a file name to use for the event logs file.	File name can only contain A-Z, a-z, 0-9 or the symbols -._().	N/A
Account	Enter the SFTP server account name to use to connect to the SFTP server.	N/A	N/A
Password	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.

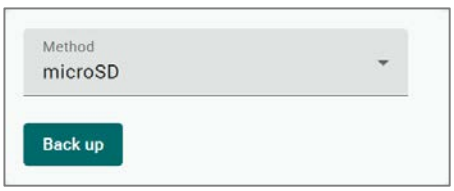


UI Setting	Description	Valid Range	Default Value
Method	Select a method for backing up event logs.	Local / TFTP / SFTP / USB / microSD	Local

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
Method	Select a method for backing up event logs.	Local / TFTP / SFTP / USB / microSD	Local

Auto Event Log Backup

When **Automatically Back Up** is enabled, when the event log is full, the oldest 1000 event logs will be backed up to an inserted ABC-02 configuration tool or microSD card and then deleted from the device to make space for new logs.

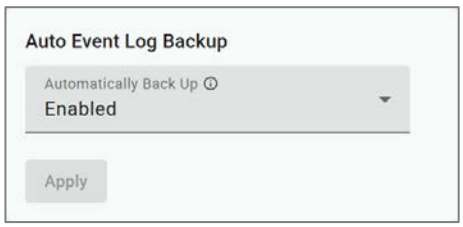
Note

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
Automatically Back Up	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:

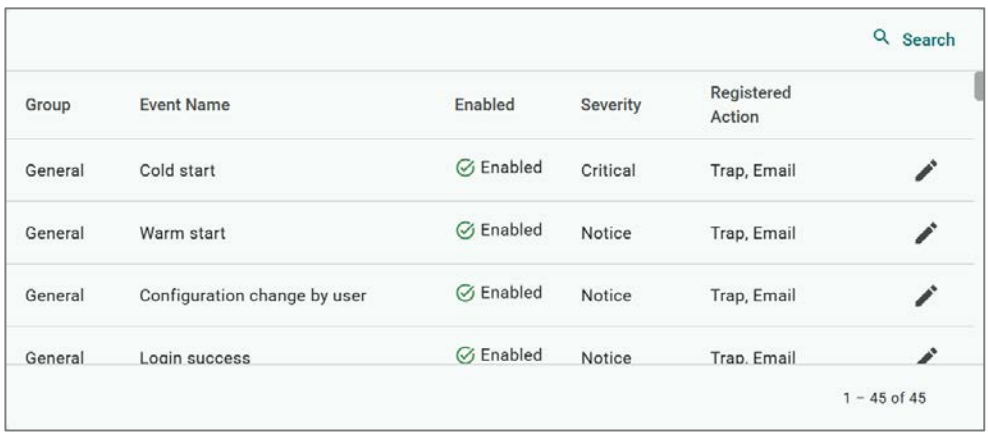
- System and Functions
- Port

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



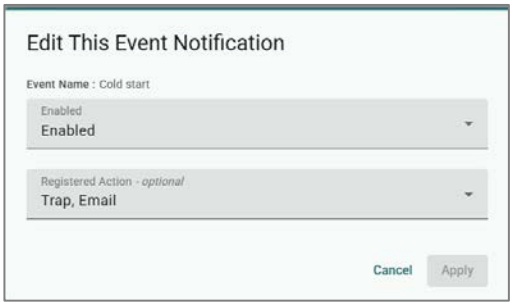
UI Setting	Description
Group	Shows which group this event belongs to.
Event Name	Shows the name of the event. Refer to Event Log Descriptions for more details.
Enabled	Shows whether event notifications are enabled for this kind of event.
Severity	Shows the severity assigned to the event. Refer to the Severity Level List for more details.
Registered Action	Shows which action will be taken for this kind of event. • **Trap**: A notification is sent to the Trap server when the event is triggered. • **Email**: A notification is sent to the email server defined in the Email Settings section. **Note** This feature supports weaker authentication or encryption, and may not be secure over untrusted networks. Take appropriate security precautions. • **Relay**: A notification is sent through the relay interface, if the device has one, when the event is triggered. **Note** The types of actions available may vary depending on the event type and the device model.

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.



UI Setting	Description	Valid Range	Default Value
Event Name (View-only)	Shows the name of the event. Refer to Event Log Descriptions for more information.	(Fixed)	(Fixed)
Enabled	Enable or disable notifications for this event.	Enabled / Disabled	Enabled
Registered Action	Select which actions to take when the event occurs. Multiple actions may be selected. • **Trap**: A notification will be sent to the Trap server. • **Email**: A notification email will be sent to the email server defined in the Email Settings section. • **Relay**: An alarm notification will be triggered through the relay output of the device, if your device is equipped with one.	Trap / Email / Relay	Trap, Email

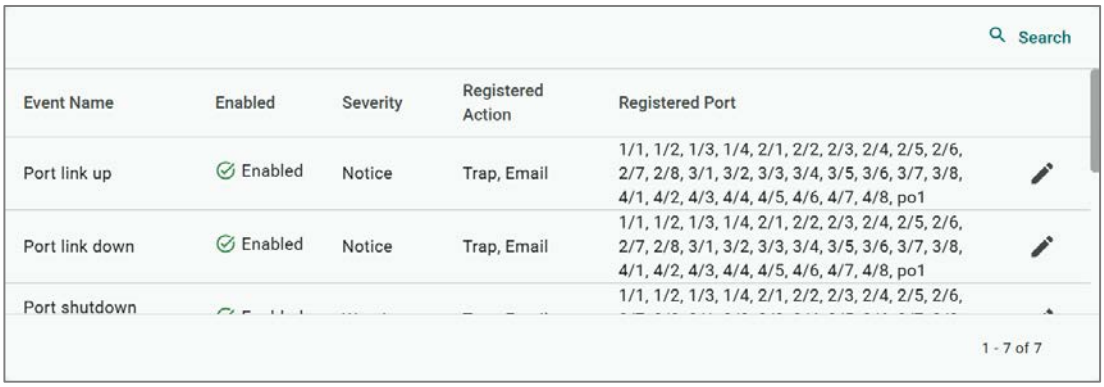
Event Notifications - Port

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.

Port Event List



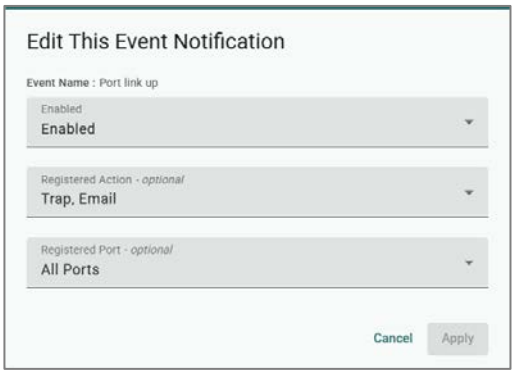
UI Setting	Description
Event Name	Shows the name of the port event.
Enabled	Shows whether event notifications are enabled for this kind of event.
Severity	Shows the severity assigned to the event. Refer to the Severity Level List for more details.
Registered Action	Shows which action will be taken for this kind of event. **Trap**: A notification is sent to the Trap server when the event is triggered. **Email**: A notification is sent to the email server defined in the Email Settings section. **Syslog**: An event log is recorded to the Syslog server defined in the Syslog section. **Relay:** A notification is sent through the relay interface, if the device has one, when the event is triggered.
Registered Port	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.



UI Setting	Description	Valid Range	Default Value
Event Name (View-only)	Shows the name of the port event.	(Fixed)	(Fixed)
Enabled	Enable or disable notifications for this event.	Enabled / Disabled	Enabled
Registered Action	Select which actions to take when the event occurs. Multiple actions may be selected. • **Trap**: A notification will be sent to the Trap server. • **Email**: A notification email will be sent to the email server defined in the Email Settings section. • **Relay**: An alarm notification will be triggered through the relay output of the device, if your device is equipped with one.	Trap / Email / Relay	Trap, Email
Registered Port	Specify the ports that will use the registered action.	Drop-down list of ports	All Ports

About 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 Formats

This device supports different syslog formats.

RFC 3164

Also known as BSD syslog format, RFC 3164 syslog messages contain information to form a header followed by a message:

`<PRIORITY>TIMESTAMP HOSTNAME TAGS: MESSAGE`

PRIORITY	Indicates the syslog priority of the event.
TIMESTAMP	Indicates the date and time of the event. The following date format is used: `Mmm dd hh:mm:ss`
HOSTNAME	Indicates the host device that originally sent the syslog message.
TAGS	Additional information tags about the event. This device uses: `CLASSIFICATION: [boot=COUNT][uptime=VALUE]` Moxa devices use the classification of the relevant feature, according to the device's web UI.
MESSAGE	The event message, which may be in legacy or CEF message format. Refer to Message Formats for more information.

Example RFC 3164 message using legacy message format:

```
<156> Jan  8 23:58:37 moxa Redundancy: [boot=3079][uptime=21d22h4m40s]
Topology change detected on Ring 1 of Turbo Ring v2.
```

Example RFC 3164 message using CEF message format:

```
<156> Jan  8 23:59:13 moxa CEF:0|MOXA|TN-4520B-12P-4GP-4GBP-T|v2.0 Build
2025_0917_1811|1073742862|Topology change (Turbo Ring)|5|dvchost=moxa
dvc=192.168.127.106 index=1
```

RFC 5424

RFC 5424 defines an updated syslog format that includes additional fields:

<PRIORITY>VERSION TIMESTAMP HOSTNAME APP-NAME PROCID MSGID STRUCTURED-DATA MESSAGE

PRIORITY	Indicates the syslog priority of the event.
VERSION	Indicates the syslog protocol specification version used for the syslog message.
TIMESTAMP	Indicates the date and time of the event. ISO-8601 date format is used.
HOSTNAME	Indicates the host device that originally sent the syslog message.
APP-NAME	Indicates the device or application that originated the message. Moxa devices use the classification of the relevant feature, according to the device's web UI.
PROCID	This device does not use this field, so a - is used as a placeholder.
MSGID	Indicates the ID of the message type. Refer to Event Log Descriptions for the event IDs used by this device.
STRUCTURED-DATA	This device does not use this field, so a - is used as a placeholder.
MESSAGE	The event message, which may be in legacy or CEF message format. Refer to Message Formats for more information.

Example RFC 5424 message using legacy message format:

<156>1 2026-01-09T01:23:24+00:00 moxa Redundancy - 1073742862 - Topology change detected on Ring 1 of Turbo Ring v2.

Example RFC 5424 message using CEF message format:

<156>1 2026-01-09T01:23:49+00:00 moxa Redundancy - 1073742862 - CEF:0|MOXA|TN-4520B-12P-4GP-4GBP-T|v2.0 Build 2025_0917_1811|1073742862|Topology change (Turbo Ring)|5|dvchost=moxa dvc=192.168.127.106 index=1

Message Formats

This device supports both legacy and CEF message formats for syslog logging.

Refer to Event Log Descriptions for more details on messages used for specific events.

Legacy Message Format

The legacy message format uses a simple event description.

Example legacy message:

```
Topology change detected on Ring 1 of Turbo Ring v2
```

CEF Message Format

The Common Event Format (CEF) is a standardized, text-based format for logging security-related events from various sources. Built on the syslog format, CEF provides a structured and consistent way to log events, making it a crucial component for effective security information and event management (SIEM) solutions.

By using a standardized logging format, CEF simplifies managing and analyzing security logs, making it easier to:

- Collect and aggregate log data from diverse systems and applications
- Analyze and troubleshoot issues efficiently
- Automate the analysis of logs to reduce manual effort
- Identify security threats, patterns, and trends across the network

Example CEF message:

```
CEF:0|Moxa|RKS-G4028-L3-4GS-HV-T|v6.0 Build 2025_1201_1045|0x4000040e|Topology change (Turbo Ring)|5|index=1
```

Refer to CEF Message Format for Event Logs for more information.

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

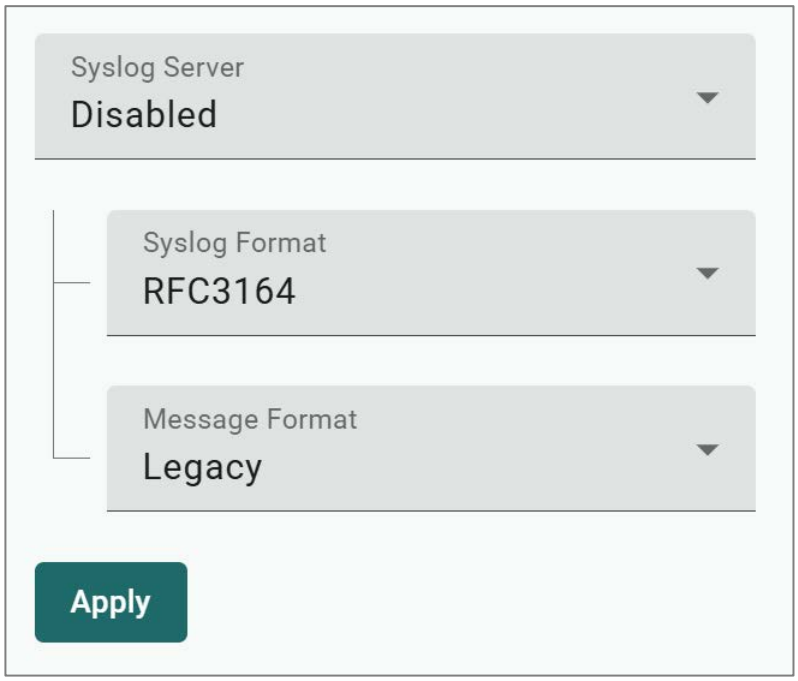
Menu Path: Diagnostics > Event Logs and Notifications > Syslog - General

This page lets you configure the Syslog server settings.

Syslog Settings

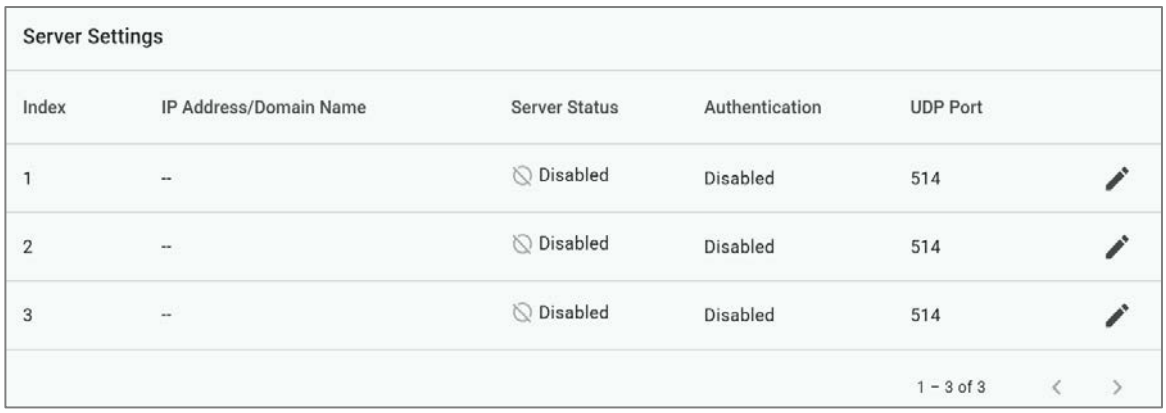
Note

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.



UI Setting	Description	Valid Range	Default Value
Syslog	Enable or disable syslog logging for your device.	Enabled / Disabled	Disabled
Syslog Format	Specify the syslog format to use.	RFC3164 / RFC5424	RFC3164
Message Format	Specify the message format to use.	Legacy / CEF (Common Event Format)	Legacy

Syslog Server Settings List



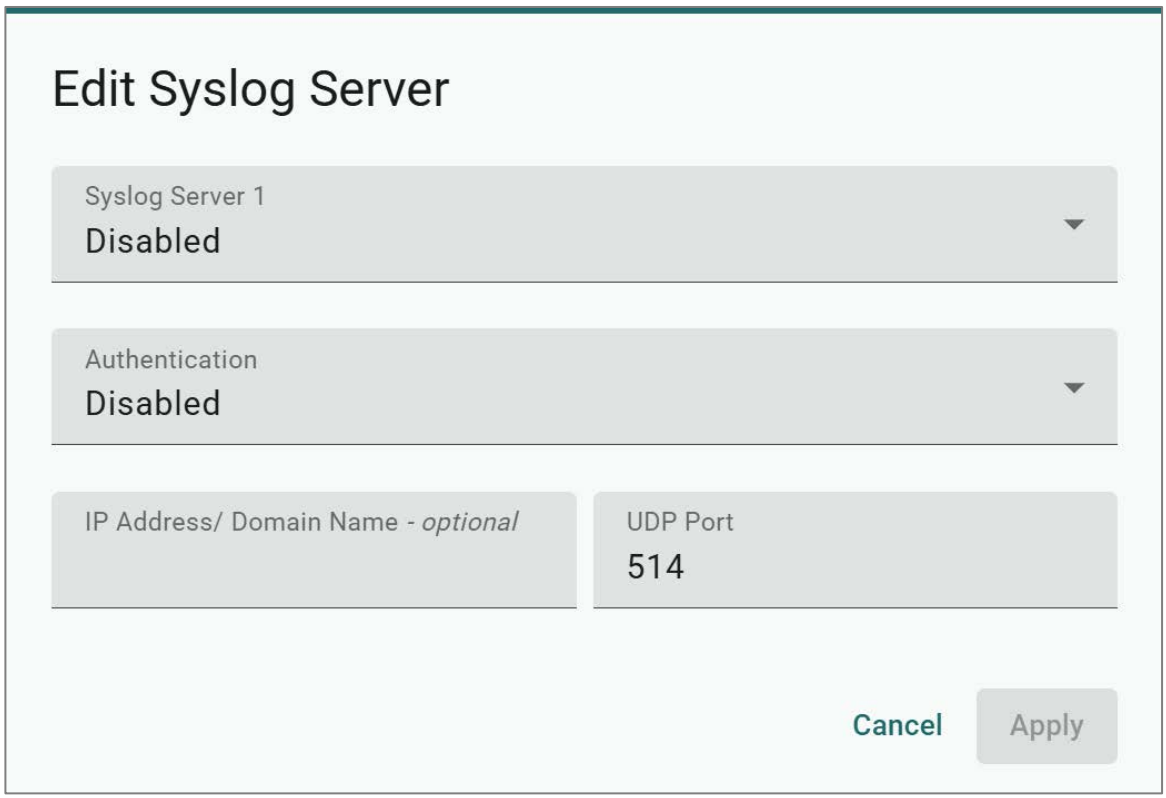
UI Setting	Description
Index	Shows the index of the syslog server.
IP Address/Domain Name	Shows the IP address or domain name of the syslog server.
Server Status	Shows whether the syslog server is enabled.
Authentication	Shows whether authentication via TLS is enabled for the syslog server.
UDP Port	Shows the UDP port of the syslog server.

Editing a Syslog Server

Menu Path: Diagnostics > Event Logs and Notifications > Syslog - General

This page lets you edit the syslog server settings.

Click **Apply** to save your changes.



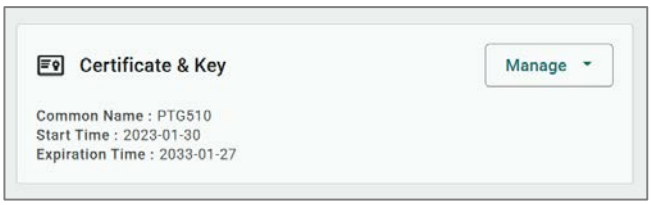
UI Setting	Description	Valid Range	Default Value
Syslog Server 1/2/3	Enable or disable the specified syslog server.	Enabled / Disabled	Disabled
Authentication	Select whether to authenticate via TLS or disable authentication. **Note** To enable TLS, a certificate and key set must be created first on the "Authentication" tab.	Disabled / TLS	Disabled
IP Address/ Domain Name	Enter the IP address or domain name of the related syslog server.	Valid IP address or domain name	N/A
UDP Port	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.





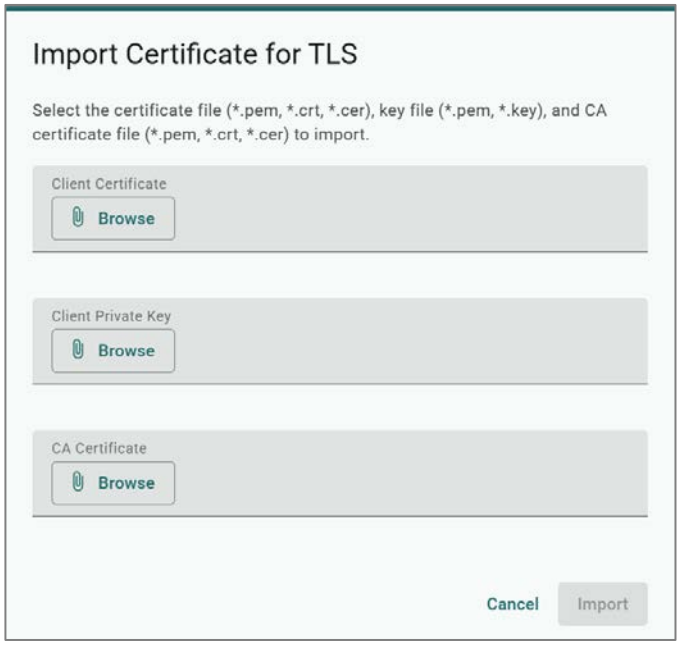
UI Setting	Description
Common Name	Shows the name of the imported certificate and keys.
Start Time	Shows the start time of the imported certificate and keys.
Expiration Time	Shows the expiration time of the imported certificate and keys.

Adding a Syslog Certificate and Key Set

Menu Path: Diagnostics > Event Logs and Notifications > Syslog - Authentication

To import a client certificate and key for syslog authentication over TLS, click **Manage** on the **Diagnostics > Event Logs and Notifications > Syslog - Authentication** page and select **Import Certificate**. This dialog will let you import a TLS certificate and its related keys.

Click **Import** to save your changes.



UI Setting	Description	Valid Range	Default Value
Client Certificate	Click the **Browse** button and select a client certificate file from your computer to import.	N/A	N/A
Client Private Key	Click the **Browse** button and select a client private key file from your computer to import.	N/A	N/A
CA Certificate	Click the **Browse** button 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.

Note

This feature supports weaker authentication or encryption, and may not be secure over untrusted networks. Take appropriate security precautions.

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.

Limitations

You can configure up to 2 SNMP trap/inform recipients.

SNMP Trap / Inform Recipients



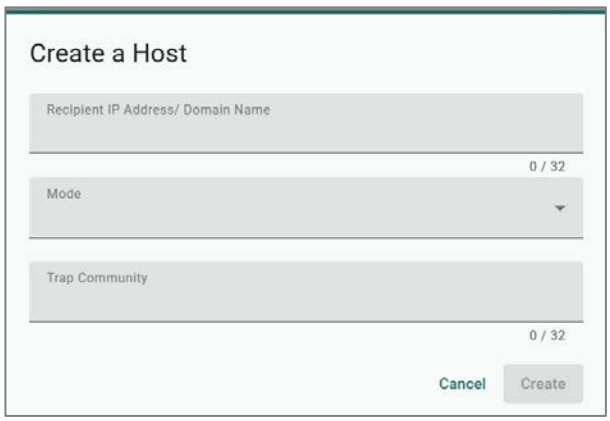
UI Setting	Description
Recipient IP Address/ Domain Name	Shows the IP address or domain name of the recipient trap server that will receive notifications.
Mode	Shows the mode used for SNMP notifications.
Trap Community	Shows the community string used for authentication.

Creating an SNMP Trap/Inform Host

Menu Path: Diagnostics > Event Logs and Notifications > SNMP Trap/Inform - General

Clicking the **Create** 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.



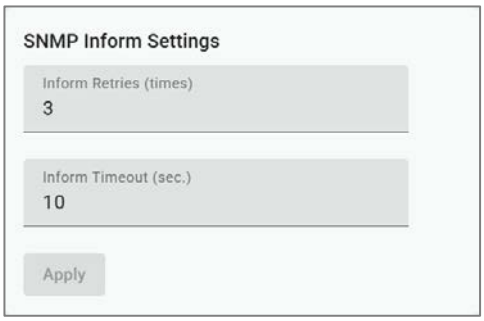
UI Setting	Description	Valid Range	Default Value
Recipient IP Address/ Domain Name	Specify the IP address or the name of the recipient trap server that will receive notifications.	Valid IP address or domain name, 0 to 32 characters	N/A

UI Setting	Description	Valid Range	Default Value
Mode	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. • **Trap V1**: Use Trap V1 for SNMP notifications. • **Trap V2c**: Use Trap V2 for SNMP notifications. • **Inform V2c**: Use Inform V2 for SNMP notifications. • **Trap V3**: Use Trap V3 for SNMP notifications. • **Inform V3**: Use Inform V3 for SNMP notifications.	Trap V1 / Trap V2 / Inform V2 / Trap V3 / Inform V3	N/A
Trap Community	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
Inform Retries	Specify the number of times to retry sending an inform notification.	1 to 99	3
Inform Timeout	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/inform account.



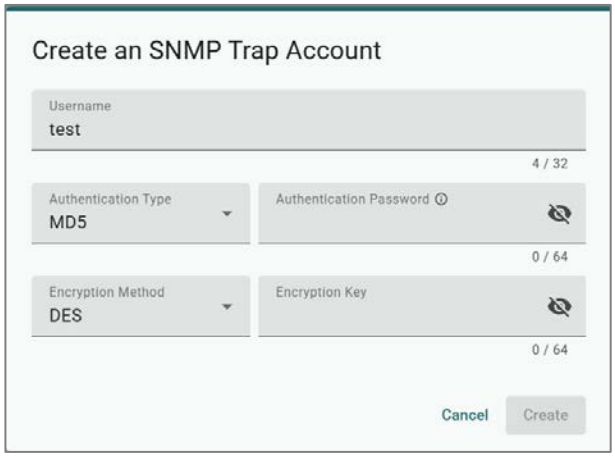
UI Setting	Description
Username	Shows the username for the SNMP trap account.
Authentication Type	Shows which authentication method is used for the account.
Encryption Method	Shows which encryption method is used for the account.

Creating an SNMP Trap Account

Menu Path: Diagnostics > Event Logs and Notifications > SNMP Trap / Inform - SNMP Trap / Inform Accounts

Clicking the **Create** 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.



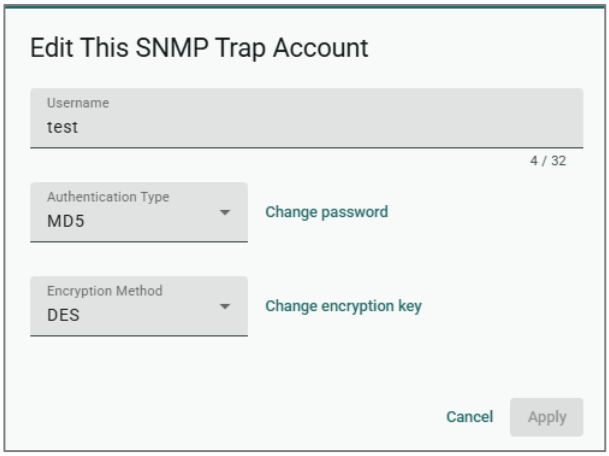
UI Setting	Description	Valid Range	Default Value
Username	Specify a username for the SNMP trap account.	4 to 32 characters	N/A
Authentication Type	Select which authentication method to use for the account.	None / MD5 / SHA / SHA-256 / SHA-512	None
Authentication Key **(if Authentication Type is not None)**	Specify an authentication key to use for the account.	8 to 64 characters	N/A
Encryption Method	Disable encryption or select which encryption method to use for the account.	Disabled / DES / AES	Disabled
Encryption Key **(if Encryption Method is not Disabled)**	Specify an encryption password for the account.	8 to 64 characters	N/A

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.



UI Setting	Description	Valid Range	Default Value
Username	Specify a username for the SNMP trap account.	4 to 32 characters	N/A
Authentication Type	Select which authentication method to use for the account. Click **Change password** to specify a new authentication password for the account.	None / MD5 / SHA / SHA-256 / SHA-512	None
Encryption Method	Disable encryption or select which encryption method to use for the account. Click **Change encryption key** to specify a new encryption key for the account.	Disabled / DES / AES	Disabled

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.

About Email Settings

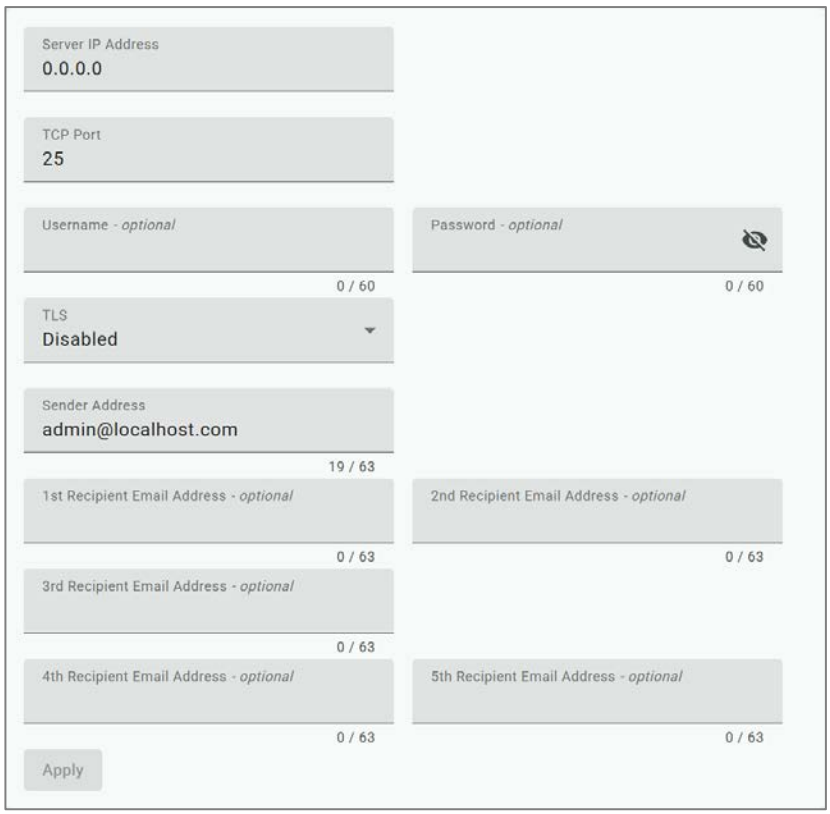
Email Settings lets you configure email notifications for important events. This lets you receive alerts directly in your inbox, providing a convenient way to stay informed about critical network issues.

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.



UI Setting	Description	Valid Range	Default Value
Server IP Address	Specify the IP address of the email server.	Valid IP address	N/A
TCP Port	Specify the TCP port of the email server.	1 to 65535	25
Username	Specify the username used to log in to the email server.	0 to 60 characters	N/A
Password	Specify the password used to log in to the email server.	0 to 60 characters	N/A

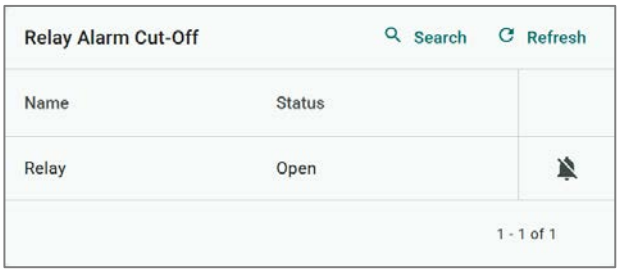
UI Setting	Description	Valid Range	Default Value
TLS	Enable or disable TLS (Transport Layer Security).	Enabled / Disabled	Disabled
Sender Address	Specify the sender email address to use for email notifications.	Valid email address up to 63 characters	N/A
1st / 2nd / 3rd / 4th / 5th Recipient Email Address	Enter an email address to send email notifications to. You can set up to 5 email addresses to send email notifications to.	Valid email address up to 63 characters	N/A

Relay Alarm

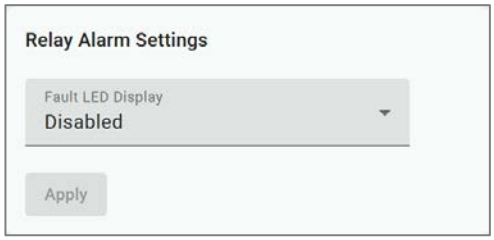
Menu Path: Diagnostics > Event Logs and Notifications > Relay Alarm

This page lets you see the status of the relay alarm and configure related settings.

Relay Alarm Cut-Off Status



UI Setting	Description
Name	Shows the name of the relay.
Status	Shows whether the relay is currently open or closed.



UI Setting	Description	Valid Range	Default Value
Fault LED Display	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 User Accounts for more information on user accounts.

Settings	Admin	Supervisor	User
IEC 61850			
MMS	R/W	R/W	R
GOOSE Check	R/W	R/W	R
Modbus TCP	R/W	R/W	R
EtherNet/IP	R/W	R/W	R
PROFINET	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.

> **Note**
>
> This feature supports weaker authentication or encryption, and may not be secure over untrusted networks. Take appropriate security precautions.

Connecting With an MMS Server

To connect with an MMS server, the following key parameters need to be set:

1. **IP Address and Port**
    a. **IP Address**: The network address of the MMS server.
    b. **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. 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. 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:
    a. **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
Remote P Selector	No limitation
Remote S Selector	1
Remote T Selector	No limitation
Local P Selector	1
Local S Selector	1
Local T Selector	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.

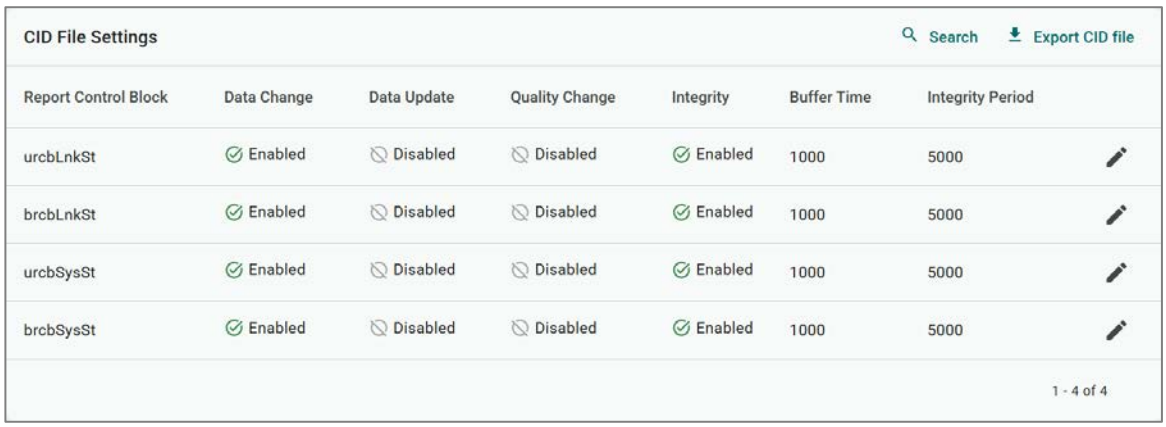
MMS Settings



UI Setting	Description	Valid Range	Default Value
MMS	Enable or disable the MMS server for your device.	Enabled / Disabled	Disabled
IED Name	Specify the IED name for your device.	1 to 48 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.



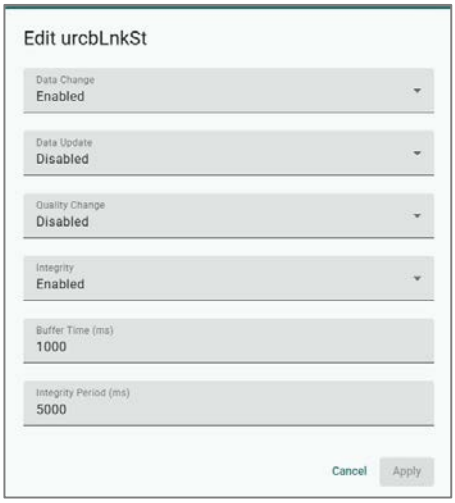
UI Setting	Description
Report Control Block	Shows which report control block the entry is for. • **urcbLnkSt:** Unbuffered Report Control Block Link Status • **brcbLnkSt:** Buffered Report Control Block Link Status • **urcbSysSt:** Unbuffered Report Control Block System Status • **brcnSysSt:** Buffered Report Control Block System Status
Data Change	Shows whether report generation is enabled for data change (dchg) events.
Data Update	Shows whether report generation is enabled for data update (dupd) events.
Quality Change	Shows whether report generation is enabled for quality change (qchg) events.
Integrity	Shows whether integrity report generation is enabled for the report control block.
Buffer Time	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.
Integrity Period	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.



UI Setting	Description	Valid Range	Default Value
Data Change	Enable or disable report generation when there is a data change event. A data change (dhcg) relates to a change in a value of a data attribute.	Enabled / Disabled	Enabled
Data Update	Enable or disable report generation when there is a data update event. 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.	Enabled / Disabled	Disabled
Quality Change	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
Integrity	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 **Integrity Period**) generate a report with the values of all members of the referenced data set.	Enabled / Disabled	Enabled
Buffer Time	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
Integrity Period	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



UI Setting	Description
CA Name	Shows the name of the CA for the T-Profile certificate.
Expiration Date	Shows when the T-Profile certificate will expire. The date format is YYYY-MM-DD hh:mm:ss (year, month, date, hour, minute, second).

Edit T-Profile Security

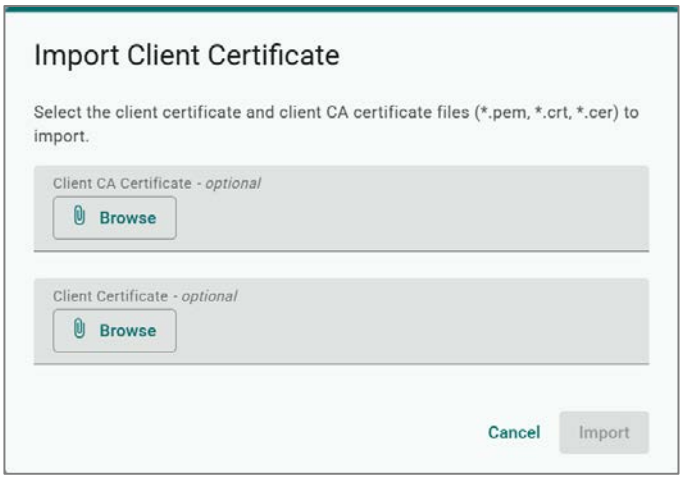
If you click on **Manage > Edit T-Profile Security** for **T-Profile Certificate**, this dialog will appear.



UI Setting	Description	Valid Range	Default Value
T-Profile Security	Enable or disable T-Profile security for the device.	Enabled / Disabled	Disabled

T-Profile - Import Client Certificate

If you click on **Manage > Import Client Certificate** for **T-Profile Certificate**, this dialog will appear.



UI Setting	Description	Valid Range	Default Value
Client CA Certificate	Click the **Browse** button and select a client CA certificate file from your computer to import.	N/A	N/A
Client Certificate	Click the **Browse** button and select a client certificate file from your computer to import.	N/A	N/A

A-Profile Certificate Information



UI Setting	Description
CA Name	Shows the name of the CA for the A-Profile certificate.
Expiration Date	Shows when the A-Profile certificate will expire. The date format is YYYY-MM-DD hh:mm:ss (year, month, date, hour, minute, second).

Edit A-Profile Security

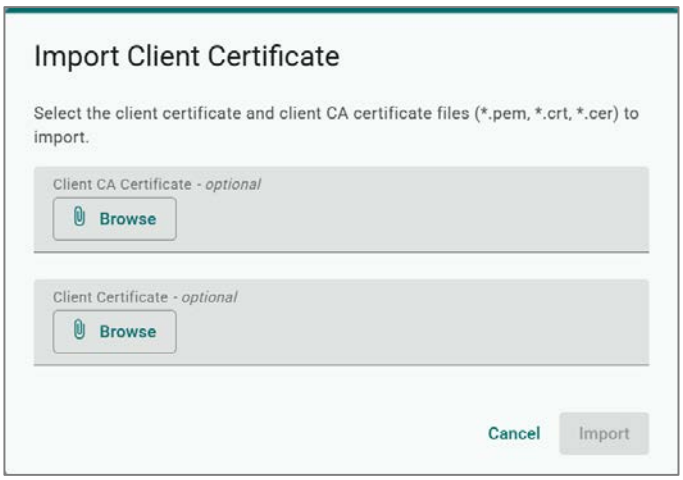
If you click on **Manage > Edit A-Profile Security** for **A-Profile Certificate**, this dialog will appear.



UI Setting	Description	Valid Range	Default Value
A-Profile Security	Enable or disable A-Profile security for the device.	Enabled / Disabled	Disabled

A-Profile - Import Client Certificate

If you click on **Manage > Import Client Certificate** for **A-Profile Certificate**, this dialog will appear.



UI Setting	Description	Valid Range	Default Value
Client CA Certificate	Click the **Browse** button and select a client CA certificate file from your computer to import.	N/A	N/A
Client Certificate	Click the **Browse** button and select a client certificate file from your computer to import.	N/A	N/A

About GOOSE Check

GOOSE Check is a proprietary Moxa feature, which detects tampering in GOOSE packets and optionally takes action on detection.

GOOSE (Generic Object Oriented Substation Event) messaging is a method for high-speed, event-driven communication between Intelligent Electronic Devices (IEDs) in a substation. These messages are used to transmit critical data like protection trips, status changes, and control commands with minimal delay.

GOOSE communication failures are traditionally difficult for engineers to troubleshoot over Ethernet.

To facilitate troubleshooting and increase security, the feature checks for two types of tampering:

- Port Tampering: GOOSE Packets with the same **GOOSE Address (DA)** (Destination Address) and **APPID**, but different source ports
- Source Address (SA) Tampering: GOOSE Packets with the same **GOOSE Address (DA)** and **APPID**, but different MAC Source Addresses (MAC SA)

Where both port and source address tampering are detected, packets are treated as port-tampered.

When **GOOSE Check** is enabled, anomalies are saved in the event log, and may trigger other user-specified actions, such as dropping packets or disabling the port that delivers the packets. Disabled ports may be reactivated manually.

GOOSE Check uses monitoring entries to validate GOOSE packets. Entries come from two sources:

- Static Entries: User-specified entries under the **Settings** tab. Static entries are visible in both the **Settings** and **Status** tabs
- Dynamically: When **GOOSE Lock** is disabled, the device automatically populates the list based on received packets. Dynamic entries are shown in the **Status** tab only. Dynamic learning considers the first set of values received for any given entry to be genuine.

Static entries still employ dynamic learning to learn **Ingress Port** and MAC Source Addresses (MAC SA). Learned **Ingress Port** entries are shown in the **Status** tab, while MAC Source Addresses (MAC SA) are not visible in the UI.

GOOSE Lock

GOOSE Lock is a feature that operates in addition to **GOOSE Check**, and uses an allowlist paradigm to create a tamper-evident digital seal. GOOSE packets not on the allow list trigger **Lock Violation: Warning** on the **Status** tab. This warning persists until the device is rebooted or the feature is reset. Specifically, the allowlist uses the following entry fields from the **Status** tab:

- **APPID**
- **GOOSE Address (DA)**

GOOSE packets not matching the above fields will trigger **Lock Violation: Warning** under the **Status** tab when **GOOSE Lock** is enabled. All elements must correspond to single entry, and cannot be mixed between entries.

Enabling **GOOSE Lock** freezes dynamic learning.

Important: Dynamic learning recommended before enabling **GOOSE Lock** to avoid excessive logging and possible interruptions.

Since **Ingress Port** can only be learned dynamically—even for Static Entries—enabling **GOOSE Lock** without prior dynamic learning will cause **GOOSE Check** to register all GOOSE packets as port-tampered. Without prior dynamic learning, choosing a GOOSE Check **Tamper Response** other **No Action** will result in blocking all GOOSE Packets and possibly disabling the ports. Choosing **No Action** will result in logging activity.

To avoid this, a period of dynamic learning should be permitted before enabling **GOOSE Lock**. During the dynamic learning period, monitor the **Status** tab carefully to ensure correct population of the monitoring table.

Configuring GOOSE Check

Verify GOOSE packets and take action on packets suspected of tampering.

Users planning to use GOOSE Lock should make sure that there are active GOOSE packets on the network to populate the monitoring table through dynamic learning. GOOSE Lock freezes dynamic learning, and enabling the feature prematurely may cause unwanted blocking behavior.

1. Sign in to the device with administrator credentials.
2. Go to **Industrial Application** > **IEC 61850** > **GOOSE Check**, and then click **Settings**.

3. Under **GOOSE Check**, choose **Enabled** from the drop down.

GOOSE Lock and **Tamper Response** appear.

4. Configure the following options:

Option	Values
GOOSE Lock	• **Disabled**: Allows continuous dynamic learning in addition to static entries. • **Enabled**: Freezes dynamic learning. Compares GOOSE Packets to **APPID** and **GOOSE Address (DA)** fields on the **Status** tab table. GOOSE packets not corresponding to a monitoring table entry will trigger **Lock Violation: Warning**, visible from **Status**.
Tamper Response	• **No Action**: Suspected tampering logged, no further action taken. • **Drop**: Drops packets suspected of tampering. • **Port Disable**: Disables ports transmitting packets suspected of tampering.

Note

Important: Dynamic learning recommended before enabling GOOSE Lock to avoid excessive logging and possible interruptions.

Since Ingress Port can only be learned dynamically—even for Static Entries—enabling GOOSE Lock without prior dynamic learning will cause GOOSE Check to register all GOOSE packets as port-tampered. Without prior dynamic learning, choosing a GOOSE Check Tamper Response other No Action will result in blocking all GOOSE Packets and possibly disabling the ports. Choosing No Action will result in logging activity.

To avoid this, a period of dynamic learning should be permitted before enabling GOOSE Lock. During the dynamic learning period, monitor the Status tab carefully to ensure correct population of the monitoring table.

5. Before continuing. click **Apply** to save your settings.

6. To add static entries to the Monitoring table, click ***[Add]***.

The Create Static GOOSE Entry screen appears.

7. Specify an **APP ID** in hex and a **GOOSE Address (DA)**, and then click **Apply**.

GOOSE Address (DA) prefills the first four octets `01:0C:CD:01:`, requiring two octets.

Note

GOOSE Check detects tampering by checking entries against learned Source Port and Source Address - which manual entries cannot specify. If used in conjunction with GOOSE Lock, a period of dynamic learning should be permitted before enabling GOOSE Lock to ensure proper functionality.

GOOSE packets not matching both parameters will trigger **Tamper Response** actions.

8. **Optional:** Continue to add entries until the table matches your network requirements.

- To check the current state of GOOSE Check packets, go to **Industrial Application** > **IEC 61850** > **GOOSE Check** and then click **Status**.
- To re-enable ports disabled by **Tamper Response Port Disable**, go to **Port** > **Port Interface** > **Port Settings**, click ***[Edit]*** corresponding to the disabled port, and then set **Admin** to **Enabled**. Click **Apply** to save your changes.

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

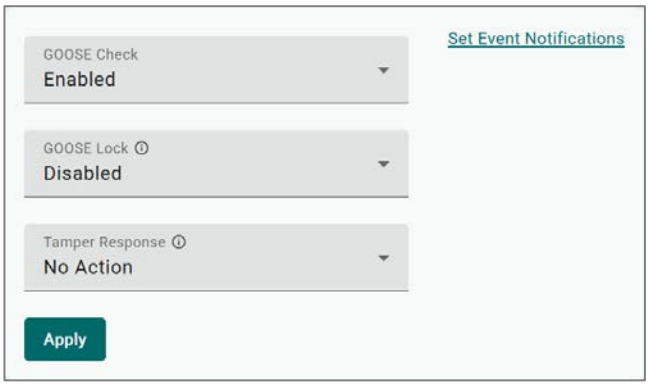
Menu Path: Industrial Application > IEC 61850 > GOOSE Check - Settings

This page lets you configure GOOSE check for your device.

Limitations

You can create up to 100 GOOSE monitoring entries.

GOOSE Check Settings



UI Setting	Description	Valid Range	Default Value
GOOSE Check	Enable or disable **GOOSE Check** on the device.	Enabled / Disabled	Disabled
GOOSE Lock **(If GOOSE Check is Enabled)**	Enable or disable **GOOSE Lock**. When enabled, packets that are not shown in the monitoring table will be dropped.	Enabled / Disabled	Disabled
Tampered Response **(If GOOSE Check is Enabled)**	Select the action to take if a GOOSE check detects tampering. • **No Action:** No action will be taken for tampered packets, but an event will still be recorded. • **Drop:** All tampered packets will be dropped. Other traffic will be handled normally. • **Port Disable:** The relevant port will be disabled.	No Action / Drop / Port Disable	No Action

GOOSE Check Monitoring List



UI Setting	Description
APP ID	Shows the GOOSE application identifier for the GOOSE message.
GOOSE Address (DA)	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 **Create** 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.



UI Setting	Description	Valid Range	Default Value
APP ID	Specify the application identifier for the GOOSE message.	Hex values from 0000 to ffff	N/A
GOOSE Address (DA)	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



UI Setting	Description
GOOSE Lock Status	Shows whether GOOSE lock is enabled.
Lock Violation Status	Shows the current GOOSE lock violation status. This status is automatically refreshed every 5 minutes. • **Normal:** All detected GOOSE packets are shown in the monitoring table. • **Warning**: Unexpected GOOSE packets were detected that are not be shown in the monitoring table.

GOOSE Message List



UI Setting	Description
Type	Shows the type of the ingress GOOSE message. • **Static:** The GOOSE message is defined on this device. • **Dynamic:** The GOOSE message is learned from GOOSE packets.
APP ID	Shows the application identifier of the ingress GOOSE message.
GOOSE Address (DA)	Shows the destination MAC address of the ingress GOOSE message.
GoCB Name	Shows the IED name and GOOSE control block name of ingress GOOSE packets.
VLAN ID	Shows the VLAN ID of the ingress GOOSE message.
Ingress Port	Shows the ingress port of the GOOSE message.
Rx Counter	Shows the packet counter of the ingress GOOSE message.
Status	Shows the communication status of the GOOSE message. • **Healthy**: The communication status is normal. • **Timeout**: The communication status is abnormal. This GOOSE message did not pass through the device at the correct time. • **Tampered**: 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.

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.

Note

This feature supports weaker authentication or encryption, and may not be secure over untrusted networks. Take appropriate security precautions.

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
Word access (16-bit access)	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.



UI Setting	Description	Valid Range	Default Value
Modbus TCP	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.

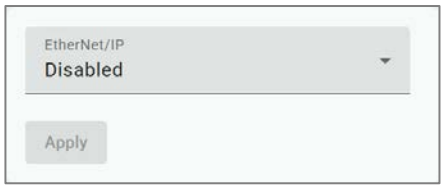
Note

This feature supports weaker authentication or encryption, and may not be secure over untrusted networks. Take appropriate security precautions.

EtherNet/IP

Menu Path: Industrial Application > EtherNet/IP

This page lets you enable EtherNet/IP functionality for your device.



UI Setting	Description	Valid Range	Default Value
EtherNet/IP	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.

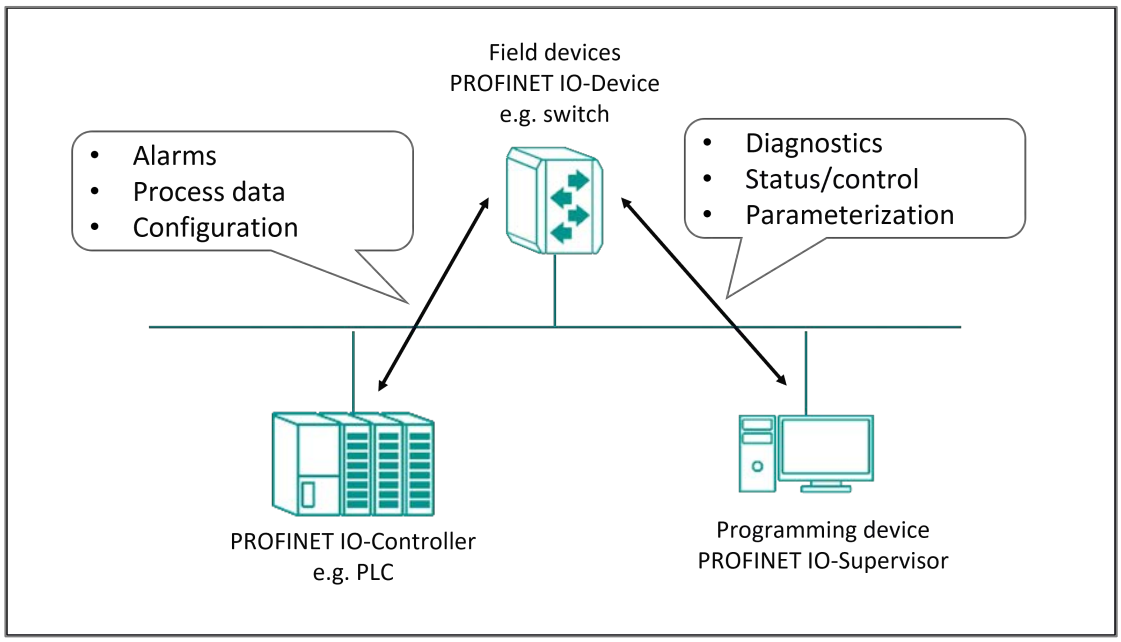
Note

This feature supports weaker authentication or encryption, and may not be secure over untrusted networks. Take appropriate security precautions.

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.

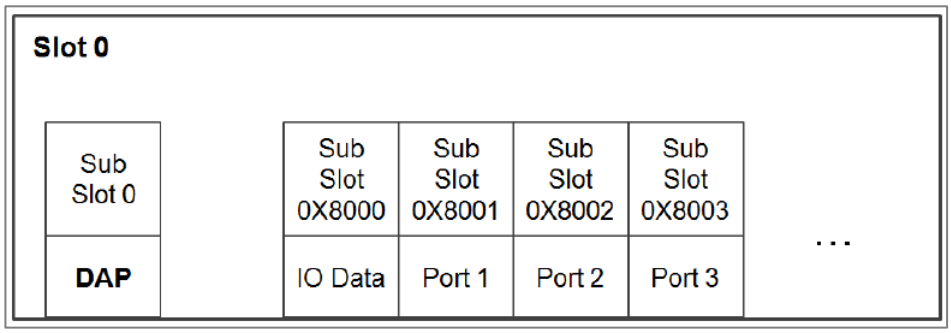
IO-Devices are standalone units designed to transmit real-time (RT) information to IO-Controllers (PLCs). They do not attempt to communicate directly with other devices. Instead, they directly provide their real-time (cyclic) data to an IO-Controller and may send some alarm or diagnostic (acyclic) data 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.



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
Device	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
Device	Input	1	Reserved for redundancy protocol		

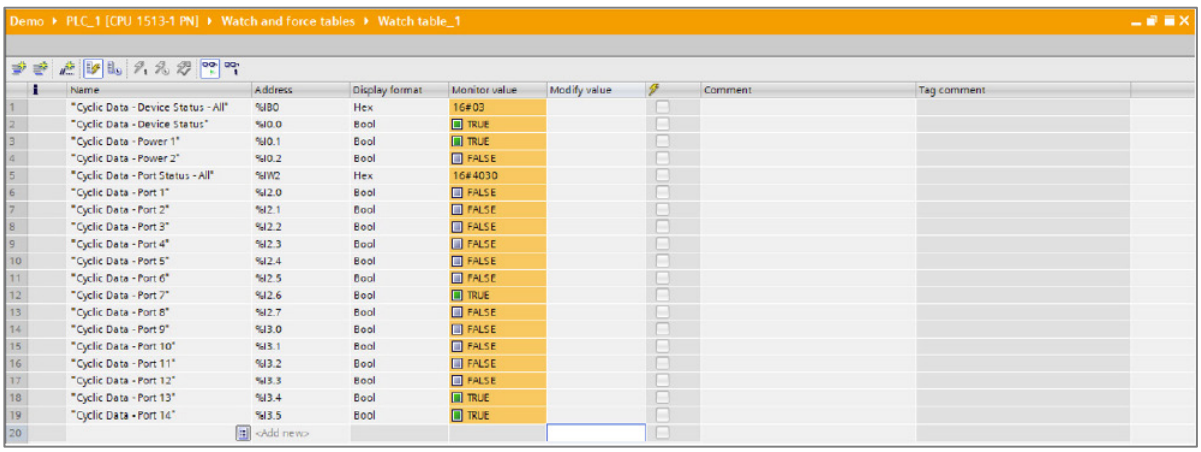
- **Port Status**

Category	Direction	Byte	Bit	Name	Description
Port	Input	0	0	Port 1 Connection	0 is not connected, 1 is connected
			1	Port 2 Connection	0 is not connected, 1 is connected
			2	Port 3 Connection	0 is not connected, 1 is connected
			[...]	[...]	[...]

Category	Direction	Byte	Bit	Name	Description
			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
Port	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:



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	Fault Status	ro	0	Unavailable
			1	Device detect fault
			2	OK
2	Power 1 Status	ro	0	Unavailable
			1	Power 1 fails
			2	OK
3	Power 2 Status	ro	0	Unavailable
			1	Power 2 fails
			2	OK
4	DI 1 Status	ro	0	Unavailable
			1	Closed

Byte	Name	Access	Value	Description
			2	Open
5	DI 2 Status	ro	0	Unavailable
			1	Closed
			2	Open
6	Spanning Tree Config	ro	0	Unavailable
			1	Disable
			2	RSTP
			3	MSTP
7	Turbo Ring v2 Config	ro	0	Unavailable
			1	Disable
			2	Enable
8	Turbo Ring v2 Ring 1 Config	ro	0	Unavailable
			1	Disable
			2	Enable
9	Turbo Ring v2 Ring 1 Status	ro	0	Unavailable
			1	Disable
			2	Broken
			3	Healthy
10	Turbo Ring v2 Ring 2 Config	ro	0	Unavailable
			1	Disable
			2	Enable
11	Turbo Ring v2 Ring 2 Status	ro	0	Unavailable
			1	Disable

Byte	Name	Access	Value	Description
			2	Broken
			3	Healthy
12	Turbo Chain Config	ro	0	Unavailable
			1	Disable
			2	Head
			3	Member
			4	Tail
13	Dual Homing Config	ro	0	Unavailable
			1	Disable
			2	Primary path always first
			3	Maintain current path
			4	Primary path sensing recovery
14	Media Redundancy Protocol Config	ro	0	Unavailable
			1	Disable
			2	Enable
15	Media Redundancy Protocol Manager Status	ro	0	Unavailable
			1	Disable
			2	Initiation
			3	Awaiting Connection
			4	Primary Ring Port Link Up
			5	Ring Open
			6	Ring Closed
16	Media Redundancy Protocol Client Status	ro	0	Unavailable

Byte	Name	Access	Value	Description
			1	Disable
			2	Initiation
			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
0	Status Alarm	rw	0	Do not send any alarms	0: No alarms
			1	Send alarm if any status change	
1	Power Alarm 1	rw	0	Do not send power failed alarm	0: No alarms
			1	Send alarm if power supply 1 fails	
2	Power Alarm 2	rw	0	Do not send power failed alarm	0: No alarms
			1	Send alarm if power supply 2 fails	
3	RSTP Topology Changed Alarm	rw	0	Do not send RSTP topology changed alarm	0: No alarms
			1	Send alarm if RSTP topology changed	
4	MSTP Topology Changed Alarm	rw	0	Do not send MSTP topology changed alarm	0: No alarms

Byte	Name	Access	Value	Description	Default Value
			1	Send alarm if MSTP topology changed	
5	Turbo Ring V2 Ring Broken	rw	0	Do not send TR2 broken alarm	0: No alarms
			1	Send alarm if TR2 is broken	
6	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
Mode 0 - Factory Default Mode	Original Factory Reset	Cleans all configured settings including PROFINET
Mode 1	Reset Application data	Resets I&M data and the alarm configuration of devices and ports
Mode 2	Reset Communication parameter	Resets Device Name to " " and IP to 0.0.0.0
Mode 3	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.

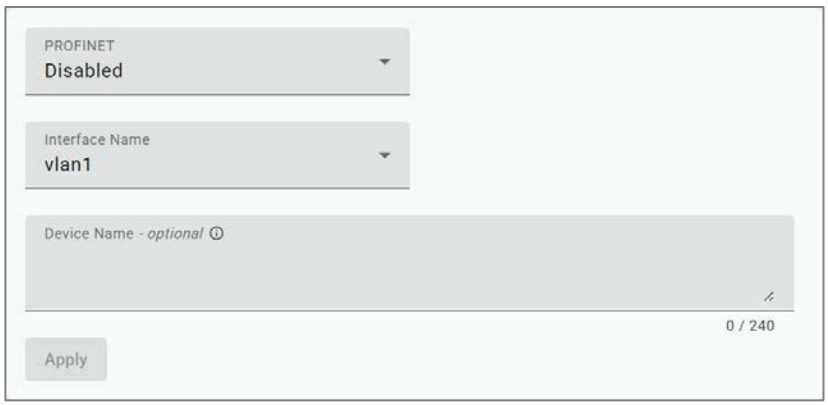
This page includes these tabs:

- Settings
- Status

PROFINET - Settings

Menu Path: Industrial Application > PROFINET - Settings

This page lets you configure PROFINET for your device.

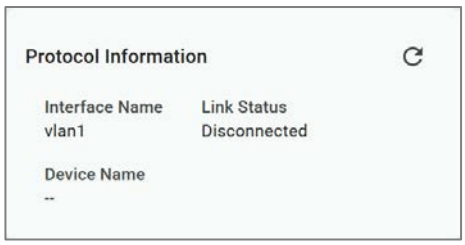


UI Setting	Description	Valid Range	Default Value
PROFINET	Enable or disable PROFINET for your device. This allows your device to be detected in a PROFINET network.	Enabled / Disabled	Disabled
Interface Name	Select which interface to use for PROFINET.	Drop-down list of interfaces	vlan1
Device Name	Specify the labels you want to use to identify this device in PROFINET. Multiple labels can be entered, separated by a period(.). For example, "moxa.device-01" can be entered to specify "moxa" and "device-01" as separate labels. **Note** PROFINET labels are subject to the following naming rules: • Labels only support the following characters: a-z, 0-9, and dashes (-) • Labels must be 1 to 63 characters long • Labels cannot be in a 4-number format similar to IP addresses • Labels cannot start with “port” followed by 3 or more digits • Labels cannot start or end with a period (.) or a dash (-)	1 to 63 characters for each label 0 to 240 characters total	N/A

PROFINET - Status

Menu Path: Industrial Application > PROFINET - Status

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



UI Setting	Description
Interface Name	Shows the interface used for PROFINET.
Device Name	Shows the user-defined labels for the device.
Link Status	Shows the PROFINET link status.

Chapter 4

Security Hardening Guide

Security Hardening Guide Overview

This chapter provides an overview of security strategy, standards, and recommended best practices to improve the security landscape.

The threat landscape is constantly evolving, and no security guide can ever provide 100% protection. This chapter is constantly being expanded, and is not exhaustive.

Security Best Practices

Product Security

This section provides essential information on the installation of your product.

Physical Installation Guidelines

Physical protection of devices is vital to network security.With physical access to devices, prospective attackers can physically bypass security mechanisms, alter network conditions, or plant additional malicious devices in networks. Follow these tips to help reduce the risk of tampering with networking devices by unauthorized personnel.

- Install the device in an access-controlled area.

To further protect your device from potential physical attacks, it is important to conduct a risk analysis and implement appropriate physical security measures. Consider physical security like installation within a locked cabinet, surveillance, security guards, and access control systems, among other measures. The specific measures you choose should be based on your environment and the level of risk you face.

- Install a Layer 2 switch within the security perimeter.

This perimeter can be established by setting up a firewall at the border, as the switch is not designed to be directly connected to the Internet. Note that the switch should not be classified as zone or boundary equipment. Avoid connecting the device directly to the Internet, as this can leave your network vulnerable to security breaches.

- Follow the Quick Installation Guide included in the package of your device.

It contains step-by-step instructions that are easy to follow and will help you set up the device quickly and efficiently.

- Examine and monitor anti-tamper labels applied to the device enclosures.

These labels provide a quick and easy way for administrators to determine if the device has been tampered with.

- Protect or deactivate any ports that are not currently in use.

Fewer active ports mean fewer avenues of attack. Refer to the Port Interface section in the User Manual.

- Protect reset buttons and other physical controls.

An attacker could bypass software/firmware security by forcing a reset and restoring default device credentials. Ensure that management interfaces, reset buttons, and other physical access routes are protect. For example, a device in a locked cabinet could still be vulnerable to being reset using a probe through a vent. Ensure that access to the locked cabinet is controlled, and that the reset button itself is covered or inaccessible from vents.

Account Management Guidelines

Manage user accounts, set passwords, and restrict access to authorized personnel only.

- Assign the appropriate account privileges.

Limit the number of users with admin privileges to only those who need to perform device configuration or modifications. For other users, read-only access is sufficient. Moxa devices supports both local account authentication and remote centralized mechanisms, including Radius and TACACS+. This allows for flexible and secure access control options.

- Implement good password practices.

Good password practices include:

  - Enabling and configuring a Password Policy to ensure your password meets specified requirements.
  - Setting the minimum password length to at least eight characters.
  - Require passwords to have at least one uppercase and lowercase letter, a digit, and a special character.
  - Set password expiration.
  - Replacing all default passwords and secure default accounts.
  - Use unique passwords.
  - Update passwords regularly.
  - Never share passwords.

Note

Based on trends in cybersecurity regulations, we recommend users increase the complexity of their passwords to the highest level to further strengthen password security.

- Verify and manage account activity.
    - Enable event logging and periodically check for login failures or irregular activity.
    - Consider centralized management or automation of log details.
    - Consider enabling account lockout. After too many sign-in attempts, the account can be deactivated or the source IP blocked. Evaluate operational impacts of account or IP blocks to ensure the right balance of security and continuous operation.
- Do not include sensitive information in user-configurable feedback.

Some messages can be configured, such as showing an error message after a failed login. Do not include any sensitive information in these messages, or any other information that might give an attacker an advantage. Possible sensitive information might include:

- Hints about accounts or passwords
- Unnecessary information about password requirements that might help an attacker narrow down brute force candidates.
- Detailed contact information for administrators that could be used in spearphishing attacks.

Protecting Vulnerable Network Ports

Understand security risks and mitigate them by configuring network ports correctly.

- Changing port numbers for active, including TCP port numbers for HTTP, HTTPS, Telnet, and SSH.
- Disable any ports that are not in use, as they could pose an unacceptable security risk.
- Use encrypted communication protocols wherever available.

Consider the following alternatives

- HTTPS instead of HTTP
- SSH instead of Telnet
- SFTP instead of TFTP
- SNMPv3 instead of SNMPv1/v2c
- 802.1x with EAP-PEAP instead of MAC Authentication Bypass

Refer to Network Interface for more information.

- Enable encryption for encryption-optional protocols.

Encryption-optional protocols (encryption) include:

- 802.1x (EAP-PEAP authentication)
- SNMPv3 (authentication and encryption)
- Syslogs (TLS)

- Avoid using Ping Tracking to external devices (e.g. over the internet).
- Disable Loop Protection when no longer needed.
- Configure automatic session locking or idle timeouts so that idle sessions cannot be hijacked.
- Generate new SSL certificates and SSH keys for devices prior to using HTTPS or SSH applications.

Refer to SSH & SSL for more information.

Maintaining Communication Integrity

Ensure that information sent is accurate, complete, and secure.

Maintaining communication integrity reduces risks risk of data corruption or interception, and associated security breaches, data loss, and other negative effects on networks and their users.

- Use encryption.

Encryption uses mathematical algorithms to convert data into a secret code, making it extremely difficult for people without the correct codes to read or change the data. By using encryption, you can ensure that the data being transmitted is secure and cannot be intercepted by unauthorized users. For certificates, use a

key strength of at least RSA 2048, and a hash algorithm strength of at least SHA256.

- Use digital signatures.

Digital signatures verify the authenticity and integrity of digital documents or messages. Using a digital signature, you can ensure that the message or document came from the expected sender and has not been altered.

- Implement access control.

Access control restricts access to only authorized users to the network and its resources. By implementing access control measures, such as firewalls or access control lists, you can prevent unauthorized access and reduce the risk of data breaches.

- Implement multiple security mechanisms.
  Layered multiple security mechanisms such as DHCP Snooping and Dynamic ARP Inspection helps improve resilience against various types of cyberattacks.

Communication Integrity Features

Moxa devices provide support for secure versions of protocols to help maintain communication integrity.

HTTPS (Hypertext Transfer Protocol Secure)

HTTPS is a secure version of the regular HTTP protocol for transmitting data over the internet. HTTPS uses TLS (Transport Layer Security) encryption and digital certificates to protect the data in transit from interception, tampering, or eavesdropping.

Refer to Management Interface for more information.

SSH (Secure Shell)

SSH is a secure protocol for remote terminal login and secure file transfers. SSH uses encryption to protect the data in transit, making it difficult for anyone to intercept or tamper with it. SSH also provides authentication and access control features to ensure only authorized users can access the network.

Refer to Management Interface for more information.

SFTP

SFTP is a secure version of FTP (File Transfer Protocol) that uses encryption to protect the data in transit. SFTP also provides authentication and access control features to ensure only authorized users can access the network.

Refer to Management Interface for more information.

SNMP v3 (Simple Network Management Protocol version 3)

SNMP v3 is a secure version of the SNMP protocol used for network management and monitoring. SNMP v3 uses encryption and authentication to protect the data in transit, making it difficult for anyone to intercept or tamper with it. SNMP v3 also provides access control features to ensure only authorized users can access the network. When using SNMPv3, make sure encryption and authentication are enabled and configured.

Refer to SNMP for more information.

> **Note**
>
> SNMP managers should be used in accordance with their own security hardening guides and recommended security procedures.

Device Access Control Best Practices

Device access control is an essential aspect of network security that helps protect against unauthorized access to network resources.Unauthorized access can occur through various means, including physical access to network devices, hacking, or social engineering. Without proper access control measures in place, networks are vulnerable to security breaches, data theft, and other malicious activities.

Device access control is particularly important for organizations that handle sensitive data, such as financial institutions, healthcare providers, and government agencies. By implementing device access control, these organizations can limit access to sensitive information and prevent security breaches. Below are some ways to ensure device access control:

- Adopt the **Principle of Least Privilege**.

This principle involves granting users, applications, or systems the minimum level of access or permissions they need to perform their specific tasks and nothing more. Requests for additional access, such as HTTPS, SSH, or Moxa services for administration, should be carefully evaluated before being approved.

- Use strong passwords.

Passwords should be complex and unique for each device. Passwords should also be changed regularly to maintain security.

- Implement allowlists.

Allowlists are authorized devices or users allowed to access a particular network resource. Allowlists can be managed at the device, network, or application levels. Network administrators can use allowlists to ensure that only authorized devices or users can access sensitive resources. The key feature of an allowlist is that anything not on the allowlist is automatically blocked, ensuring only authorized devices, uses, or services can operate freely in a network environment.

- Implement Traffic Storm Control.
  Limits excessive broadcast traffic to maintain network performance. Broadcast storms can occur accidentally when devices are misconfigured, but they can also be a tool used in denial-of-service attacks.

About Device Integrity and Authenticity

Integrity and authenticity are vital elements of trust within a network.

Device integrity refers to the state of a device being complete, unaltered, and free from any unauthorized changes or modifications.

Authenticity refers to the assurance that the device is genuine and comes from a trusted source.

Both integrity and authenticity are critical aspects of device security. Methods to sustain these aspects include:

- Configuration Backup & Encryption
- Secure Boot

Configuration Backup and Encryption

Configuration backup and encryption protects a device's sensitive data and configuration by created an encrypted copy storing it securely. In the event of unauthorized device changes, correct configuration information can be quickly and securely restored.

The process involves creating a backup of the device's configuration and then encrypting it using a strong encryption algorithm. The encrypted backup is then stored securely to prevent unauthorized access. This process is particularly important for devices that store sensitive information, such as network equipment, servers, and other critical infrastructure. Encrypting the configuration backup ensures that the data remains protected even if the backup location is compromised.

Refer to Configuration Backup and Restore for more information.

Secure Boot

Secure Boot is a security mechanism designed to ensure that devices boot using only software that is verified as trusted. The primary function of Secure Boot is to prevent unauthorized software from running during the boot process. It achieves this by verifying the integrity and authenticity of the bootloader and firmware.

A bootloader refers to the initial software that runs when a device is powered on. Its primary role is to load the device's operating system. Firmware is software embedded within the device that manages and controls the device's hardware functions.

Moxa hardware makes use of cryptographic modules embedded in devices to support verification processes. The device's ROM (read-only memory) contains approved bootloaders and associated digital certificates, which are used to verify the integrity of the firmware.

When the device boots, the first thing to run is the bootloader. Secure boot checks the digital signature against the certificate stored in ROM. If the signatures match, the boot process continues. If they do not match, or there is evidence of tampering, the boot process halts to prevent potential security breaches.

Securing USB Interfaces on Network Devices

- Disable USB ports when not in use.

  USB ports should be disabled by default to prevent unauthorized or accidental use.

- Limit rights to enable or configure USB ports to a minimum number of authorized users.

Use role-based access control (RBAC) or require multi-factor authentication (MFA) to enable USB ports.

- Standardize procedures and rigorously observe them.

Your procedures should cover:

  - When and why USB interfaces can be used
  - The type and number of USB devices permitted
  - How data on those devices must be secured. Ensure that all employees and users understand and observe these procedures

Device Resource Management and Monitoring

Moxa devices provide a number of features to help customers manage device resources efficiently and monitor security.

About Device Resource Monitoring

Network device resource management is essential for network reliability and security. By monitoring use of network resources, administrators can verify that network guidelines are being followed and devices are operating efficiently and effectively.

Proactive monitoring and management of device resources such as CPU utilization, memory utilization, and network traffic allows administrators to identify potential security breaches early, and help avoid network downtime and disruption. For example, abnormal spikes in network traffic or CPU utilization could be indicative of a malware infection or a denial-of-service attack.

Examples of activities to monitor include:

- Connected ports
- CPU usage
- Memory usage

Refer to Device Summary for more information.

About Event Logs for Monitoring

In addition to real-time monitoring and management, Moxa devices provide advanced logging options to help identify security events. Chosen event types can also generate notifications to notify administrators of unusual events where attention is needed, or to feed into larger security monitoring systems.

You can leverage system logs to monitor events, such as failed logins or access attempts from unauthorized accounts. Event logs respond the same way to the same events, providing comprehensive visibility into security events.

Refer to Event Log for more information about Event Logs.

Refer to Event Notifications for more information about Event Notifications.

Refer to SNMP - General for more information about SNMP configuration.

About Port Mirroring for Monitoring

Port Mirroring duplicates data transmitted over a port for analysis.

You can use port mirroing to mirror the trafic of an Ethernet port connected to untrusted networks to allow for monitoring and analysis of trafic that would otherwise be uncontrolled.

Refer to Port Mirroring for more information.

Recommended Settings for Services and Features

When prioritizing device security, the first point of assessment is often the network interfaces and services.By deactivating unneeded interfaces and services, one can reduce potential vulnerabilities and associated security threats. Additionally, activating the appropriate security features enhances early anomaly detection and bolsters the device's defense against cyber attacks.

Note

Factory defaults are described in each feature section.

Common Protocols and Ports

Service Name	Default Port	Default Setting	Security Suggestions
HTTP	TCP 80	Enabled	Disable if possible to avoid leaks from unencrypted traffic.
HTTPS	TCP 443	Enabled	
Telnet	TCP 23	Enabled	Disable if possible to avoid leaks from unencrypted traffic.
SSH	TCP 22	Enabled	
NTP/SNTP	UDP 123	Disabled	Use SNTP to synchronize system time if possible. Enable NTP authentication if possible.
SNMP	UDP 161 UDP 162 TCP 10161 TCP 10162	Disabled	For V1 & V2c, change default community string names, i.e. public & private, to other unique names. For V3, enable SNMP admin account authentication.
Syslog	UDP 514	Disabled	Enabling Syslog is recommended to avoid missing critical logs due to limited local storage. This sends logs to an external syslog server, where they can be securely stored and retained. The syslog server is responsible for keeping these logs for a minimum period required by local regulations, ensuring critical incidents are properly documented and accessible when needed.
RADIUS	UDP 1812	Disabled	Enabling RADIUS authentication can help administrators manage password changes more efficiently.
Moxa Services	TCP 443 UDP 40404	Enabled	These 2 ports are only used by the Moxa management software. Disable it if you don't use Moxa management software.

Security-Related Functions

Function	Default Setting	Security Suggestions
Password Policy	Disable	Enable password policy to comply enterprise security policies.
Login policy	Disable	Enable a login policy to heighten resistance against brute force attacks and terminating any inactive login sessions.
Malformed Packets Filtering	Disable	The "Malformed Packets Filtering" feature logs events at a user-defined severity level whenever the system discards malformed packets. Depending on the protocols active in your network, you can choose to enable this feature or leave it disabled.
DoS Policy	None	Select a DoS policy according to your network traffic to increase network robustness.
Session control	None	Configure session control policies appropriate for your traffic to improve network reliability.
802.1X over ports	Disable	Enable 802.1X port authentication to block unauthorized LAN access.
Traffic Storm Control	Enable	Enable Traffic Storm Control to manage the amount of unknown traffic on the network.
Trusted Access	Enabled	By default, the device permits all connections from the LAN attempting to access it. For enhanced security, block all LAN connections attempting to access the device. Then, use a trusted IP list to specify which trusted IPs are allowed access to the device.
Static Port Lock	Disable	Static port lock, also known as MAC Table or MAC Sticky, is a port security feature that remembers the first MAC address used, and will not initiate links with other MAC addresses.

Caution

The following are known to have security flaws:

- EthernetIP
- Modbus TCP
- MMS
- PROFINET
- Radius server
- Email notification
- SNMP v1/v2c
- TACACS+
- Telnet
- TFTP
- SNTP
- MAB
- NTP authentication
- MD5

Use alternatives or take extra precautions.

Considerations for GOOSE Check

GOOSE Check **Tamper Response** may impact network communication when misconfigured.

Before using **GOOSE Check Tamper Response Port Disable**, carefully evaluate the network to ensure the risk of attaching unexpected devices is low. Unexpected devices may trigger **Tamper Response**. Ports disabled by **GOOSE Check** do not automatically recover, possibly affecting network communication.

To re-enable ports disabled by **Tamper Response Port Disable**, go to **Port** > **Port Interface** > **Port Settings**, click ***[Edit]*** corresponding to the disabled port, and then set **Admin** to **Enabled**. Click **Apply** to save your changes.

Refer to GOOSE Check for more information.

Protocols / Services with Weak Authentication / Encryption

Some protocols and services support weaker authentication or encryption, and may not be secure over untrusted networks.

Choose secure alternatives or take precautions to mitigate possible threats.

Services

- TACACS+
- RADIUS
- 802.1x
- MAB
- NTP server
- NTP/SNTP client
- PTP
- DHCP relay
- mDNS
- Tracking
- Email notification
- TFTP
- SNMP v1/v2
- GVRP/GMRP
- DNS client
- DHCP client
- DHCP server
- LACP
- Loop protection
- LLDP

- IGMP snooping

Redundant Protocols

- MRP
- Turbo Ring v2
- Turbo Chain
- RSTP/MSTP

Industrial Protocols

- MMS server
- Ethernet/IP
- Modbus TCP
- Profinet
- GOOSE check

L3 protocols

- RIP (NOS v6.0)
- BFD (NOS v6.0)
- VRRP
- PIM-DM
- PIM-SM

Common Threats and Countermeasures

These are examples of common known threats, and suggestions for mitigation.

Incident Category	Detailed Description	Mitigation Suggestions
Tampering & Information Disclosure	An attacker can read or modify data transmitted over HTTP data flow.	Disable HTTP, and replace HTTP transmission with HTTPS.

Incident Category	Detailed Description	Mitigation Suggestions
Tampering & Information Disclosure	An attacker can read or modify data transmitted over Telnet data flow.	Disable Telnet, and replace HTTP transmission by SSH.
Information Disclosure	Data flowing across TFTP may be sniffed by an attacker.	Use SFTP instead of FTP.
Denial of Service	SNMP Server crashes, halts, stops or runs slowly by excessive quires.	Enable rate limit to stop excessive SNMP requests.
Denial of Service	RADIUS Server crashes, halts, stops or runs slowly by excessive quires.	Enable rate limit to stop excessive RADIUS requests.
Repudiation	Devices fail to synchronize a system time with a trusted NTP/SNTP server.	Enable NTP authentication to verify a connection with the trusted NTP/SNTP server.

Note

Create an incident response plan and follow it carefully. Ensure your procedures allow for user reporting and admin response to those reports. Many threats manifest themselves as irregular device behavior – such as device inability to provide basic services like routing or firewall functions, which in turn lead to interruptions or unauthorized access. Create a plan that allows admins to prepare, reboot, and monitor devices with abnormal behavior.

Recommended Operational Roles and Duties

Adhering to the principle of least privilege reduces risks by ensuring users operate at the minimum privilege required to complete their tasks.

Instead of individual allocation, privilege levels should be tied to specific job functions. For optimized device security, we recommend three distinct privilege levels, each tailored for different management needs.

Note

Customize user roles based on your organization needs, and eliminate unneeded roles.

Administrator

Designated for system management, this privilege level permits:

- Creation and deletion of configuration objects, files, and user accounts.

- Monitoring system status and resources.
- Modifying parameter values.
- Reviewing stored data within the device.

Administrator Responsibilities:

- Reset and periodically change the default administrator password.
- Ensure password complexity aligns with enterprise security policies.
- Manage and authorize individuals with appropriate access privileges.
- Disable non-essential interfaces or network services.
- Enable secure communication protocols to guard against data breaches.
- Regularly update firmware to address potential vulnerabilities.

Supervisor

Tailored for network experts or operators, this privilege grants:

- Monitoring of system status and resources.
- Adjusting values in configuration objects or files.
- Access to review data stored in the device.

Supervisor Responsibilities:

- Continuously monitor system status and resources to maintain device functionality.
- Routinely verify the integrity of device configuration objects and files.
- Manage trusted devices through IP and MAC allowlisting.
- Oversee and respond to system alerts to preempt device failures and security threats.

Auditor

Reserved for audit-focused personnel, this level allows:

- Monitoring of system status and resources.
- Reviewing data stored within the device.

Auditor Responsibilities:

- Regularly inspect logs to identify and assess incidents and their associated risks.

Moxa devices provide three user privilege categories: admin, supervisor, and user. We advise aligning the admin role for administrator users, the supervisor role for supervisor users, and the user role for auditor users.

Recommended Patching and Backup Practices

Moxa's guidance on ensuring device security through regular firmware upgrades and configuration backups.

Configuration Backup

For network operators and system administrators, it is essential to regularly back up device configurations. This precaution allows for quick recovery in unforeseen scenarios, such as cyber attacks.

> **Note**
>
> Prioritize use of secure transfer protocols – such as SFTP – for file transfers to protect the configuration maintenance process.

Recommendations for Vulnerability Management

As the adoption of the Industrial IoT (IIoT) continues to grow rapidly, security becomes an increasingly high priority.

The Moxa Product Security Incident Response Team (PSIRT) takes a proactive approach to protect our products from security vulnerabilities and help our customers better manage security risks.

To report vulnerabilities for Moxa products, please submit your findings on the following web page: https://www.moxa.com/en/support/product-support/security-advisory/report-a-vulnerability.

For the most up-to-date Moxa security information, please visit our security advisory page: https://www.moxa.com/en/support/product-support/security-advisory

Recommendations for Decommissioning

To avoid any sensitive information such as account passwords or network configurations from disclosure, always delete all imported certificates and reset devices to factory default before you decommission your devices.

Note

Things to keep in mind when decommissioning or re-purposing devices:

- Device data can be cleared using the Factory Reset options. When reseting devices, make sure to confirm the operation and allow it sufficient time to complete.
- Delete all logs, and verify deletion.
- After all reset processes are complete, verify that all sensitive data has been cleared.

Security Standards and Concepts

Introduction to Defense in Depth

The Defense-in-Depth strategy is used to protect systems from various types of attacks by using multiple independent defense mechanisms.This involves incorporating multiple layers of security to protect the product against potential attacks and vulnerabilities at various stages of its design, development, and use.

It is crucial to understand that no single protection can guarantee complete security. That's why the Defense-in-Depth approach makes it difficult for attackers to leverage one weakness to attack the product or network as a whole. This approach requires attackers to overcome multiple obstacles undetected, increasing the difficulty level. By leveraging multiple security features and layers of protection in a product, vulnerabilities in any one layer can be mitigated.

About AAA - Authentication, Authorization, and Accounting

Authentication, **A**uthorization, and **A**ccounting (AAA) is a user-based access control paradigm.AAA coexists with other security practices. While product security and network security focus on device or process security, AAA focuses on users.

AAA comprises a set of functions for an administrator to determine which users can access a network device, which services are available to authorized users, and collect information about user activities for audits or charging purposes if required. When implemented well, AAA can provide an extra layer of security across different aspects.

Authentication

Authentication provides a method of identifying a user before access to the network device is granted, typically by having the user enter a valid username and password and/or provide a physical token or digital certificate. Additional policies such as a password complexity check or login failure lockout can also increase access security.

Authorization

After authentication is successful, a user can be authorized to use specific resources on the device or perform specific operations. For instance, a normal user with limited permissions may only view the device's system settings, whereas an administrator would have full control to view or edit all system settings.

Accounting

Accounting keeps track of user activities on the device. It monitors the resources a user consumes during network access. This can include the amount of data sent and received through an Ethernet port or the number of user login failures.

About Authentication Types

Handle authentication with the local device exclusively, or with a remote server using local accounts only as a fallback.

It is important to choose the right authentication method, or combination of authentication methods for your network environment and use case. Moxa devices offer the following authentication options.

Local Authentication

Local authentication uses the accounts and settings stored on the local network device to identify users (authentication), determine which services they can use (authorization), and track basic user activities such as amount of data transferred or number of login failures (accounting).

Remote Authentication

Remote authentication uses accounts configured on a RADIUS server - allowing AAA to be configured from a single, centralized location. However, it is important to note that local authentication is retained as a fallback mechanism to ensure the device can be configured if the RADIUS server becomes inaccessible. Additionally, Moxa products support backup RADIUS servers if the primary becomes inaccessible. Due consideration should be given to the configuration and maintenance of backup servers for redundancy.

Features	Local	Remote
Configuration location	Local device	Remote RADIUS server, local as fallback
Number of accounts	Few	Many
Password security requirements	Limited	Many
Allowed services	Specified locally	Determined by server
Authority types	Admin, User, Supervisor	Admin, User
User feedback on failed login	Custom prompt	Server-defined
Setup effort	Low	High
***Allowed services are usually dependent on authority types.**		

Example: Creating a Local User

Local accounts are authenticated and managed by the local device, and function even when remote RADIUS servers are unavailable.

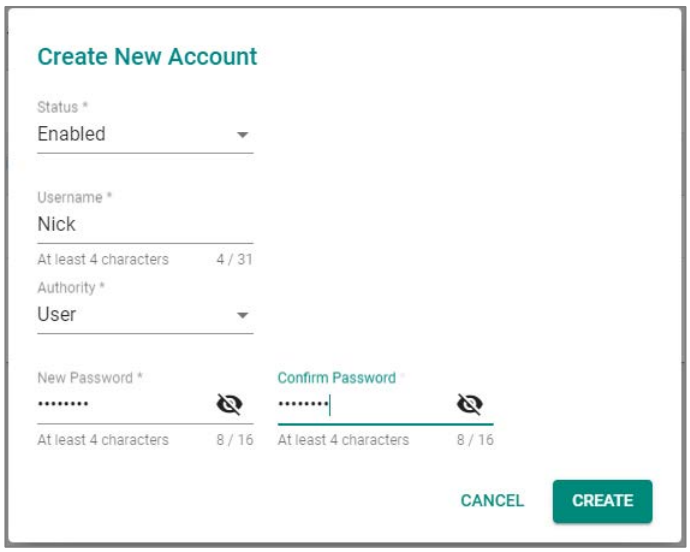
Make sure you have an account with **Admin** authority.

In this example, create a local user with simple **User** level authority to fill the Authentication of the AAA tripod. Once the user has been created, add additional access controls.

1. Sign in to the device with admin credentials.
2. Go to **System** > **Account Management** > **User Accounts**, and then click ***[Add]***.

   The Create New Account panel appears.
3. Set **Status** to **Enabled**.
4. In the **Username** field, type `Nick`.
5. Set **Authority** as **User**.
6. In the **New Password** field, type `1qaz!@#$`, and then type again to confirm.
7. Click **Create**.

By creating the user **Nick**, Authorization and Accounting details can now be configured.



Now that a user account has been created, add account controls. Account controls allow setting a warning for incorrect passwords, account lockouts, and automatic logout.

Example: Configuring Account Controls for Local Users

Login Failure Account Lockout and Auto Logout increase the security of local accounts.

Make sure you have set **Authentication Protocol** as **Local** or **RADIUS, Local** to ensure that local accounts can be used to **Security** > **Authentication** > **Login Authentication**.

Enabling additional account controls can increase resistance to brute-force attacks as well as enable troubleshooting. This example demonstrates how to set account lockouts after failed login attempts and manage idle users.

1. Sign in to the device with administrator credentials.
2. Go to **Security** > **Device Security** > **Login Policy**.

   The Login Policy panel appears.
3. In the **Login Authentication Failure Message** field, type the following:

   `Warning! The account will be temporarily locked if there are too many consecutive login failures.`

Note

Do not configure the message with any information that might help an attacker guess a password or conduct phishing operations, such as password hints or staff contact information.

4. Set **Login Failure Account Lockout** to **Enabled**.
5. In the **Login Failure Retry Threshold** field, type 3.

This is the number of failed attempts before the user account will be temporarily blocked.

Temporary can bans help prevent password guessing and brute force attacks by preventing attackers from rapidly guessing many passwords.

6. In the **Lockout Duration** field, type 5.

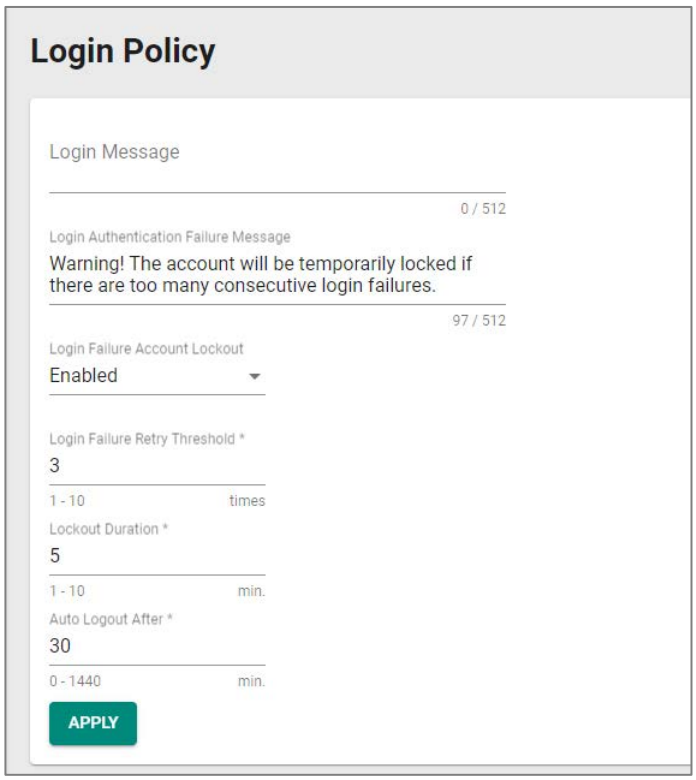
This specifies the number of minutes the account will be locked.

7. In the **Auto Lockout After** field, type 30.

This is the amount of time in minutes before inactive accounts automatically log out.

This configuration:

- Displays a warning message on failed login attempts, enabling troubleshooting
- Blocks accounts for five minutes after three unsuccessful login attempts, limiting the effectiveness of credential guessing
- Automatically logs out inactive user accounts after thirty minutes, reducing risks of unauthorized access through idle consoles



Optionally, configure allowed access protocols.

Example: Configuring a Remote RADIUS Server

In this example, the RADIUS server handles all Authentication, Authorization, and Accounting.

Make sure you have a working RADIUS server and corresponding configuration information. In our example, we use a server that has the following settings:

- PAP authentication protocol
- An address of 192.168.127.1
- UDP port 1812
- A preconfigured shared key

Remote Authentication Dial-In User Service (RADIUS) servers may make it easier to manage large numbers of users from a central location.

1. Sign in to the device with admin credentials

2. Go to **Security** > **Authentication** > **Login Authentication**, and then set **Authentication Protocol** to **RADIUS, Local**.

This setting will use the remote RADIUS server as the primary authentication source, and use local authentication as a fallback if the RADIUS server is unavailable.

> **Note**
>
> Enabling a RADIUS authentication will not remove local accounts. Make sure local accounts have a strong, unique password. Local accounts are still required both for RADIUS server configuration as well as for local fallback if the RADIUS server is not reachable. Go to Security > Authentication > RADIUS.

3. The RADIUS Server will appear.
4. Configure all of the following:

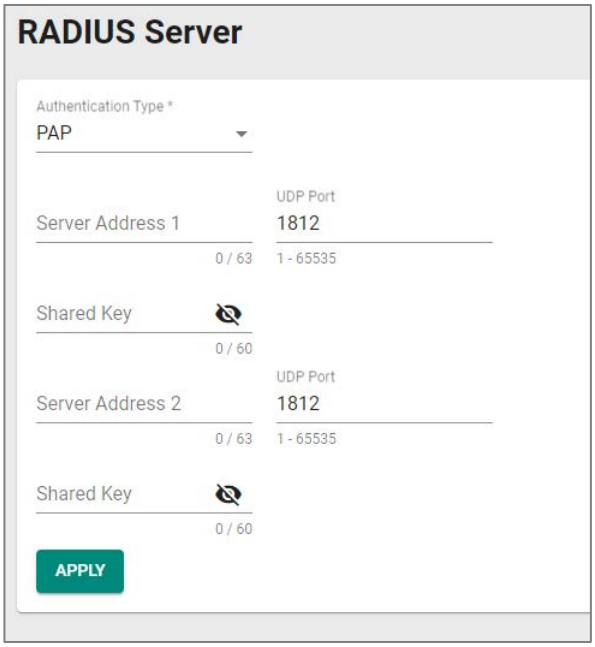
Field	Setting
Authentication Type	**PAP**
Server Address 1	192.168.127.1
UDP Port	1812
Shared Key	Enter your Shared Key here.

These configuration options are provided as an example only, and will need to match your network environment.

5. Click **Apply**.

By configuring a remote authentication, the network device will redirect user login requests to the RADIUS server. When logging in with remote user `Peter`, the RADIUS server will process the authentication request and determine whether to grant access to the device. If `Peter` does not match RADIUS or Local information, access will be denied.

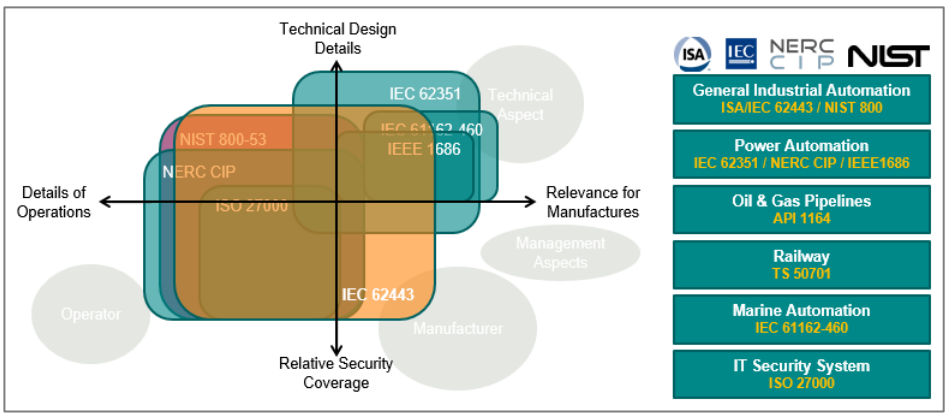
In situations where the RADIUS server is not reachable or unavailable, users such as `Nick` or other existing local users can still access the network device using their local passwords.



ISA / IEC 62443 Standards and Architecture

Security Reference Standards

In the field, large networks are connected through switches and routers. These devices manage all data traffic and serve as the main bridge between devices. However, if these switches and routers are compromised, the repercussions can cascade to all connected devices. To help mitigate this risk, Moxa implements the ISA/IEC 62443-4-2 standard into our network device designs.



Industries such as electricity, oil and gas, rail transportation, and maritime have established their own standards for security. These standards include guidelines and regulations designed to address each industry's unique concerns. Among these standards,62443 is the most comprehensive, covering a wide range of industries and security concerns, making it an excellent choice for organizations that prioritize security in their operations.

ISA/IEC 62443 Standards and Architecture

The ISA/IEC 62443 standard is a set of guidelines and best practices designed to help organizations secure their industrial automation and control systems (IACS) against cyber threats. The framework helps assess risks to IACS and implement appropriate security measures to protect against cyber attacks and malware. The standard consists of multiple parts, with each covering different aspects of industrial cybersecurity.

Parts of ISA/IEC 62443	Scope	Sections
ISA/IEC 62443-1	General	Part 1-1: Terminology, concepts, and models Part 1-2: Master glossary of terms and abbreviations Part 1-3: System security compliance metrics Part 1-4: IACS security lifecycle and use-cases
ISA/IEC 62443-2	Process and Program requirements	Part 2-1: Establishing an industrial automation and control system security program Part 2-2: Implementation guidance for an IACS security management system Part 2-3: Patch management in the IACS environment Part 2-4: Security program requirements for IACS service providers
ISA/IEC 62443-3	Systems	Part 3-1: Security technologies for industrial automation and control systems Part 3-2: Security risk assessment and system design Part 3-3: System security requirements and security levels
ISA/IEC 62443-4	Components	Part 4-1: Secure product development lifecycle requirements Part 4-2: Technical security requirements for IACS components

Product suppliers adhere to the ISA/IEC 62443 standard to provide components for Industrial Automation and Control System \(IACS\) solutions. These components can be:

- Individual items
- Combined products forming a system or subsystem

Additionally, system integrators use the following sections of the ISA/IEC 62443 standard:

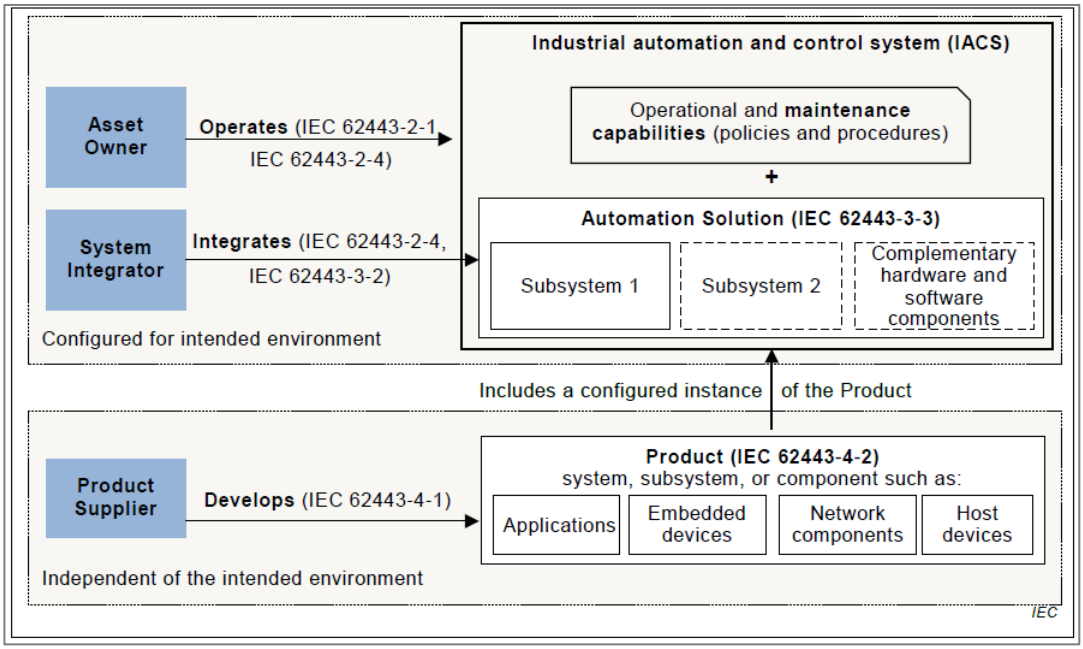
- IEC 62443-2-1
- IEC 62443-2-4
- IEC 62443-3-2
- IEC 62443-3-3

These standards help integrators:

- Determine security zones
- Specify security capability levels for each zone
- Integrate products into an Automation Solution

General **ISA/IEC 62443-1**	**ISA-/IEC 62443-1-1** **Foundational Requirements (FR)**
System **ISA/IEC 62443-3**	ISA-/IEC 62443-3-3 System Requirements (SR)
Component **ISA/IEC 62443-4**	ISA-/IEC 62443-4-2 Component Requirements (CR)

Once the solution is ready, it's installed on-site, becoming a vital part of the IACS.



Establishing Foundational Requirements

FR 1	Identification and Authentication Control
FR 2	User Control
FR 3	System Integrity
FR 4	Data Confidentiality
FR 5	Restricted Data Flow
FR 6	Timely Response to Events
FR 7	Resource Availability

Once an organization settles on target security levels, foundational requirements can help further specify requirements based on the seven foundational security functions \(FRs\). The ISA/IEC 62443 framework includes:

- **System Requirements (SRs)**: Detailed in Part 3-3, these are guidelines for those shaping the system's overall architecture.
- **Component Requirements (CRs)**: Outlined in Part 4-2, they cater to designers focusing on individual components.

Both system and component designers reference these standards, ensuring the final product's security aligns with what the asset owner's requirements. This methodology not only bolsters the product's defense against specific threat levels but also optimizes resource utilization among stakeholders. As a side note, every FR from Part 1-1 is paired with four distinct security levels, which trace back to standards set in Parts 3-3 and 4-2. For simplicity in cross-referencing, CRs are numerically aligned with their corresponding SRs.

Component Requirements

Part 4-2 extends the SRs from Part 3-3 by introducing CRs tailored for a variety of IACS components. These components fall under four broad categories.

Generic	Specific
Component Requirements (CR)	Software Applications
	Embedded Devices
	Host Devices
	Network Devices

While a majority of Part 4-2's criteria are generic and apply uniformly across categories, there are exceptions. Unique, component-specific stipulations are clearly signposted, with exhaustive details available in dedicated clauses. For details, consult the original standards.

Requirement Enhancements

CRs may contain one or more requirement enhancements (RE). REs are additional requirements attached to CRs that add additional conditions to accommodate higher security levels.

Applying FR 1: User Identification and Authentication

FR 1 codifies the principle that all users—humans, software processes, or devices—must first be identified and authenticated before accessing systems or assets.

Recognizing the need to verify different kinds of users, FR 1 uses the following CRs:

- **CR 1.1** focuses on human users.
- **CR 1.2** addresses software processes and devices.

Identification vs. Authentication: Consider a person's ID card. While the card identifies its owner, can someone else misuse it? Certainly. Here, the distinction between 'identifying' (matching a person to an ID card) and 'authenticating' (confirming the card holder's authenticity) becomes crucial. Each process has distinct methods and requirements.

Understanding CR and RE in Determining Security Levels: CR represents foundational requirements, whereas RE (related entity) accounts for advanced needs. Together, they define the security capacity of a component. Each component's security level, according to FR, ranges from 0 (no requirements) to 4.

For instance:

- **Security Level 1**: Implementing basic identification and authentication for all human users.
- **Security Level 2**: Incorporates RE1 - uniquely identify and authenticate users, like using ID cards for employees.
- **Security Level 3**: Engages RE2 - multifactor authentication.

Multifactor Authentication Unraveled: Typically, this methodology hinges on:

1. **Knowledge**: Passwords or PINs.
2. **Possession**: Devices like smartphones or security keys.
3. **Inherence**: Biometrics such as fingerprints.

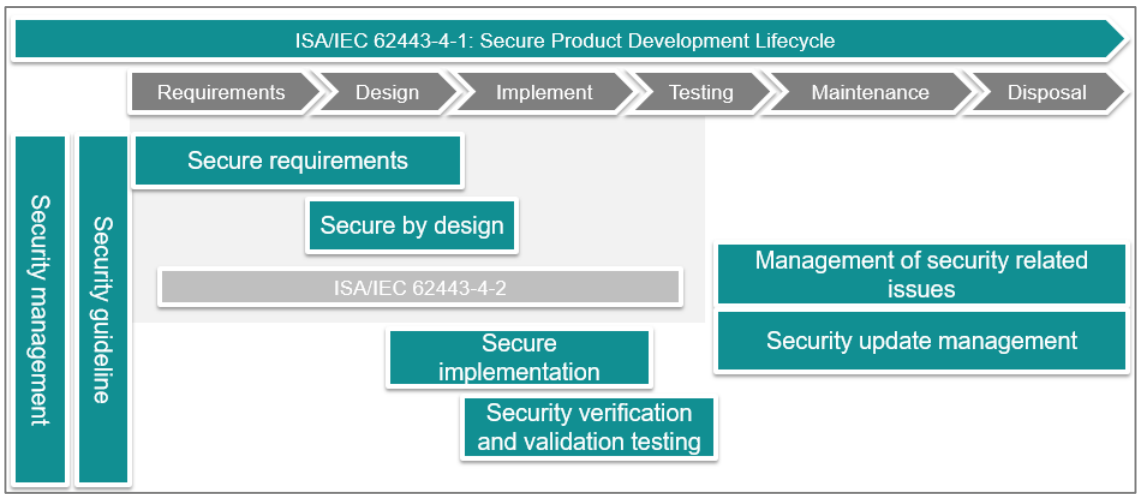
To achieve Level 3, a combination of at least two of these factors is essential.

Security Level	Attack Type				
	Example Threat Actor	Violation Type	Means	Resource Level	Motivation
SL-1	• Ordinary user	Coincidental	N/A	N/A	N/A
SL-2	• Entry-level hacker	Intentional	Simple	Low	Low
SL-3	• Terrorist Organization • Organized crime	Intentional	Sophisticated	Moderate	Moderate

Security Level	Attack Type				
	Example Threat Actor	Violation Type	Means	Resource Level	Motivation
SL-4	• Nation state	Intentional	Sophisticated	Extended	High

Product Lifecycle and Security

Component security plays a role throughout the product lifecycle



How Moxa applies ISA / IEC 62443-4-1

Our commitment to security includes to adhering to the ISA/IEC 62443-4-1 standard, considering security at each stage of the product's lifecycle. This includes the safeguarding of our corporate network, keys, secure design and implementation proficiencies, testing processes, and post-sales services. Our approach involves extensive training and certification of all team members associated with product design, execution, and assistance. Moreover, we offer robust support mechanisms like vulnerability handling and patch management.

Component Security with IEC 62443-4-2

IEC 62443-4-2 serves as a guide for product suppliers, helping us decipher the specific security capability benchmarks for control system components. This standard not only clarifies which requirements should be assigned but also pinpoints those that must be

integral to the components. The fusion of these component requirements with their enhancement requirements defines the component's target security level.

Chapter 5

Appendix

Advanced Mode Settings

This table shows settings that are only available in **Advanced Mode**.

Location in UI	Advanced Mode Items
System > Management Interface > User Interface	• Moxa Service settings
System > Time > Time Synchronization - General	If **Clock Type** is **Transparent Clock**: • BMCA setting
Port > Link Aggregation	• Link Algorithm setting • Link Aggregation Port List
Port > PoE - Scheduling	• PoE - Scheduling tab
Layer 2 Switching > VLAN - Settings **Layer 2 Switching > VLAN - Status**	• Forbidden Port setting
Layer 2 Switching > QoS > Ingress Rate Limit	• Type setting • CBS setting • EBS setting • Mode setting • Conform Action setting • Exceed Action setting
Layer 2 Switching > QoS > Egress Shaper	• CBS setting
Layer 2 Switching > Multicast > IGMP Snooping - VLAN Settings	• Startup Query Interval information • Startup Query Count information • Other Query Present Interval information
Layer 2 Switching > Multicast > Static Multicast	• Forbidden Port setting
IP Configuration	• IPv6 settings
Redundancy > Spanning Tree - General	If **STP Mode** is **STP/RSTP**: • Link Type setting
Redundancy > Spanning Tree - Guard	• Root Guard setting • Loop Guard setting

Location in UI	Advanced Mode Items
Redundancy > Spanning Tree - Status	• Root Inconsistency information • Loop Inconsistency information
Security > Network Security > IEEE 802.1X - General	• Reauthentication Period setting • Server Timeout setting • Supp Timeout setting • Tx Period setting
Security > Network Security > Access Control List - Settings	If **Rule Type** is **Permit**: • Rate Limit Type settings

CEF Message Format for Event Logs

The CEF message format for Moxa switch event logs contains the following information:

`CEF: Version|Device Vendor|Device Product|Device Version|CEF Event ID|Event Name|Severity|Extension (Key + Value)`

Example CEF message:

`CEF:0|Moxa|RKS-G4028-L3-4GS-HV-T|v6.0 Build 2025_1201_1045|0x4000040e|Topology change (Turbo Ring)|5|index=1`

Version

This indicates the CEF Specification version used for the message.

Device Vendor

This shows the vendor of the device the message comes from, e.g., `MOXA`.

Device Product

This shows the product name of the device the message comes from, e.g., `MDS-G4028`, `TN-4500B`.

Device Version

This shows the version number of the device the message comes from, e.g., `v5.0 Build 2023_1206_1706`.

CEF Event ID

The CEF event ID definition has a length of 8 bytes, with different bytes used to carry specific information.

To see which event corresponds with a specific CEF Event ID, refer to Event Log Descriptions.

Bytes 0-1: OS Identification

The first two bits are used for OS encoding:

- `01` = MX-NOS
- `10` and `11` = reserved
- The remaining 6 bits are currently undefined and reserved.

For example, MX-NOS would be `01` (MX-NOS) + `000000` (reserved bits) = `01000000`

Converting this binary code to hexadecimal will result in **0x40**.

Bytes 2-3: Revision

This field indicates the revision number. The first version is **0x00**. This field should be incremented if there are changes to the event's severity or name.

Bytes 4-5: Classification System (Feature ID)

This field contains the Feature ID.

Menu Tree Title	Feature ID
System	0x00
Port	0x01
Layer 2 Switching	0x02
IP Configuration	0x03
Redundancy	0x04
Network Service	0x05
Security	0x06
Diagnostics	0x07

Menu Tree Title	Feature ID
Industrial	0x08
Routing	0x10

Bytes 6-7: Sequence Number

This field contains the sequential number for the event. The first ID is **0x00**.

Event Name

This field refers to the name of the event.

Severity

This field describes the severity of the event, with higher numbers indicating higher severity.

Standard syslog severity levels are mapped to the Common Event Format (CEF) severity levels as follows:

Syslog Severity	CEF Severity	Description
0	10	Emergency
1	8	Alert
2	7	Critical
3	6	Error
4	5	Warning
5	4	Notice
6	1	Informational
7	0	Debug

Extension (Key + Value)

This contains additional information that follows the **Extension (Key + Value)** format, based on Chapter 2 of *Micro Focus Security ArcSight Common Event Format Version 25*.

For parameters that do not have a proper key name in the above document, the Moxa defined CEF key names are as follows:

CEF Key Name	Full Name	Data Type	Length	Meaning
dportIndex	destinationPortIndex	String	7	The index of target (destination) ports: the index of a port or port-channel.
dportType	destinationPortType	String	15	The type of target (destination) ports: Port or port-channel.
drole	destinationRole	String	31	The role of the target ports or device in the protocol,. e.g., for RSTP, the port roles include root port, destination port, alternate port, backup port, and disabled port.
dstate	destinationState	String	15	The state of the targeting systems/ports/functions. One state example for interfaces is up or down.
index	indexValue	Integer	N/A	The alphabetical list of names, subjects, etc. related to the pages on which they are mentioned. e.g., Index of module, index of power input, index of port
intfIp	interfaceIP	IPv4 Address	N/A	The interface IP address. In Layer 3 switches, each interface has its own IP address.
intfName	interfaceName	String	15	The interface name used to identify an L3 interface. e.g., vlan1, vlan10
intVlan	interfaceVlan	Integer	N/A	The interface VLAN. In Layer 3 switches, each interface has its own VLAN ID.
method	method	String	15	The media used for file operations such as backup, restore or firmware upgrade. e.g., HTTP/HTTPS, SFTP, TFTP, ABC-02, ABC-03
moduleType	TypeOfModule	String	7	The type of module responsible for generating the event. e.g., Management module(MGMT)/Power Module(PWR1 or PWR2)

CEF Key Name	Full Name	Data Type	Length	Meaning
netAddr	networkAddress	String	31	The range of an IP network.
nodeType	IreRemNodeType	String	15	Doubly Attached Node (DAN) type used in PRP/HSR, as indicated in the received supervision frame.
sportIndex	sourcePortIndex	String	7	The index of ports responsible for generating the event: the index of a port or port-channel.
sportType	sourcePortType	String	15	The type of ports responsible for generating the event: Port or port-channel.
srole	sourceRole	String	31	The role of the ports or device in the protocol responsible for generating the event. e.g., for RSTP, the port roles include root port, destination port, alternate port, backup port, and disabled port.
sstate	sourceState	String	15	The state of the systems/ports/functions responsible for generating the event. One state example for interfaces is up or down.
threshold	thresholdValue	Floating Point	N/A	The threshold value that must be reached to trigger an action.
value	valueOrNumber	Floating Point		A number value. e.g., power value, number of packets, priority value
vlanId	vlanID	Integer	N/A	The ID of the VLAN.

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
ODVA	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
MOXA	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)	**0x3DF**, the vendor ID of Moxa is 991.
2	Get	Device Type		UINT (16)	**0x2C**, “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		✓	Set_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)
Output	1	18
Input	50	16
Configuration	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
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
Input	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							
Output	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
Power Source Status	Base Switch Object	1	Power Source	4
Global Admin State			Global Port Admin State	7
Global Link Status			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
1	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)	Number of Forward_Open service requests received. A device may reject a set request to this attribute, using General Status Code **0x09** (Invalid Attribute Value), if the attribute value sent is not zero. (Vol1_3.33 3-5.2 Instance Attributes)

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
	Scheduled (2)	47	Safety I/O I/O
	High (1)	43	I/O
	Low (0)	31	No recommendation at present
• CIP UCMM **• CIP class 2 / 3** **• All other EtherNet / IP Encapsulation messages**	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)	Status of switch power source. Bits 0-1: State of the Power Source 1. 00 = Not Present (Power source not present in switch) 01 = Not Powered (Power source present but not powered) 10 = Faulted(internal) (Power source present but faulted) 11 = Powered and ok (Power source present, powered, and OK) Bits 2-3: State of the Power Source 2. The values are same as bits 0-1. Bits 4-5: State of the Power Source 3. The values are same as bits 0-1. Bits 6-7: State of the Power Source 4. The values are same as bits 0-1. Bits 8-9: State of the Power Source 5. The values are same as bits 0-1. Bits 10-11: State of the Power Source 6. The values are same as bits 0-1. Bits 12-13: State of the Power Source 7. The values are same as bits 0-1. Bits 14-15: State of the Power Source 8. The values are same as bits 0-1.
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)	Switch existing port. 0 = Port Absent 1 = Port Present
7	Get	Global Port Admin State	ARRAY OF DWORD (32)	Port Admin State. 0 = Port Disabled 1 = Port Enabled
8	Get	Global Port Link Status	ARRAY OF DWORD (32)	Ports Link Status. 0 = Link Inactive (Down) 1 = Link Active (Up) Bit 0-31: Port 0-31 Link status.

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.
6	Get/Set	Host Name		STRING	Host name. ASCII characters. Maximum length is 64 characters.
13	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
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		✓	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
0	Ethernet Link class
1	1st switch port
2	2nd switch port
3	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
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.
100	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.
6	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.)
10	Get	Interface Label		SHORT_STRING	Port description. Maximum length is 64 characters.
11	Get	Interface Capability		(Struct.)	Indication of capabilities of the interface

	Capability Bits	DWORD (32)	Interface capabilities, other than speed/duplex. Bit 0: Manual Setting Requires Reset 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. 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. Bit 1: Auto-Negotiate Value 0: Not support AN Value 1: Support AN Bit 2: Auto-MDIX Value 0: Not support auto MDIX Value 1: Support auto MDIX Bit 3: Manual Speed/Duplex Value 0: Not support manual setting of speed/duplex. Value 1: Supports manual setting of speed/duplex via the Interface Control attribute (#6) Bit 4 to 31: Reserved, all zero

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.
			HCOutOctets	ULINT (64)	Octets sent on the interface. This counter is a 64-bit version of Out Octets.
			HCOutUcastPkts	ULINT (64)	Unicast packets sent on the interface. This counter is a 64-bit version of Out Ucast Packets.
			HCOutMulticastPkts	ULINT (64)	Multicast packets sent on the interface.
			HCOutBroadcastPkts	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)	Frames received that are not an integral number of octets in length and do not pass the FCS check. This counter is a 64-bit version of Alignment Errors.
			HCStatsFCSErrors	ULINT (64)	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.
			HCStatsInternalMacTransmitErrors	ULINT (64)	Frames for which transmission fails due to an internal MAC sublayer transmit error. This counter is a 64-bit version of MAC Transmit Errors.
			HCStatsFrameTooLongs	ULINT (64)	Frames received that exceed the maximum permitted frame size. This counter is a 64-bit version of Frame Too Long Errors.
			HCStatsInternalMacReceiveErrors	ULINT (64)	Frames for which reception on an interface fails due to an internal MAC sublayer receive error. This counter is a 64-bit version of MAC Receive Errors.

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	Indicates the status of link auto-negotiation 0 = Auto-negotiation in progress. 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. 2 = Auto negotiation failed but detected speed. Duplex was defaulted. Default value is product-dependent; recommended default is half duplex. 3 = Successfully negotiated speed and duplex. 4 = Auto-negotiation not attempted. Forced speed and duplex.
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 BTYE (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** Actual Moxa supported transmit interval range is 5 to 32768.
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** Actual Moxa supported transmit interval range is 5 to 32768.

Attr ID	Access Rule	Name	(Struct.)	Data Type	Description
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
2	Get	MAC Address		ETH_MAC_ADDR	The MAC address will be set by the first occurrence of a MAC ID that exists in the following list: 1. The CIP MAC Address (TLV Type = 127, Subtype = 2) 2. The Chassis ID (TLV Type = 1) only if subtype = 2 3. The Port ID (TLV Type = 2) only if subtype = 3 4. All zero

Attribute ID	Access Rule	Name	(Struct.)	Data Type	Description
3	Get	Interface Label		SHORT_STRING	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: 1. The CIP Interface Label (TLV Type = 127, Subtype = 1) 2. The Chassis ID (TLV Type = 1) only if subtype = 6 3. The Port ID (TLV Type = 2) only if subtype = 5 4. A null string
4	Get	Time to Live		UINT (16)	The number of seconds the neighboring information is to be considered valid. 0 = Reserved 1-65535 = Time To Live (in seconds)
5	Get	System Capabilities TLV		(Struct.)	A structure that contains bitmaps of both the supported and enabled capabilities of the neighboring device.

Attribute ID	Access Rule	Name	(Struct.)	Data Type	Description
			System Capabilities	WORD (16)	The capabilities which the neighboring device supports based on currently loaded firmware. 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 **Note** EtherNet/IP Bridged multiport neighboring devices are expected to assert high bits 0 & 2.

Attribute ID	Access Rule	Name	(Struct.)	Data Type	Description
			Enabled Capabilities	WORD (16)	The capabilities currently enabled on the neighboring device. 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 **Note** EtherNet/IP Bridged multiport neighboring devices are expected to assert high bits 0 & 2.
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)	The IP address shall be set to a valid Class A, B, or C address. And shall not be set to all zeros or the loopback address (127.0.0.1).
7	Get	CIP Identification		(Struct.)	The CIP Identification TLV of the neighboring device, if present. Set by the CIP Identification TLV (TLV Type = 127, Subtype = 09), if present. Otherwise 0

Attribute ID	Access Rule	Name	(Struct.)	Data Type	Description
			Vendor ID	UINT (16)	Vendor ID
			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.
8	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)
2	Get	L2 Redundancy	USINT (8)	Bit mask of device roles. Bit 0: RSTP 0 = RSTP Disabled 1 = RSTP Enabled Bit 1: MSTP 0 = MSTP Disabled 1 = MSTP Enabled Bit 2: Turbo Chain 0 = Turbo Chain Disabled 1 = Turbo Chain Enabled Bit 3: Turbo Ring v2 0 = Turbo Ring v2 Disabled 1 = Turbo Ring v2 Enabled Bit 4: Dual-Homing 0 = Dual-Homing Disabled 1 = Dual-Homing Enabled Bit 5: MRP 0 = MRP Disabled 1 = MRP Enabled

Attr ID	Access Rule	Name	Data Type	Description
3	Get	Relay Alarm Status	USINT (8)	Relay alarm event-triggered status. When Relay alarm is triggered, value will change from 0x0 to 0x1. Bit 0: Relay (MGMT-Relay) alarm status 0 = Alarm doesn't trigger. 1 = Alarm triggered. Bit 1: PWR1-Relay alarm status 0 = Alarm doesn't trigger. 1 = Alarm triggered. Bit 2: PWR2-Relay alarm status 0 = Alarm doesn't trigger. 1 = Alarm triggered.
4	Get/Set	Cold Start	USINT (8)	System cold start event notification. (Bit 1 should call MGMT-Relay if device support more than 1 relay. Bit 2-3 depends on device supported relay number.) Bit 0: Event notification enable. 0 = Disabled 1 = Enabled Bit 1: Relay (MGMT-Relay) alarm enable. 0 = Disabled 1 = Enabled Bit 2: PWR1-Relay alarm enable. 0 = Disabled 1 = Enabled Bit 3: PWR2-Relay alarm enable. 0 = Disabled 1 = Enabled

Attr ID	Access Rule	Name	Data Type	Description
5	Get/Set	Warm Start	USINT (8)	System warm start event notification. (Bit 1 should call MGMT-Relay if device support more than 1 relay. Bit 2-3 depends on device supported relay number.) Bit 0: Event notification enable. 0 = Disabled 1 = Enabled Bit 1: Relay (MGMT-Relay) alarm enable. 0 = Disabled 1 = Enabled Bit 2: PWR1-Relay alarm enable. 0 = Disabled 1 = Enabled Bit 3: PWR2-Relay alarm enable. 0 = Disabled 1 = Enabled
6	Get/Set	Redundant port health check fail	USINT (8)	Redundant port health check fail. (Bit 1 should call MGMT-Relay if device support more than 1 relay. Bit 2-3 depends on device supported relay number.) Bit 0: Event notification enable. 0 = Disabled 1 = Enabled Bit 1: Relay (MGMT-Relay) alarm enable. 0 = Disabled 1 = Enabled Bit 2: PWR1-Relay alarm enable. 0 = Disabled 1 = Enabled Bit 3: PWR2-Relay alarm enable. 0 = Disabled 1 = Enabled

Attr ID	Access Rule	Name	Data Type	Description
7	Get/Set	PD over current	USINT (8)	Current of port has exceeded the safety limit. (Bit 1 should call MGMT-Relay if device support more than 1 relay. Bit 2-3 depends on device supported relay number.) Bit 0: Event notification enable. 0 = Disabled 1 = Enabled Bit 1: Relay (MGMT-Relay) alarm enable. 0 = Disabled 1 = Enabled Bit 2: PWR1-Relay alarm enable. 0 = Disabled 1 = Enabled Bit 3: PWR2-Relay alarm enable. 0 = Disabled 1 = Enabled
8	Get/Set	PD no response	USINT (8)	The device connected to this port is not responding to the PD failure check. (Bit 1 should call MGMT-Relay if device support more than 1 relay. Bit 2-3 depends on device supported relay number.) Bit 0: Event notification enable. 0 = Disabled 1 = Enabled Bit 1: Relay (MGMT-Relay) alarm enable. 0 = Disabled 1 = Enabled Bit 2: PWR1-Relay alarm enable. 0 = Disabled 1 = Enabled Bit 3: PWR2-Relay alarm enable. 0 = Disabled 1 = Enabled

Attr ID	Access Rule	Name	Data Type	Description
9	Get/Set	Power On	USINT (8)	Power supply on event notification. (Bit 1 should call MGMT-Relay if device support more than 1 relay. Bit 2-3 depends on device supported relay number.) Bit 0: Event notification enable. 0 = Disabled 1 = Enabled Bit 1: Relay (MGMT-Relay) alarm enable. 0 = Disabled 1 = Enabled Bit 2: PWR1-Relay alarm enable. 0 = Disabled 1 = Enabled Bit 3: PWR2-Relay alarm enable. 0 = Disabled 1 = Enabled
10	Get/Set	Power Off	USINT (8)	Power supply off event notification. (Bit 1 should call MGMT-Relay if device support more than 1 relay. Bit 2-3 depends on device supported relay number.) Bit 0: Event notification enable. 0 = Disabled 1 = Enabled Bit 1: Relay (MGMT-Relay) alarm enable. 0 = Disabled 1 = Enabled Bit 2: PWR1-Relay alarm enable. 0 = Disabled 1 = Enabled Bit 3: PWR2-Relay alarm enable. 0 = Disabled 1 = Enabled

Attr ID	Access Rule	Name	Data Type	Description
11	Get/Set	DI on	USINT (8)	Digital input on event notification. (Bit 1 should call MGMT-Relay if device support more than 1 relay. Bit 2-3 depends on device supported relay number.) Bit 0: Event notification enable. 0 = Disabled 1 = Enabled Bit 1: Relay (MGMT-Relay) alarm enable. 0 = Disabled 1 = Enabled Bit 2: PWR1-Relay alarm enable. 0 = Disabled 1 = Enabled Bit 3: PWR2-Relay alarm enable. 0 = Disabled 1 = Enabled
12	Get/Set	DI off	USINT (8)	Digital input off event notification. (Bit 1 should call MGMT-Relay if device support more than 1 relay. Bit 2-3 depends on device supported relay number.) Bit 0: Event notification enable. 0 = Disabled 1 = Enabled Bit 1: Relay (MGMT-Relay) alarm enable. 0 = Disabled 1 = Enabled Bit 2: PWR1-Relay alarm enable. 0 = Disabled 1 = Enabled Bit 3: PWR2-Relay alarm enable. 0 = Disabled 1 = Enabled

Attr ID	Access Rule	Name	Data Type	Description
13	Get/Set	Port On	USINT (8)	Port link up event notification. (Bit 1 should call MGMT-Relay if device support more than 1 relay. Bit 2-3 depends on device supported relay number.) Bit 0: Event notification enable. 0 = Disabled 1 = Enabled Bit 1: Relay (MGMT-Relay) alarm enable. 0 = Disabled 1 = Enabled Bit 2: PWR1-Relay alarm enable. 0 = Disabled 1 = Enabled Bit 3: PWR2-Relay alarm enable. 0 = Disabled 1 = Enabled
14	Get/Set	Port Off	USINT (8)	Port link down event notification. (Bit 1 should call MGMT-Relay if device support more than 1 relay. Bit 2-3 depends on device supported relay number.) Bit 0: Event notification enable. 0 = Disabled 1 = Enabled Bit 1: Relay (MGMT-Relay) alarm enable. 0 = Disabled 1 = Enabled Bit 2: PWR1-Relay alarm enable. 0 = Disabled 1 = Enabled Bit 3: PWR2-Relay alarm enable. 0 = Disabled 1 = Enabled

Attr ID	Access Rule	Name	Data Type	Description
15	Get/Set	Port shutdown by Port Security	USINT (8)	Port shutdown by Port Security event notification. (Bit 1 should call MGMT-Relay if device support more than 1 relay. Bit 2-3 depends on device supported relay number.) Bit 0: Event notification enable. 0 = Disabled 1 = Enabled Bit 1: Relay (MGMT-Relay) alarm enable. 0 = Disabled 1 = Enabled Bit 2: PWR1-Relay alarm enable. 0 = Disabled 1 = Enabled Bit 3: PWR2-Relay alarm enable. 0 = Disabled 1 = Enabled
16	Get/Set	Port shutdown by Rate Limit	USINT (8)	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.) Bit 0: Event notification enable. 0 = Disabled 1 = Enabled Bit 1: Relay (MGMT-Relay) alarm enable. 0 = Disabled 1 = Enabled Bit 2: PWR1-Relay alarm enable. 0 = Disabled 1 = Enabled Bit 3: PWR2-Relay alarm enable. 0 = Disabled 1 = Enabled

Attr ID	Access Rule	Name	Data Type	Description
17	Get/Set	Port recovered by Rate Limit	USINT (8)	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.) Bit 0: Event notification enable. 0 = Disabled 1 = Enabled Bit 1: Relay (MGMT-Relay) alarm enable. 0 = Disabled 1 = Enabled Bit 2: PWR1-Relay alarm enable. 0 = Disabled 1 = Enabled Bit 3: PWR2-Relay alarm enable. 0 = Disabled 1 = Enabled
18	Get/Set	Fiber Check Warning	USINT (8)	Fiber check warning event notification. (Bit 1 should call MGMT-Relay if device support more than 1 relay. Bit 2-3 depends on device supported relay number.) Bit 0: Event notification enable. 0 = Disabled 1 = Enabled Bit 1: Relay (MGMT-Relay) alarm enable. 0 = Disabled 1 = Enabled Bit 2: PWR1-Relay alarm enable. 0 = Disabled 1 = Enabled Bit 3: PWR2-Relay alarm enable. 0 = Disabled 1 = Enabled

Attr ID	Access Rule	Name	Data Type	Description
19	Set	Relay Alarm Cut-off	USINT (8)	Cut off the relay alarm. (Bit 0 should call MGMT-Relay if device support more than 1 relay. Bit 1-2 depends on device supported relay number.) Bit 0: Relay (MGMT-Relay) 0 = Don't cut-off relay 1 = Cut-off relay Bit 1: PWR1-Relay 0 = Don't cut-off relay 1 = Cut-off relay Bit 2: PWR2-Relay 0 = Don't cut-off relay 1 = Cut-off relay
20	Set	Reset MIB Count	USINT (8)	Reset port MIB counters. (Ethernet Link object's attributes 4-5 and 12-13.) Any value indicates to reset port MIB counter.
21	Set	Reset Device	USINT (8)	Reboot and reset to default 0 = Reserved. 1 = Reboot the device 2 = Reset to default

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

CIP Tags

This page shows the tags related to CIP objects. These tags correspond to the object's attributes.

Tags for Identity Objects

Data Type: MOXA_Identity_Object

Name	Data Type	Description
Vendor ID	INT	ODVA Vendor ID. Moxa=0x3DF
Device Type	INT	0x2C, "Managed Ethernet Switch"
Product Code	INT	Refer to the Product Code Table. Example: RKS-G4028-4GT-HV = 0x1301
Major Revision	SINT	The structure member, major
Minor Revision	SINT	The structure member, minor
Status	INT	Summary status of the device
Serial Number	DINT	Switch serial number
Product Name	STRING	Switch model name
Assigned Name	MOXA_String	User assigned switch name
Geographic Location	MOXA_String	User assigned switch location

Tags for TCPIP Objects

Data Type: MOXA_TCPIP_Interface_Object

Name	Data Type	Description
Status	DINT	Interface status

Name	Data Type	Description
Configuration Capability	DINT	Interface capability flags
Configuration Control	DINT	Interface control flags
Path Size	INT	Size of Path
Object Path 1	INT	Logical segments identifying the physical link object
Object Path 2	INT	Logical segments identifying the physical link object
IP Address	DINT	The device's IP address
Network Mask	DINT	The device's network mask
Gateway Address	DINT	Default gateway address
Name Server 1	DINT	Primary name server
Name Server 2	DINT	Secondary name server
Domain Name	STRING	Default domain name
Host Name	STRING	Host name
Encapsulation Inactivity Timeout	INT	Number of seconds of inactivity before TCP connection closes.

Tags for Ethernet Link Objects

Data Type: MOXA_Ethernet_Link_Object

Name	Data Type	Description
Interface Speed	DINT	Interface speed currently in use. Speed in Mbps (e.g., 0, 10, 100, 1000, etc.)
Interface Flags	MOXA_Interface_Object_Flags_v0	Interface status flags
Physical Address	SINT[6]	MAC layer address
InOctets	DINT	Octets received on the interface

Name	Data Type	Description
InUcastPackets	DINT	Unicast packets received on the interface
InNucastPackets	DINT	Non-unicast packets received on the interface
InDiscards	DINT	Inbound packets received on the interface but discarded
InErrors	DINT	Inbound packets that contain errors (does not include In Discards)
OutOctets	DINT	Octets sent on the interface
OutUcastPackets	DINT	Unicast packets sent on the interface
OutNucastPackets	DINT	Non-unicast packets sent on the interface
OutDiscards	DINT	Outbound packets discarded
OutErrors	DINT	Outbound packets that contain errors
Alignment Errors	DINT	Frames received that are not an integral number of octets in length
FCS Errors	DINT	Frames received that do not pass the FCS check
Single Collisions	DINT	Successfully transmitted frames which experienced exactly one collision
Multiple Collisions	DINT	Successfully transmitted frames which experienced more than one collision
SQE Test Errors	DINT	Number of times SQE test error message is generated
Deferred Transmissions	DINT	Frames for which first transmission attempt is delayed because the medium is busy
Late Collisions	DINT	Number of times a collision is detected later than 512 bit-times into the transmission of a packet

Name	Data Type	Description
Excessive Collisions	DINT	Frames for which transmission fails due to excessive collisions
MAC Transmit Errors	DINT	Frames for which transmission fails due to an internal MAC sublayer transmit error
Carrier Sense Errors	DINT	Times that the carrier sense condition was lost or never asserted when attempting to transmit a frame
Frame Too Long	DINT	Frames received that exceed the maximum permitted frame size
MAC Receive Errors	DINT	Frames for which reception on an interface fails due to an internal MAC sublayer receive error
Control Bits	INT	0 Auto-negotiate 0 indicates 802.3 link auto-negotiation is disabled. 1 indicates auto-negotiation is enabled
Forced Interface Speed	INT	Speed at which the interface shall be forced to operate. Speed in Mbps (10, 100, 1000, etc.)
Interface Label	STRING	Label like "TX5"
Capability Bits	DINT	Capability Bits contains an array of bits that indicate whether the interface supports capabilities such as auto-negotiation and auto-MDIX.
Speed Duplex Array	SINT	Number of elements
Interface Speed Duplex Capability	MOXA_Interface	The total number of octets received on the interface. This counter is a 64-bit version of In Octets.
HC InOctets	LINT	Unicast packets received on the interface. This counter is a 64-bit version of In Ucast Packets.
HC InMulticastPkts	LINT	Multicast packets received on the interface.

Name	Data Type	Description
HC InBroadcastPkts	LINT	Broadcast packets received on the interface.
HC OutOctets	LINT	Octets sent on the interface. This counter is a 64-bit version of Out Octets.
HC OutUcastPkts	LINT	Unicast packets sent on the interface. This counter is a 64-bit version of Out Ucast Packets.
HC OutMulticastPkts	LINT	Multicast packets sent on the interface.
HC OutBroadcastPkts	LINT	Broadcast packets sent on the interface.
HC StatsFCSErrors	LINT	Frames received that are not an integral number of octets in length and do not pass the FCS check. This counter is a 64-bit version of Alignment Errors.
HC StandardMacTransmitErrors	LINT	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.
HC StatsFrameTooLong	LINT	Frames for which transmission fails due to an internal MAC sublayer transmit error. This counter is a 64-bit version of MAC Transmit Errors.
HC StatsInternalMacReceiveErrors	LINT	Frames received that exceed the maximum permitted frame size. This counter is a 64-bit version of Frame Too Long Errors.
HC StatsSymbolErrors	LINT	Frames for which reception on an interface fails due to an internal MAC sublayer receive error. This counter is a 64-bit version of MAC Receive Errors.
Port State	LINT	Switch port state.
Media Type	STRING	Port media type.

Name	Data Type	Description
Traffic Storm Control	SINT	Traffic storm control enabled.
Port On Event	SINT	Registered port for port on event notification.
Port Off Event	SINT	Registered port for port off event notification.
Port Shutdown by PSEC Event	SINT	Registered port for port shut down by Port Security event notification.
Port Shutdown by Rate Limit Event	SINT	Registered port for port shut down by Rate Limit event notification.
Port Recovery by Rate Limit Event	SINT	Registered port for port recovered by Rate Limit event notification.
Fiber Check Warning Event	SINT	Registered port for fiber check warning event notification.

Tags for Moxa Networking Objects

Data Type: MOXA_Networking_Object

Name	Data Type	Description
System Firmware Version	DINT	Switch firmware version
System Fault Status	DINT	Switch fault status
Switch Port Number	SINT	Switch max port number
Port Exist	DINT[2]	Switch per port exist
Port Enable	DINT[2]	Switch per port exist 0:Enable 1:Disable
Port Link Status	DINT[2]	Switch per port link status
IGMP Snooping	SINT	IGMP snooping enable: 0: Disable 1: Enable

Name	Data Type	Description
Query Interval	DINT	Query Interval range from 20~600 sec
IGMP Enhanced Mode	SINT	IGMP enhanced mode 0: Disable (default) 1: Enable
Relay 1	SINT	Override relay warning setting 0: Disable (default) 1: Enable
Relay 2	SINT	Override relay warning setting 0: Disable (default) 1: Enable
Power 1 Relay Warning	SINT	Power input 1 failure (on à off) 0: Disable (default) 1: Enable(relay 1) 2: Enable(relay 2)
Power 2 Relay Warning	SINT	Power input 2 failure (on à off) 0: Disable (default) 1: Enable(relay 1) 2: Enable(relay 2)
DI 1 Off Relay Warning	SINT	DI 1 (off) 0: disable (default) 1: Enable(relay 1) 2: Enable(relay 2)
DI 1 On Relay Warning	SINT	DI 1 (on) 0: Disable (default) 1: Enable(relay 1) 2: Enable(relay 2)
DI 2 Off Relay Warning	SINT	DI 2 (off) 0: Disable (default) 1: Enable(relay 1) 2: Enable(relay 2)

Name	Data Type	Description
DI 2 On Relay Warning	SINT	DI 2 (on) 0: Disable (default) 1: Enable(relay 1) 2: Enable(relay 2)
Turbo Ring Break Relay Warning	SINT	Turbo Ring Break (Ring Master Only) 0: Disable (default) 1: Enable (relay 1) 2: Enable (relay 2)
CPU Usage	SINT	Percent of usage (0-100)
Device Up Time	DINT	Number of seconds since device was powered up
Reset Mib Counter	SINT	Reset port MIB counters
Redundant Device Mode	DINT	Bit 0: RSTP, Bit 1: Turbo Ring, Bit 2: Turbo Ring v2, Bit 3: Turbo Chain, Bit 4: MSTP
Reset Device	SINT	1: restart the device 2: reset to default

Tags for Moxa Base Switch Objects

Data Type: MOXA_Base_Switch_Object

Name	Data Type	Description
Device Up Time	DINT	Time since device was powered up.
Total Port Count	DINT	Number of physical available ports.
System Firmware Version	STRING	System Firmware Version.
Power Source	INT	Status of switch power source.
Port Mask Size	INT	Number of DWORDs in port array attributes.

Name	Data Type	Description
Existing Port	DINT (4)	Switch existing port.
Global Port Admin State	DINT (4)	Port Admin State.
Global Port Link Status	DINT (4)	Ports Link Status.

Pre-configured Tags in the Moxa AOI

The Moxa AOI supports all the CIP tags listed in the tables below, but in the AOI, we only preconfigure logic links between selected tags and Moxa switches.

To monitor non-configured tags, PLC programmers will need to create the links manually. Otherwise, in RSLogix 5000, the value column of these tags will display as “0”. If you experience problems creating new links, please contact Moxa technical support for assistance.

Note

For preconfigured tags, Moxa has already created the logic links between the CIP tags and Moxa Ethernet switches so RSLogix 5000 can get/set switch information correctly.

The tables below specify all preconfigured tags in Moxa AOI with a ※ mark.

Identity Object (0x01)

Pre-Configured Tags	Attribute Name
※	Vendor ID
※	Device Type
※	Product Code
※	Revision
※	Status
※	Serial Number

Pre-Configured Tags	Attribute Name
※	Product Name
	Assigned Name
	Geographic Location

Base Switch Object (0x51)

Pre-Configured Tags	Attribute Name
※	Device Up Time
※	Total Port Count
※	System Firmware Version
※	Power Source
※	Port Mask Size
※	Existing Port
※	Global Port Admin State
※	Global Port Link Status

TCP/IP Interface Object (0xF5)

Pre-Configured Tags	Attribute Name
※	Status
※	Configuration Capability
※	Configuration Control
※	Physical Link Object

Pre-Configured Tags	Attribute Name
※	Interface Configuration
※	Host Name
※	Encapsulation Inactivity Timeout

Ethernet Link Object (0xF6)

Pre-Configured Tags	Attribute Name
※	Interface Speed
※	Interface Flags
※	Physical Address
※	Interface Counters
	Media Counters
※	Interface Control
	Interface Label
	Interface Capability
	HC Interface Counters
	HC Media Counters
※	Port State
	Media Type
※	Traffic Storm Control
※	Port On event
※	Port Off event

Pre-Configured Tags	Attribute Name
※	Port shut down by Port Security event
※	Port shut down by Rate Limit event
※	Port recovered by Rate Limit event
※	Fiber Check Warning

Moxa Networking Object (0x404)

Pre-Configured Tags	Attribute Name
※	CPU Usage
※	L2 Redundancy
※	Relay Alarm Status
	Cold Start
	Warm Start
	Redundant port health check fail
	PD over current
	PD no response
	Power On
	Power Off
	DI on
	DI off
※	Port On
※	Port Off

Pre-Configured Tags	Attribute Name
※	Port shutdown by Port Security
※	Port shutdown by Rate Limit
※	Port recovered by Rate Limit
※	Fiber Check Warning
	Relay Alarm Cut-off
※	Reset MIB Count
※	Reset Device

I/O Message Object

Pre-Configured Tags	Attribute Name
※	Relay Alarm Status
※	Existing Port
※	Global Port Link Status
※	Global Port Admin State

Configuration Types

This table describes the different types of configurations that your device uses.

Configuration Type	Description
Startup Config	The configuration that is loaded when the device boots up. These settings persist even when the device is powered off.
Running Config	The configuration that is currently in use by the device. • **If auto-save is enabled**, all changes will be saved to the startup config, and will be retained when the device powers off. • **If auto-save is disabled**, any unsaved changes will be lost when the device powers off. Refer to Disable/Enable Auto Save for more information.
Factory Default Config	The pre-defined factory default configuration of your device. This configuration cannot be changed.

Event Log Descriptions

This section details the different events that can be recorded in the event log files.

Events are organized by classification.

Event log descriptions include the following information:

Severity	Severity of the event.
Event Description	Event description used for the legacy message format and the event name in the CEF message format. Double braces {{ }} indicate placeholders for event-specific text that will be provided by the device.
Classification	Classification of the event, which follows the menu tree structure in the device's web UI.
CEF Event ID (Hexadecimal)	8-byte CEF event ID for the event.
CEF Event ID (Decimal)	Decima CEF event ID for the event. This is the CEF Event ID that appears in Moxa CEF messages.
Arg1 - Arg6	Additional information for the event that appears in the Extension (Key + Value) part of the CEF message format.

1. System

1.1 Cold start

Severity	Critical
Event Description	System has performed a cold start.
Classification	System
CEF Event ID	0x40000000
CEF Description	System has performed a cold start.
Arg1	
Arg2	
Arg3	
Arg4	
Arg5	
Arg6	

1.2 Warm start

Severity	Notice
Event Description	System has performed a warm start.
Classification	System
CEF Event ID	0x40000001
CEF Description	System has performed a warm start.
Arg1	
Arg2	
Arg3	
Arg4	
Arg5	
Arg6	

1.3 Configuration change by user

Severity	Notice
Event Description	Configuration {{modules}} changed by user {{username}}. If user configure through SNMPv3: Configuration {{modules}} changed by {{username}} via snmp service.
Classification	System
CEF Event ID	0x40000002
CEF Description	Configuration {{sourceServiceName}} changed by user {{suser}}.
Arg1	sourceServiceName
Arg2	suser
Arg3	
Arg4	
Arg5	
Arg6	

1.4 Login success

Severity	Notice
Event Description	[Account: {{user_name}}] successfully logged in via {{interface}}.

Classification	System
CEF Event ID	0x40000003
CEF Description	[Account: {{suser}}] successfully logged in via {{app}}.
Arg1	suser
Arg2	app
Arg3	
Arg4	
Arg5	
Arg6	

1.5 Login failure

Severity	Warning
Event Description	[Account: {{user_name}}] failed to log in via {{interface}}.
Classification	System
CEF Event ID	0x40000004
CEF Description	[Account: {{suser}}] failed to log in via {{app}}.
Arg1	suser
Arg2	app
Arg3	
Arg4	
Arg5	
Arg6	

1.6 Login lockout

Severity	Warning
Event Description	[Account: {{user_name}}] locked due to {{failed_times}} failed login attempts.
Classification	System
CEF Event ID	0x40000005
CEF Description	[Account: {{suser}}] locked due to {{cnt}} failed login attempts.
Arg1	suser

Arg2	cnt
Arg3	
Arg4	
Arg5	
Arg6	

1.7 Account settings change

Severity	Notice
Event Description	Account settings updated for [Account: {{user_name}}].
Classification	System
CEF Event ID	0x40000006
CEF Description	Account settings {{reason}} for [Account: {{suser}}].
Arg1	reason
Arg2	suser
Arg3	
Arg4	
Arg5	
Arg6	

1.8 Configuration import

Severity	Notice
Event Description	Configuration import by {{username}} via {{method}} {{succeeded /failed}}.
Classification	System
CEF Event ID	0x40000007
CEF Description	Configuration import by {{suser}} via {{method}} {{outcome}}.
Arg1	suser
Arg2	method
Arg3	outcome
Arg4	
Arg5	

Arg6	

1.9 Configuration export

Severity	Notice
Event Description	Configuration export by {{username}} via {{method}} {{succeeded /failed}}.
Classification	System
CEF Event ID	0x40000008
CEF Description	Configuration export by {{suser}} via {{method}} {{outcome}}.
Arg1	suser
Arg2	method
Arg3	outcome
Arg4	
Arg5	
Arg6	

1.10 Password change

Severity	Notice
Event Description	Password changed for [Account: {{user_name}}].
Classification	System
CEF Event ID	0x40000009
CEF Description	Password changed for [Account: {{suser}}].
Arg1	suser
Arg2	
Arg3	
Arg4	
Arg5	
Arg6	

1.11 Power Off→On

Severity	Notice
Event Description	Power {{index}} turned on.
Classification	System
CEF Event ID	0x4000000a
CEF Description	Power {{index}} turned on.
Arg1	index
Arg2	
Arg3	
Arg4	
Arg5	
Arg6	

1.12 Power On→Off

Severity	Notice
Event Description	Power {{index}} turned off.
Classification	System
CEF Event ID	0x4000000b
CEF Description	Power {{index}} turned off.
Arg1	index
Arg2	
Arg3	
Arg4	
Arg5	
Arg6	

1.13 Sync status change

Severity	Warning

Event Description	The PTP sync status changed from {{PreSyncStatus}} to {{CurSyncStatus}}.
Classification	System
CEF Event ID	0x4000000c
CEF Description	The PTP sync status changed from {{sstate}} to {{dstate}}.
Arg1	sstate
Arg2	dstate
Arg3	
Arg4	
Arg5	
Arg6	

1.14 Grandmaster clock change

Severity	Warning
Event Description	The PTP Grandmaster clock changed from {{mac addr}} to {{mac addr}}.
Classification	System
CEF Event ID	0x4000000d
CEF Description	The PTP Grandmaster clock changed from {{smac}} to {{dmac}}.
Arg1	smac
Arg2	dmac
Arg3	
Arg4	
Arg5	
Arg6	

1.15 Port state change

Severity	Info
Event Description	The state of PTP port {{index}}/{{number}} changed from {{state}} to {{state}}.
Classification	System
CEF Event ID	0x4000000e
CEF Description	The state of PTP port {{sportIndex}} changed from {{sstate}} to {{dstate}}.

Arg1	sportIndex
Arg2	sstate
Arg3	dstate
Arg4	
Arg5	
Arg6	

1.16 PTP message with the wrong domain number

Severity	Warning
Event Description	The PTP message with the wrong domain number was received from port {{index}}/{{number}}.
Classification	System
CEF Event ID	0x4000000f
CEF Description	The PTP message with the wrong domain number was received from port {{sportIndex}}.
Arg1	sportIndex
Arg2	
Arg3	
Arg4	
Arg5	
Arg6	

1.17 Announce message with different interval

Severity	Warning
Event Description	Announce message with a different interval received on port {{index}}/{{number}}.
Classification	System
CEF Event ID	0x40000010
CEF Description	Announce message with a different interval received on port {{sportIndex}}.
Arg1	sportIndex
Arg2	
Arg3	

Arg4	
Arg5	
Arg6	

1.18 Announce timeout

Severity	Warning
Event Description	PTP port {{index}}/{{number}} Announce receipt timer timed out.
Classification	System
CEF Event ID	0x40000011
CEF Description	PTP port {{sportIndex}} Announce receipt timer timed out.
Arg1	sportIndex
Arg2	
Arg3	
Arg4	
Arg5	
Arg6	

1.19 Send message failed

Severity	Warning
Event Description	PTP port {{index}}/{{number}} failed to transmit {{Type}}.
Classification	System
CEF Event ID	0x40000012
CEF Description	PTP port {{sportIndex}} failed to transmit {{reason}}.
Arg1	sportIndex
Arg2	reason
Arg3	
Arg4	
Arg5	
Arg6	

1.20 ABC-02 insertion/removal

Severity	Notice
Event Description	ABC-02 was {{inserted/removed}}.
Classification	System
CEF Event ID	0x40000013
CEF Description	ABC-02 was {{reason}}.
Arg1	reason
Arg2	
Arg3	
Arg4	
Arg5	
Arg6	

1.21 ABC-03 insertion/removal

Severity	Notice
Event Description	ABC-03 was {{inserted/removed}}.
Classification	System
CEF Event ID	0x40000014
CEF Description	ABC-03 was {{reason}}.
Arg1	reason
Arg2	
Arg3	
Arg4	
Arg5	
Arg6	

1.22 Module insertion

Severity	Notice
Event Description	M{{index}} module was inserted.

Classification	System
CEF Event ID	0x40000015
CEF Description	M{{index}} module was inserted.
Arg1	index
Arg2	
Arg3	
Arg4	
Arg5	
Arg6	

1.23 Module removal

Severity	Notice
Event Description	M{{index}} module was removed.
Classification	System
CEF Event ID	0x40000016
CEF Description	M{{index}} module was removed.
Arg1	index
Arg2	
Arg3	
Arg4	
Arg5	
Arg6	

1.24 Power module insertion

Severity	Notice
Event Description	Power module {{index}} was inserted.
Classification	System
CEF Event ID	0x40000017
CEF Description	Power module {{index}} was inserted.
Arg1	index

Arg2	
Arg3	
Arg4	
Arg5	
Arg6	

1.25 Power module removal

Severity	Notice
Event Description	Power module {{index}} was removed.
Classification	System
CEF Event ID	0x40000018
CEF Description	Power module {{index}} was removed.
Arg1	index
Arg2	
Arg3	
Arg4	
Arg5	
Arg6	

1.26 Power module overheating risk

Severity	Warning
Event Description	Unknown power module {{module}} detected. Use a suitable power module to avoid potential overheating.
Classification	System
CEF Event ID	0x40000019
CEF Description	Unknown power module {{moduleType}} detected. Use a suitable power module to avoid potential overheating.
Arg1	moduleType
Arg2	
Arg3	
Arg4	

Arg5	
Arg6	

1.27 Unsupported power module hardware version

Severity	Notice
Event Description	Unsupported hardware revision of power module {{index}} detected.
Classification	System
CEF Event ID	0x4000001a
CEF Description	Unsupported hardware revision of power module {{index}} detected.
Arg1	index
Arg2	
Arg3	
Arg4	
Arg5	
Arg6	

1.28 Unknown module

Severity	Warning
Event Description	Failed to initialize unknown module {{index}}.
Classification	System
CEF Event ID	0x4000001b
CEF Description	Failed to initialize unknown module {{index}}.
Arg1	index
Arg2	
Arg3	
Arg4	
Arg5	
Arg6	

1.29 Hardware revision is not allowed

Severity	Error
Event Description	The hardware revision of Line Module {{index}} is not allowed.
Classification	System
CEF Event ID	0x4000001c
CEF Description	The hardware revision of Line Module {{index}} is not allowed.
Arg1	index
Arg2	
Arg3	
Arg4	
Arg5	
Arg6	

1.30 Firmware upgrade success

Severity	Notice
Event Description	Firmware successfully upgraded by {{username}}.
Classification	System
CEF Event ID	0x4000001d
CEF Description	Firmware successfully upgraded by {{suser}}.
Arg1	suser
Arg2	
Arg3	
Arg4	
Arg5	
Arg6	

1.31 Firmware upgrade failure

Severity	Warning
Event Description	Firmware upgrade failed by {{username}}.

Classification	System
CEF Event ID	0x4000001e
CEF Description	Firmware upgrade failed by {{suser}}.
Arg1	suser
Arg2	
Arg3	
Arg4	
Arg5	
Arg6	

1.32 Account log out

Severity	Notice
Event Description	[Account: {{user_name}}] logged out.
Classification	System
CEF Event ID	0x4000001f
CEF Description	[Account: {{suser}}] logged out.
Arg1	suser
Arg2	
Arg3	
Arg4	
Arg5	
Arg6	

1.33 Account removal

Severity	Notice
Event Description	[Account: {{user_name}}] removed by admin.
Classification	System
CEF Event ID	0x40000020
CEF Description	[Account: {{suser}}] removed by admin.
Arg1	suser

Arg2	
Arg3	
Arg4	
Arg5	
Arg6	

1.34 Module change

Severity	Notice
Event Description	M{{index}} module changed.
Classification	System
CEF Event ID	0x40000021
CEF Description	M{{index}} module changed.
Arg1	index
Arg2	
Arg3	
Arg4	
Arg5	
Arg6	

1.35 DIP setting failure

Severity	Notice
Event Description	DIP setting failed due to a configuration conflict.
Classification	System
CEF Event ID	0x40000022
CEF Description	DIP setting failed due to a configuration conflict.
Arg1	
Arg2	
Arg3	
Arg4	
Arg5	

Arg6	

1.36 Issue event log to syslog server

Severity	Emergency
Event Description	The system power has lost.
Classification	System
CEF Event ID	0x40000023
CEF Description	The system power has lost.
Arg1	
Arg2	
Arg3	
Arg4	
Arg5	
Arg6	

1.38 Self-healing system reboot (main function)

Severity	Info
Event Description	The system performed a self-healing reboot to resolve abnormal main function behavior.
Classification	System
CEF Event ID	0x40000025
CEF Description	The system performed a self-healing reboot to resolve abnormal main function behavior.
Arg1	
Arg2	
Arg3	
Arg4	
Arg5	
Arg6	

1.39 Self-healing system reboot (framework)

Severity	Info
Event Description	The system performed a self-healing reboot to resolve abnormal framework behavior.
Classification	System
CEF Event ID	0x40000026
CEF Description	The system performed a self-healing reboot to resolve abnormal framework behavior.
Arg1	
Arg2	
Arg3	
Arg4	
Arg5	
Arg6	

2. Port

2.1 Port link up

Severity	Notice
Event Description	Port {{index}}/{{number}} status changed to link up.
Classification	Port
CEF Event ID	0x40000100
CEF Description	Port {{sportIndex}} status changed to link up.
Arg1	sportIndex
Arg2	
Arg3	
Arg4	
Arg5	
Arg6	

2.2 Port link down

Severity	Notice
Event Description	Port {{index}}/{{number}} status changed to link down.
Classification	Port
CEF Event ID	0x40000101
CEF Description	Port {{sportIndex}} status changed to link down.
Arg1	sportIndex
Arg2	
Arg3	
Arg4	
Arg5	
Arg6	

2.3 PD power on

Severity	Notice
Event Description	Port {{number}} PD power on.
Classification	Port
CEF Event ID	0x40000103
CEF Description	Port {{sportIndex}} PD power on.
Arg1	sportIndex
Arg2	
Arg3	
Arg4	
Arg5	
Arg6	

2.4 PD power off

Severity	Notice
Event Description	Port {{number}} PD power off.
Classification	Port
CEF Event ID	0x40000104
CEF Description	Port {{sportIndex}} PD power off.
Arg1	sportIndex
Arg2	
Arg3	
Arg4	
Arg5	
Arg6	

2.5 Low input voltage

Severity	Warning
Event Description	The input voltage of the power supply dropped below 46 VDC. Adjust the voltage to between 46 and 57 VDC to meet PoE voltage requirements.
Classification	Port
CEF Event ID	0x40000105
CEF Description	The input voltage of the power supply dropped below 46 VDC. Adjust the voltage to between 46 and 57 VDC to meet PoE voltage requirements.
Arg1	
Arg2	
Arg3	
Arg4	
Arg5	
Arg6	

2.6 PD overcurrent

Severity	Error
Event Description	The current of port {{number}} exceeded the safety limit. Check the device status.

Classification	Port
CEF Event ID	0x40000106
CEF Description	The current of port {{sportIndex}} exceeded the safety limit. Check the device status.
Arg1	sportIndex
Arg2	
Arg3	
Arg4	
Arg5	
Arg6	

2.7 PD no response

Severity	Error
Event Description	Port {{number}} device is not responding to the PD failure check. Please check the device status.
Classification	Port
CEF Event ID	0x40000107
CEF Description	Port {{sportIndex}} device is not responding to the PD failure check. Please check the device status.
Arg1	sportIndex
Arg2	
Arg3	
Arg4	
Arg5	
Arg6	

2.8 Power budget overrun

Severity	Warning
Event Description	The consumed power {{power_value}} of all the PDs exceeded the maximum input power {{input_power_value}}.

Classification	Port
CEF Event ID	0x40000108
CEF Description	The consumed power {{value}} of all the PDs exceeded the maximum input power {{threshold}}.
Arg1	value
Arg2	threshold
Arg3	
Arg4	
Arg5	
Arg6	

2.9 Power detection failure

Severity	Warning
Event Description	Port {{number}} device is {{Not present/Legacy PD/802.3 af/802.3 at/Non-PD or PD short circuit/Unknown/Not applicable/802.3 bt SS/802.3 bt DS}}. {{No action required./Please enable PoE power output./Please disable PoE power output./Please select PoE output mode to Auto./Please select PoE output mode to High power./Please select PoE output mode to Force./Please enable legacy PD detection./Please raise external power supply voltage greater than 44 VDC./Please raise external power supply voltage greater than 46 VDC.}}
Classification	Port
CEF Event ID	0x40000109
CEF Description	Port {{sportIndex}} device is {{reason}}. {{msg}}
Arg1	sportIndex
Arg2	reason
Arg3	msg
Arg4	
Arg5	
Arg6	

2.10 Port link up (port channel)

Severity	Notice
Event Description	Port channel {{Channel id}} changed to link up.

Classification	Port
CEF Event ID	0x4000010a
CEF Description	Port channel {{sportIndex}} changed to link up.
Arg1	sportIndex
Arg2	
Arg3	
Arg4	
Arg5	
Arg6	

2.11 Port link down (port channel)

Severity	Notice
Event Description	Port channel {{Channel id}} changed to link down.
Classification	Port
CEF Event ID	0x4000010b
CEF Description	Port channel {{sportIndex}} changed to link down.
Arg1	sportIndex
Arg2	
Arg3	
Arg4	
Arg5	
Arg6	

2.12 Interface up

Severity	Notice
Event Description	Interface {{intfName}} status changed to up.
Classification	Port
CEF Event ID	0x4000010c
CEF Description	Interface {{intfName}} status changed to up.
Arg1	intfName

Arg2	
Arg3	
Arg4	
Arg5	
Arg6	

2.13 Interface down

Severity	Notice
Event Description	Interface {{intfName}} status changed to down.
Classification	Port
CEF Event ID	0x4000010d
CEF Description	Interface {{intfName}} status changed to down.
Arg1	intfName
Arg2	
Arg3	
Arg4	
Arg5	
Arg6	

2.14 Non-PD or PD short circuit

Severity	Warning
Event Description	The device connected to Port {{number}} detected as a non-PD or the PD short circuited. Check device status.
Classification	Port
CEF Event ID	0x4000010e
CEF Description	The device connected to Port {{sportIndex}} detected as a non-PD or the PD short circuited. Check device status.
Arg1	sportIndex
Arg2	
Arg3	
Arg4	

Arg5	
Arg6	

3. Layer 2 Switching

3.1 Port shutdown (Rate Limit)

Severity	Warning
Event Description	Port {{index}}/{{number}} shut down due to traffic overload.
Classification	L2
CEF Event ID	0x40000200
CEF Description	Port {{sportIndex}} shut down due to traffic overload.
Arg1	sportIndex
Arg2	
Arg3	
Arg4	
Arg5	
Arg6	

3.2 Port recovery (Rate Limit)

Severity	Warning
Event Description	Port {{index}}/{{number}} recovered by Rate Limit.
Classification	L2
CEF Event ID	0x40000201
CEF Description	Port {{sportIndex}} recovered by Rate Limit.
Arg1	sportIndex
Arg2	
Arg3	
Arg4	
Arg5	

Arg6	

5. Redundancy

5.1 Topology Changed(MRP, Turbo Ring, Turbo Chain, Dual Homing)

Severity	Warning
Event Description	Topology changed by Dual Homing.
Classification	Redundancy
CEF Description	Topology changed by Dual Homing.
Arg2	
Arg3	
Arg4	
Arg5	
Arg6	

5.2 Topology Changed(MRP, Turbo Ring, Turbo Chain, Dual Homing)

Severity	Warning
Event Description	Topology change detected, MRP {{strMRMState}}.
Classification	Redundancy
CEF Event ID	0x40000400
CEF Description	Topology change detected, MRP {{reason}}.
Arg1	reason
Arg2	
Arg3	
Arg4	
Arg5	
Arg6	

5.3 Dual homing path change

Severity	Warning
Event Description	Dual Homing path switched.
Classification	Redundancy
CEF Event ID	0x40000401
CEF Description	Dual Homing path switched.
Arg1	
Arg2	
Arg3	
Arg4	
Arg5	
Arg6	

5.4 Redundant port health check failure

Severity	Error
Event Description	Redundant port {{index}}/{{number}} health check failed.
Classification	Redundancy
CEF Event ID	0x40000402
CEF Description	Redundant port {{sportIndex}} health check failed.
Arg1	sportIndex
Arg2	
Arg3	
Arg4	
Arg5	
Arg6	

5.5 Multiple Network Coupling path change

Severity	Warning
Event Description	Status of Multiple Network Coupling path ID {{pathid}} changed.

Classification	Redundancy
CEF Event ID	0x40000403
CEF Description	Status of Multiple Network Coupling path ID {{index}} changed.
Arg1	index
Arg2	
Arg3	
Arg4	
Arg5	
Arg6	

5.6 Topology change (MSTP)

Severity	Warning
Event Description	Topology (MST{{Index}}) changed by MSTP.
Classification	Redundancy
CEF Event ID	0x40000404
CEF Description	Topology (MST{{Index}}) changed by MSTP.
Arg1	index
Arg2	
Arg3	
Arg4	
Arg5	
Arg6	

5.7 MSTP root change

Severity	Warning
Event Description	MSTP (MST{{Index}}) new root was elected in topology.
Classification	Redundancy
CEF Event ID	0x40000405
CEF Description	MSTP (MST{{Index}}) new root was elected in topology.
Arg1	index

Arg2	
Arg3	
Arg4	
Arg5	
Arg6	

5.8 MSTP new port role

Severity	Warning
Event Description	MSTP (MST{{Index}}) port {{number}} role changed from {{role}} to {{role}}.
Classification	Redundancy
CEF Event ID	0x40000406
CEF Description	MSTP (MST{{Index}}) port {{sportIndex}} role changed from {{srole}} to {{drole}}.
Arg1	index
Arg2	sportIndex
Arg3	srole
Arg4	drole
Arg5	
Arg6	

5.9 Topology change (RSTP)

Severity	Warning
Event Description	Topology changed by RSTP.
Classification	Redundancy
CEF Event ID	0x40000407
CEF Description	Topology changed by RSTP.
Arg1	
Arg2	
Arg3	
Arg4	

Arg5	
Arg6	

5.10 RSTP invalid BPDU

Severity	Warning
Event Description	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}}).
Classification	Redundancy
CEF Event ID	0x40000408
CEF Description	RSTP {{sportType}} {{sportIndex}} received an invalid BPDU (type:{{moduleType}}, value:{{value}}).
Arg1	sportType
Arg2	sportIndex
Arg3	moduleType
Arg4	value
Arg5	
Arg6	

5.11 RSTP migration

Severity	Warning
Event Description	Port-Channel {{channel id}} changed to {{rstp/stp}}. Port {{index}}/{{number}} changed to {{rstp/stp}}.
Classification	Redundancy
CEF Event ID	0x40000409
CEF Description	{{sportType}} {{sportIndex}} changed to {{sourceServiceName}}.
Arg1	sportType
Arg2	sportIndex
Arg3	sourceServiceName
Arg4	
Arg5	

Arg6	

5.12 RSTP root change

Severity	Warning
Event Description	New RSTP root was elected in the topology.
Classification	Redundancy
CEF Event ID	0x4000040a
CEF Description	New RSTP root was elected in the topology.
Arg1	
Arg2	
Arg3	
Arg4	
Arg5	
Arg6	

5.13 RSTP new port role

Severity	Warning
Event Description	RSTP Port-Channel {{channel id}} role changed from {{role}} to {{role}}. RSTP port {{index}}/{{number}} role changed from {{role}} to {{role}}.
Classification	Redundancy
CEF Event ID	0x4000040b
CEF Description	RSTP {{sportType}} {{sportIndex}} role changed from {{srole}} to {{drole}}.
Arg1	sportType
Arg2	sportIndex
Arg3	srole
Arg4	drole
Arg5	
Arg6	

5.14 Topology Changed(MRP, Turbo Ring, Turbo Chain, Dual Homing)

Severity	Warning
Event Description	Topology changed by Turbo Chain.
Classification	Redundancy
CEF Event ID	0x4000040c
CEF Description	Topology changed by Turbo Chain.
Arg1	
Arg2	
Arg3	
Arg4	
Arg5	
Arg6	

5.15 Port (channel) restart (Turbo Chain)

Severity	Notice
Event Description	Turbo Chain restarted port channel {{channel id}}. Turbo Chain restarted port {{index}}/{{number}}.
Classification	Redundancy
CEF Event ID	0x4000040d
CEF Description	Turbo Chain restarted {{sportType}} {{sportIndex}}.
Arg1	sportType
Arg2	sportIndex
Arg3	
Arg4	
Arg5	
Arg6	

5.16 Topology Changed(MRP, Turbo Ring, Turbo Chain, Dual Homing)

Severity	Warning
Event Description	Topology change detected on Ring {{RingIndex}} of Turbo Ring v2.
Classification	Redundancy
CEF Event ID	0x4000040e
CEF Description	Topology change detected on Ring {{RingIndex}} of Turbo Ring v2.
Arg1	index
Arg2	
Arg3	
Arg4	
Arg5	
Arg6	

5.17 Master mismatch

Severity	Warning
Event Description	Ring {{Index}} Master settings mismatch detected.
Classification	Redundancy
CEF Event ID	0x4000040f
CEF Description	Ring {{Index}} Master settings mismatch detected.
Arg1	index
Arg2	
Arg3	
Arg4	
Arg5	
Arg6	

5.18 Master change

Severity	Warning
Event Description	The Master of Ring {{Index}} changed.

Classification	Redundancy
CEF Event ID	0x40000410
CEF Description	The Master of Ring {{Index}} changed.
Arg1	index
Arg2	
Arg3	
Arg4	
Arg5	
Arg6	

5.19 Coupling change

Severity	Warning
Event Description	The Turbo Ring v2 coupling path status changed
Classification	Redundancy
CEF Event ID	0x40000411
CEF Description	The Turbo Ring v2 coupling path status changed
Arg1	
Arg2	
Arg3	
Arg4	
Arg5	
Arg6	

5.20 VRRP Master change

Severity	Warning
Event Description	The state of VRRP interface {{intfName}} VrId {{VrId}} changed to Master.
Classification	Redundancy
CEF Event ID	0x40000412
CEF Description	The state of VRRP interface {{intfName}} VrId {{index}} changed to Master.
Arg1	intfName

Arg2	index
Arg3	
Arg4	
Arg5	
Arg6	

5.21 A PHR Supervision frame time difference event occurred on ports A, B

Severity	Critical
Event Description	{{Node_Type}} ({{MAC_Addr}}) no longer detected on port {{Port_Str}}.
Classification	Redundancy
CEF Event ID	0x40000413
CEF Description	{{nodeType}} ({{smac}}) no longer detected on port {{sportIndex}}.
Arg1	nodeType
Arg2	smac
Arg3	sportIndex
Arg4	
Arg5	
Arg6	

5.22 MRP multi managers

Severity	Warning
Event Description	MRP multi managers: {{mac addr}}.
Classification	Redundancy
CEF Event ID	0x40000414
CEF Description	MRP multi managers: {{smac}}.
Arg1	smac
Arg2	
Arg3	
Arg4	

Arg5	
Arg6	

5.23 Tracking state change

Severity	Warning
Event Description	The state of tracking ID {{tid}} changed from up to down. The state of tracking ID {{tid}} changed from down to up.
Classification	Redundancy
CEF Event ID	0x40000415
CEF Description	The state of tracking ID {{index}} changed from {{sstate}} to {{dstate}}.
Arg1	index
Arg2	sstate
Arg3	dstate
Arg4	
Arg5	
Arg6	

5.24 Tracking action on port

Severity	Warning
Event Description	The status of port {{index}}/{{number}} changed to disabled by tracking. The status of port {{index}}/{{number}} changed to recovered by tracking.
Classification	Redundancy
CEF Event ID	0x40000416
CEF Description	The status of port {{sportIndex}} changed to {{dstate}} by tracking.
Arg1	sportIndex
Arg2	dstate
Arg3	
Arg4	
Arg5	
Arg6	

5.25 Tracking action on static route

Severity	Warning
Event Description	Tracking removed the static route. Tracking recovered the static route.
Classification	Redundancy
CEF Event ID	0x40000417
CEF Description	Tracking {{dstate}}the static route.
Arg1	dstate
Arg2	
Arg3	
Arg4	
Arg5	
Arg6	

5.26 Tracking action on VRRP ID

Severity	Warning
Event Description	The priority of VRRP ID (VRID {{vrid}}) decreased by tracking. The priority of VRRP ID (VRID {{vrid}}) recovered by tracking.
Classification	Redundancy
CEF Event ID	0x40000418
CEF Description	The priority of VRRP ID (VRID {{index}}) {{dstate}} by tracking.
Arg1	index
Arg2	dstate
Arg3	
Arg4	
Arg5	
Arg6	

5.28 Topology change (MRP Interconnection)

Severity	Warning
Event Description	Topology change detected, MRP interconnection {{strMIMState}}.

Classification	Redundancy
CEF Event ID	0x4000041a
CEF Description	Topology change detected, MRP interconnection {{reason}}.
Arg1	reason
Arg2	
Arg3	
Arg4	
Arg5	
Arg6	

5.29 SWIFT status change (RSTP)

Severity	Warning
Event Description	RSTP Swift status is {{active/inactive}}.
Classification	Redundancy
CEF Event ID	0x4000041b
CEF Description	RSTP Swift status is {{sstate}}.
Arg1	sstate
Arg2	
Arg3	
Arg4	
Arg5	
Arg6	

5.30 MRP Ring-Open

Severity	Warning
Event Description	MRP MRM port 2 changed from blocking to forwarding due to Ring-Open state.
Classification	Redundancy
CEF Event ID	0x4000041c
CEF Description	MRP MRM port 2 changed from blocking to forwarding due to Ring-Open state.
Arg1	

Arg2	
Arg3	
Arg4	
Arg5	
Arg6	

5.31 Port shutdown (Turbo Chain)

Severity	Warning
Event Description	Port {{index}}/{{number}} shut down due to Chain Protection.
Classification	Redundancy
CEF Event ID	0x4000041d
CEF Description	Port {{sportIndex}} shut down due to Chain Protection.
Arg1	sportIndex
Arg2	
Arg3	
Arg4	
Arg5	
Arg6	

5.32 Port recovery (Turbo Chain)

Severity	Warning
Event Description	Port {{index}}/{{number}} recovered by Chain Protection.
Classification	Redundancy
CEF Event ID	0x4000041e
CEF Description	Port {{sportIndex}} recovered by Chain Protection.
Arg1	sportIndex
Arg2	
Arg3	
Arg4	
Arg5	

Arg6	

5.33 Port shutdown (Turbo Ring)

Severity	Warning
Event Description	Port {{index}}/{{number}} shut down due to Ring Protection.
Classification	Redundancy
CEF Event ID	0x4000041f
CEF Description	Port {{sportIndex}} shut down due to Ring Protection.
Arg1	sportIndex
Arg2	
Arg3	
Arg4	
Arg5	
Arg6	

5.34 Port recovery (Turbo Ring)

Severity	Warning
Event Description	Port {{index}}/{{number}} recovered by Ring Protection.
Classification	Redundancy
CEF Event ID	0x40000420
CEF Description	Port {{sportIndex}} recovered by Ring Protection.
Arg1	sportIndex
Arg2	
Arg3	
Arg4	
Arg5	
Arg6	

5.35 PRP LAN cross-connection detected

Severity	Critical
Event Description	PRP LAN cross-connection detected on Port {{index}}/{{number}}.
Classification	Redundancy
CEF Event ID	0x40000421
CEF Description	PRP LAN cross-connection detected on Port {{sportIndex}}.
Arg1	sportIndex
Arg2	
Arg3	
Arg4	
Arg5	
Arg6	

7. Security

7.1 SSH key regeneration

Severity	Notice
Event Description	The SSH key was regenerated.
Classification	Security
CEF Event ID	0x40000600
CEF Description	The SSH key was regenerated.
Arg1	
Arg2	
Arg3	
Arg4	
Arg5	
Arg6	

7.2 SSL certification change

Severity	Notice
Event Description	SSL certificate changed.
Classification	Security
CEF Event ID	0x40000601
CEF Description	SSL certificate {{reason}}.
Arg1	reason
Arg2	
Arg3	
Arg4	
Arg5	
Arg6	

7.3 DHCP client ingress packet drop

Severity	Warning
Event Description	VLAN {{vlan-id}} dropped DHCP client ingress packets due to a DHCP Snooping rule violation. Total packets discarded: {{number}}.
Classification	Security
CEF Event ID	0x40000602
CEF Description	VLAN {{vlanId}} dropped DHCP client ingress packets due to a DHCP Snooping rule violation. Total packets discarded: {{value}}.
Arg1	vlanId
Arg2	value
Arg3	
Arg4	
Arg5	
Arg6	

7.4 DHCP server packet drop

Severity	Warning

Event Description	VLAN {{vlan-id}} dropped DHCP server packets due to a DHCP Snooping rule violation. Total packets discarded: {{number}}.
Classification	Security
CEF Event ID	0x40000603
CEF Description	VLAN {{vlanId}} dropped DHCP server packets due to a DHCP Snooping rule violation. Total packets discarded: {{value}}.
Arg1	vlanId
Arg2	value
Arg3	
Arg4	
Arg5	
Arg6	

7.5 DHCPSNP static entry overwrite failure

Severity	Warning
Event Description	Static entry: VLAN: {{Vlan Id}}, MAC: {{mac addr}} already exists.
Classification	Security
CEF Event ID	0x40000604
CEF Description	Static entry: VLAN: {{vlanId}}, MAC: {{smac}} already exists.
Arg1	vlanId
Arg2	smac
Arg3	
Arg4	
Arg5	
Arg6	

7.6 Port shutdown (Network Loop Protection)

Severity	Critical
Event Description	Port {{index}}/{{number}} shut down due to looping.
Classification	Security
CEF Event ID	0x40000605

CEF Description	Port {{sportIndex}} shut down due to looping.
Arg1	sportIndex
Arg2	
Arg3	
Arg4	
Arg5	
Arg6	

7.7 MACsec MKA expiration

Severity	Warning
Event Description	The secure MKA session on port {{index}}/{{number}} expired.
Classification	Security
CEF Event ID	0x40000606
CEF Description	The secure MKA session on port {{sportIndex}} expired.
Arg1	sportIndex
Arg2	
Arg3	
Arg4	
Arg5	
Arg6	

7.8 802.1X Auth Fail

Severity	Warning
Event Description	802.1x authentication failed on port {{index}}/{{number}} with {{buffer}}.
Classification	Security
CEF Event ID	0x40000607
CEF Description	802.1x authentication failed on port {{sportIndex}} with {{smac}}.
Arg1	sportIndex
Arg2	smac
Arg3	

Arg4	
Arg5	
Arg6	

7.9 Port shutdown (Port Security)

Severity	Warning
Event Description	Port {{index}}/{{number}} shut down due to a Port Security rule violation.
Classification	Security
CEF Event ID	0x40000608
CEF Description	Port {{sportIndex}} shut down due to a Port Security rule violation.
Arg1	sportIndex
Arg2	
Arg3	
Arg4	
Arg5	
Arg6	

7.10 Packet dropped by Port Security

Severity	Warning
Event Description	Port {{index}}/{{number}} dropped packets due to violation of Port Security rule.
Classification	Security
CEF Event ID	0x40000609
CEF Description	Port {{sportIndex}} dropped packets due to violation of Port Security rule.
Arg1	sportIndex
Arg2	
Arg3	
Arg4	
Arg5	
Arg6	

7.11 Trust host moved from one port to another port (Port Security)

Severity	Warning
Event Description	A trust host, MAC is {{mac address}} with VLAN {{Vlan Id}}, moved from port {{index}}/{{number}} to port {{index}}/{{number}}.
Classification	Security
CEF Event ID	0x4000060a
CEF Description	A trust host, MAC is {{smac}} with VLAN {{vlanId}}, moved from port {{sportIndex}} to port {{dportIndex}}.
Arg1	smac
Arg2	vlanId
Arg3	sportIndex
Arg4	dportIndex
Arg5	
Arg6	

7.12 Integrity check failure

Severity	Warning
Event Description	Event log integrity check failed.
Classification	Security
CEF Event ID	0x4000060b
CEF Description	Event log integrity check failed.
Arg1	
Arg2	
Arg3	
Arg4	
Arg5	
Arg6	

7.13 Integrity is missing

Severity	Warning

Event Description	The log integrity information is missing.
Classification	Security
CEF Event ID	0x4000060c
CEF Description	The log integrity information is missing.
Arg1	
Arg2	
Arg3	
Arg4	
Arg5	
Arg6	

7.14 VLAN Assignment check port mode

Severity	Error
Event Description	VLAN Assignment: Port {{index}}/{{number}} is not in Access mode.
Classification	Security
CEF Event ID	0x4000060d
CEF Description	VLAN Assignment: Port {{sportIndex}} is not in Access mode.
Arg1	sportIndex
Arg2	
Arg3	
Arg4	
Arg5	
Arg6	

7.15 VLAN Assignment check vlan

Severity	Info
Event Description	VLAN Assignment: VLAN ID {{Vlan Id}} does not exist.
Classification	Security
CEF Event ID	0x4000060e
CEF Description	VLAN Assignment: VLAN ID {{vlanId}} does not exist.

Arg1	vlanId
Arg2	
Arg3	
Arg4	
Arg5	
Arg6	

7.16 Event Logs Cleared

Severity	Notice
Event Description	Event logs have been cleared by {{account}}.
Classification	Security
CEF Event ID	0x4000060f
CEF Description	Event logs have been cleared by {{account}}.
Arg1	account
Arg2	
Arg3	
Arg4	
Arg5	
Arg6	

7.17 Configuration integrity check failure

Severity	Warning
Event Description	Configuration integrity check failed.
Classification	Security
CEF Event ID	0x40000610
CEF Description	Configuration integrity check failed.
Arg1	
Arg2	
Arg3	
Arg4	

Arg5	
Arg6	

8. Diagnostics

8.1 Event log export

Severity	Notice
Event Description	Event Log export {{successful /failed}} by {{username}} via {{method}}.
Classification	Diagnostics
CEF Event ID	0x40000700
CEF Description	Event Log export {{outcome}} by {{suser}} via {{method}}.
Arg1	outcome
Arg2	suser
Arg3	method
Arg4	
Arg5	
Arg6	

8.2 Resource log export

Severity	Notice
Event Description	Resource Log export {{successful /failed}} by {{username}} via {{method}}.
Classification	Diagnostics
CEF Event ID	0x40000701
CEF Description	Resource Log export {{outcome}} by {{suser}} via {{method}}.
Arg1	outcome
Arg2	suser
Arg3	method
Arg4	
Arg5	

Arg6	

8.3 Log capacity threshold warning

Severity	Warning
Event Description	Event log entry threshold {{logEntryNum}} reached.
Classification	Diagnostics
CEF Event ID	0x40000702
CEF Description	Event log entry threshold {{threshold}} reached.
Arg1	threshold
Arg2	
Arg3	
Arg4	
Arg5	
Arg6	

8.4 LLDP table change

Severity	Info
Event Description	LLDP remote table changed.
Classification	Diagnostics
CEF Event ID	0x40000703
CEF Description	LLDP remote table changed.
Arg1	
Arg2	
Arg3	
Arg4	
Arg5	
Arg6	

8.5 Module initialization failure

Severity	Error
Event Description	Failed to initialize module {{index}}.
Classification	Diagnostics
CEF Event ID	0x40000704
CEF Description	Failed to initialize module {{index}}.
Arg1	index
Arg2	
Arg3	
Arg4	
Arg5	
Arg6	

8.6 RMON raising alarm

Severity	Warning
Event Description	{{user defined}}.
Classification	Diagnostics
CEF Event ID	0x40000705
CEF Description	{{msg}}.
Arg1	msg
Arg2	
Arg3	
Arg4	
Arg5	
Arg6	

8.7 RMON falling alarm

Severity	Warning
Event Description	{{user defined}}.

Classification	Diagnostics
CEF Event ID	0x40000706
CEF Description	{{msg}}.
Arg1	msg
Arg2	
Arg3	
Arg4	
Arg5	
Arg6	

8.8 Fiber Check warning

Severity	Warning
Event Description	The port {{index}}/{{number}} {{Tx power/Rx power/temperature}} {{exceeded/dropped below}} the threshold.
Classification	Diagnostics
CEF Event ID	0x40000707
CEF Description	The port {{sportIndex}} {{sourceServiceName}} {{reason}} the threshold.
Arg1	sportIndex
Arg2	sourceServiceName
Arg3	reason
Arg4	
Arg5	
Arg6	

8.9 Relay trigger

Severity	Notice
Event Description	{{MGMT/PWR1/PWR2}} alarm triggered due to {{Event Name}}.
Classification	Diagnostics
CEF Event ID	0x40000709
CEF Description	{{moduleType}} alarm triggered due to {{reason}}.

Arg1	moduleType
Arg2	reason
Arg3	
Arg4	
Arg5	
Arg6	

8.10 Relay cut-off

Severity	Notice
Event Description	{{relay_name}} relay alarm was cut off.
Classification	Diagnostics
CEF Event ID	0x4000070a
CEF Description	{{moduleType}} relay alarm was cut off.
Arg1	moduleType
Arg2	
Arg3	
Arg4	
Arg5	
Arg6	

8.11 DI on

Severity	Notice
Event Description	Digital input {{index}} turned on.
Classification	Diagnostics
CEF Event ID	0x4000070b
CEF Description	Digital input {{index}} turned on.
Arg1	index
Arg2	
Arg3	
Arg4	

Arg5	
Arg6	

8.12 DI off

Severity	Notice
Event Description	Digital input {{index}} turned off.
Classification	Diagnostics
CEF Event ID	0x4000070c
CEF Description	Digital input {{index}} turned off.
Arg1	index
Arg2	
Arg3	
Arg4	
Arg5	
Arg6	

8.13 Moxa tech support login

Severity	Notice
Event Description	Moxa technical support logged in to the device for troubleshooting.
Classification	Diagnostics
CEF Event ID	0x4000070d
CEF Description	Moxa technical support logged in to the device for troubleshooting.
Arg1	
Arg2	
Arg3	
Arg4	
Arg5	
Arg6	

8.14 Moxa tech support logout

Severity	Notice
Event Description	Moxa technical support logged out of the device.
Classification	Diagnostics
CEF Event ID	0x4000070e
CEF Description	Moxa technical support logged out of the device.
Arg1	
Arg2	
Arg3	
Arg4	
Arg5	
Arg6	

8.15 Moxa tech support function activation

Severity	Notice
Event Description	The Moxa technical support function activated.
Classification	Diagnostics
CEF Event ID	0x4000070f
CEF Description	The Moxa technical support function activated.
Arg1	
Arg2	
Arg3	
Arg4	
Arg5	
Arg6	

8.16 Moxa tech support function deactivation

Severity	Notice
Event Description	The Moxa technical support function deactivated.

Classification	Diagnostics
CEF Event ID	0x40000710
CEF Description	The Moxa technical support function deactivated.
Arg1	
Arg2	
Arg3	
Arg4	
Arg5	
Arg6	

9. Industrial

9.1 DCP IP change

Severity	Notice
Event Description	IP was changed by PROFINET DCP.
Classification	Industrial
CEF Event ID	0x40000800
CEF Description	IP was changed by PROFINET DCP.
Arg1	
Arg2	
Arg3	
Arg4	
Arg5	
Arg6	

9.2 DCP default route change

Severity	Notice
Event Description	Default route changed by PROFINET DCP.
Classification	Industrial

CEF Event ID	0x40000801
CEF Description	Default route changed by PROFINET DCP.
Arg1	
Arg2	
Arg3	
Arg4	
Arg5	
Arg6	

9.3 GOOSE Check entry counter timeout

Severity	Warning
Event Description	GOOSE Timeout: {{APPID}} {{DA}} Port {{port string}}
Classification	Industrial
CEF Event ID	0x40000802
CEF Description	GOOSE Timeout: {{id}} {{dmac}} Port {{sportIndex}}
Arg1	id
Arg2	dmac
Arg3	sportIndex
Arg4	
Arg5	
Arg6	

9.4 GOOSE Check entry counter timeout clear

Severity	Warning
Event Description	GOOSE Timeout Clear: {{APPID}} {{DA}} Port {{port string}}
Classification	Industrial
CEF Event ID	0x40000803
CEF Description	GOOSE timeout clear: {{id}} {{dmac}} Port {{sportIndex}}
Arg1	id
Arg2	dmac

Arg3	sportIndex
Arg4	
Arg5	
Arg6	

9.5 GOOSE Check tampered ingress port

Severity	Warning
Event Description	Tampered GOOSE: {{APPID}} {{DA}} Port {{port string}} source port conflicted with Port {{port string}}
Classification	Industrial
CEF Event ID	0x40000804
CEF Description	Tampered GOOSE: {{id}} {{dmac}} Port {{sportIndex}} source port conflicted with Port {{dportIndex}}
Arg1	id
Arg2	dmac
Arg3	sportIndex
Arg4	dportIndex
Arg5	
Arg6	

9.6 GOOSE Check tampered source MAC address

Severity	Warning
Event Description	Tampered GOOSE: {{APPID}} {{DA}} Port {{port string}} source MAC conflicted with {{SA}}
Classification	Industrial
CEF Event ID	0x40000805
CEF Description	Tampered GOOSE: {{id}} {{dmac}} Port {{sportIndex}} source MAC conflicted with {{smac}}
Arg1	id
Arg2	dmac
Arg3	sportIndex
Arg4	smac

Arg5	
Arg6	

9.7 GOOSE Check Lock violation

Severity	Warning
Event Description	Unexpected GOOSE packet: {{APPID}} {{DA}} Port {{port string}}
Classification	Industrial
CEF Event ID	0x40000806
CEF Description	Unexpected GOOSE packet: {{id}} {{dmac}} Port {{sportIndex}}
Arg1	id
Arg2	dmac
Arg3	sportIndex
Arg4	
Arg5	
Arg6	

9.8 GOOSE Check entry reset

Severity	Notice
Event Description	GOOSE entry reset: {{APPID] {{DA}}
Classification	Industrial
CEF Event ID	0x40000807
CEF Description	GOOSE entry reset: {{id}} {{dmac}}
Arg1	id
Arg2	dmac
Arg3	
Arg4	
Arg5	
Arg6	

9.9 GOOSE Check entry delete

Severity	Notice
Event Description	GOOSE entry deleted: {{APPID] {{DA}}
Classification	Industrial
CEF Event ID	0x40000808
CEF Description	GOOSE entry deleted: {{id}} {{dmac}}
Arg1	id
Arg2	dmac
Arg3	
Arg4	
Arg5	
Arg6	

9.10 Port shutdown (GOOSE Check)

Severity	Warning
Event Description	Port {{index}}/{{number}} shut down due to a GOOSE Tampered event.
Classification	Industrial
CEF Event ID	0x40000809
CEF Description	Port {{sportIndex}} shut down due to a GOOSE Tampered event.
Arg1	sportIndex
Arg2	
Arg3	
Arg4	
Arg5	
Arg6	

11. Routing

11.1 OSPF DR change

Severity	Notice
Event Description	Interface {{IP}} DR changed from {{IP}} to {{IP}}.
Classification	Routing
CEF Event ID	0x40001000
CEF Description	Interface {{intfIp}} DR changed from {{src}} to {{dst}}.
Arg1	intfIp
Arg2	src
Arg3	dst
Arg4	
Arg5	
Arg6	

11.2 OSPF DR adjacency change

Severity	Notice
Event Description	Interface {{IP}} DR neighbor {{IP}} adjacency changed.
Classification	Routing
CEF Event ID	0x40001001
CEF Description	Interface {{intfIp}} DR neighbor {{src}} adjacency changed.
Arg1	intfIp
Arg2	src
Arg3	
Arg4	
Arg5	
Arg6	

11.3 OSPF become DR

Severity	Notice
Event Description	Interface {{IP}} become DR.
Classification	Routing
CEF Event ID	0x40001002
CEF Description	Interface {{intfIp}} become DR.
Arg1	intfIp
Arg2	
Arg3	
Arg4	
Arg5	
Arg6	

11.4 PIM-SM DR change

Severity	Notice
Event Description	PIM-SM interface {{interface name}} DR changed to {{IP address}}.
Classification	Routing
CEF Event ID	0x40001003
CEF Description	PIM-SM interface {{intfName}} DR changed to {{intfIp}}.
Arg1	intfName
Arg2	intfIp
Arg3	
Arg4	
Arg5	
Arg6	

11.5 PIM-SM RP addition (BSM)

Severity	Notice
Event Description	PIM-SM group: {{group-prefix}}/{{mask-length}} added RP {{IP address}} (priority={{number}})

Classification	Routing
CEF Event ID	0x40001004
CEF Description	PIM-SM group: {{netAddr}} added RP {{intfIp}} (priority=value}})
Arg1	netAddr
Arg2	intfIp
Arg3	value
Arg4	
Arg5	
Arg6	

11.6 PIM-SM RP deletion (BSM)

Severity	Notice
Event Description	PIM-SM group: {{group-prefix}}/{{mask-length}} deleted RP {{IP address}} (priority={{number}})
Classification	Routing
CEF Event ID	0x40001005
CEF Description	PIM-SM group: {{netAddr}} deleted RP {{intfIp}} (priority={{value}})
Arg1	netAddr
Arg2	intfIp
Arg3	value
Arg4	
Arg5	
Arg6	

11.7 BFD session up

Severity	Notice
Event Description	BFD session {{index}} is up (Neighbor IP: {{netAddr}}).
Classification	Routing
CEF Event ID	0x40001006
CEF Description	BFD session {{index}} is up (Neighbor IP: {{netAddr}}).

Arg1	index
Arg2	netAddr
Arg3	
Arg4	
Arg5	
Arg6	

11.8 BFD session down

Severity	Warning
Event Description	BFD session {{index}} is down (Neighbor IP: {{netAddr}}, Reason: {{reason}}).
Classification	Routing
CEF Event ID	0x40001007
CEF Description	BFD session {{index}} is down (Neighbor IP: {{netAddr}}, Reason: {{reason}}).
Arg1	index
Arg2	netAddr
Arg3	reason
Arg4	
Arg5	
Arg6	

11.9 BFD attempt limit overrun

Severity	Warning
Event Description	System attempted to exceed BFD session limit {{threshold}}.
Classification	Routing
CEF Event ID	0x40001008
CEF Description	System attempted to exceed BFD session limit {{threshold}}.
Arg1	threshold
Arg2	
Arg3	
Arg4	

Arg5	
Arg6	

11.10 BFD time renegotiation

Severity	Notice
Event Description	BFD time renegotiate. Session {{index}} detection time changed from {{value}} to {{value}}.
Classification	Routing
CEF Event ID	0x40001009
CEF Description	BFD time renegotiate. Session {{index}} detection time changed from {{value}} to {{value}}.
Arg1	index
Arg2	value
Arg3	value
Arg4	
Arg5	
Arg6	

Fiber Check Threshold Values for Auto Mode

This table shows the default thresholds for temperature, Tx power, and Rx power for Moxa fiber modules.

Module	Temperature Threshold (°C)	Tx Power Low Threshold (dBm)	Tx Power High Threshold (dBm)	Rx Power Low Threshold (dBm)	Rx Power High Threshold (dBm)
FEMST	120	-20	-14	-32.0	-3.0
FEMSC	120	-20	-14	-32.0	-3.0
FESSC	120	-5.0	0.0	-34.0	-3.0
SFP-1FEMLC-T	120	-18.0	-8.0	-32.0	-3.0
SFP-1FESLC-T	120	-5.0	0.0	-34.0	-3.0
SFP-1FELLC-T	120	-5.0	0.0	-34.0	-3.0
SFP-1GSXLC-T	110	-9.5	-4.0	-18.0	0.0
SFP-1GLSXLC-T	120	-9.0	-1.0	-19.0	-1.0
SFP-1GLXLC-T	120	-9.0	-3.0	-21.0	-3.0
SFP-1GLHLC-T	120	-8.0	-3.0	-23.0	-3.0
SFP-1GLHXLC-T	120	-4.0	3.0	-24.0	-1.0
SFP-1GZXLC-T	120	0.0	5.0	-24.0	-1.0
SFP-1G10ALC-T	120	-9.0	-3.0	-21.0	-3.0

Module	Temperature Threshold (°C)	Tx Power Low Threshold (dBm)	Tx Power High Threshold (dBm)	Rx Power Low Threshold (dBm)	Rx Power High Threshold (dBm)
SFP-1G10BLC-T	120	-9.0	-3.0	-21.0	-3.0
SFP-1G20ALC-T	120	-8.0	-2.0	-23.0	-2.0
SFP-1G20BLC-T	120	-8.0	-2.0	-23.0	-2.0
SFP-1G40ALC-T	120	-3.0	2.0	-23.0	-1.0
SFP-1G40BLC-T	120	-3.0	2.0	-23.0	-1.0
SFP-1GSXLC	100	-9.5	-4.0	-18.0	0
SFP-1GLSXLC	100	-9.0	-1.0	-19.0	-1.0
SFP-1GLXLC	100	-9.0	-3.0	-21.0	-3.0
SFP-1GLHLC	100	-8.0	-3.0	-23.0	-3.0
SFP-1GLHXLC	100	-4.0	3.0	-24.0	-1.0
SFP-1GZXLC	100	0.0	5.0	-24.0	-1.0
SFP-1GEZXLC	100	0.0	5.0	-30.0	-9.0
SFP-1GEZXLC-120	100	-2.0	3.0	-33.0	-8.0
SFP-1G10ALC	100	-9.0	-3.0	-21.0	-2.0
SFP-1G10BLC	100	-9.0	-3.0	-21.0	-3.0

Module	Temperature Threshold (°C)	Tx Power Low Threshold (dBm)	Tx Power High Threshold (dBm)	Rx Power Low Threshold (dBm)	Rx Power High Threshold (dBm)
SFP-1G20ALC	100	-8.0	-2.0	-23.0	-2.0
SFP-1G20BLC	100	-8.0	-2.0	-23.0	-2.0
SFP-1G40ALC	100	-3.0	2.0	-23.0	-1.0
SFP-1G40BLC	100	-3.0	2.0	-23.0	-1.0
SFP-2.5GMLC-T	120	-7.5	-1.0	-13.5	0.0
SFP-2.5GSLC-T	120	-9.0	-3.0	-15.0	3.0
SFP-2.5GLSLC-T	120	-5.0	0.0	-16.0	0.0
SFP-2.5GSLHLC-T	120	-4.0	1.0	-19.0	1.0
SFP-10GERLC-T	110	-1.0	2.0	-15.8	-1.0
SFP-10GZRLC-T	100	0.0	4.0	-23	-7.0
SFP-10GLRLC-T	120	-8.2	0.5	-14.4	0.5
SFP-10GSRLC-T	110	-5.0	-1.0	-9.9	0.5

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
0x0000	1 word	HEX	Vendor ID = 0x1393
0x0001	1 word		Unit ID (Ethernet = 1)
0x0002	2 word	HEX	Product Code (Please refer to Product Code Table)
0x0010	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
0x0030	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’
0x004B	6 words	ASCII	Product Serial Number
0x0051	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)
0x0053	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
0x0055	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
0x0058	1 word	HEX	Power 1 0x0000: Off 0x0001: ON

Address Offset	Data type	Interpretation	Description
0x0059	1 word	HEX	Power 2 0x0000: Off 0x0001: On
0x005A	1 word	HEX	Fault LED Status 0x0000: No 0x0001: Yes
0x0080	1 word	HEX	DI1 0x0000:Off 0x0001:On 0xFFFE: DI1 is Not Supported
0x0081	1 word	HEX	DI2 0x0000:Off 0x0001:On 0xFFFE: DI2 is Not Supported
0x0082	1 word	HEX	DO1 0x0000:Off 0x0001:On 0xFFFE: DO1 is Not Supported
0x0083	1 word	HEX	DO2 0x0000:Off 0x0001:On 0xFFFE: DO2 is Not Supported
0x0084	1 word	HEX	DO3 0x0000:Off 0x0001:On 0xFFFE: DO3 is Not Supported
0x0085 (Power Module 1) **0x0086 (Power Module 2)**	1 word	HEX	Power Module Present 0x0000: Not Present 0x0001: Present 0xFFFE: Power Module is Not Supported

Address Offset	Data type	Interpretation	Description
0x0087 (Power Module 1) **0x0097 (Power Module 2)**	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’
0x00A7 (Power Module 1) **0x00AD (Power Module 2)**	6 words	ASCII	Power Module Serial Number
0x00B3 (Power Module 1) **0x00B5 (Power Module 2)**	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
0x00B7 (External Module 1) **0x00B8 (External Module 2)** **...**	1 word	HEX	External Module Present 0x0000: Not Present 0x0001: Present 0xFFFE: External Module is Not Supported

Address Offset	Data type	Interpretation	Description
0x00C7 (External Module 1) **0x00D7 (External Module 2)** **...**	16 words	ASCII	External Module Name 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’
0x01C7 (External Module 1) **0x01CD (External Module 2)** **...**	6 words	ASCII	External Module Serial Number
0x0227 (External Module 1) **0x0229 (External Module 2)** **...**	2 words	HEX	External 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

Port Information

Address Offset	Data type	Interpretation	Description
0x1000 (Port 1) **0x1001 (Port 2)** **...** **Maximum Port (n)** **0x1000 + n (Channel Group 1)** **0x1000 + n + 1 (Channel Group 2)** **...**	1 word	HEX	Port Status 0x0000: Link down 0x0001: Link up 0x0002: Disable 0xFFFF: No port
0x1100 (Port 1) **0x1101 (Port 2)** **...** **Maximum Port (n)** **0x1100 + n (Channel Group 1)** **0x1100 + n + 1 (Channel Group 2)** **...**	1 word	HEX	Port Speed (Y: Channel group active port count) 0x0000: 10M-Half 0xY001: 10M-Full 0x0002: 100M-Half 0xY003: 100M-Full 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
0x1200 (Port 1) **0x1201 (Port 2)** **...** **Maximum Port (n)**	1 word	HEX	Port Flow Ctrl 0x0000:Off 0x0001:On 0xFFFE: Inactive Link 0xFFFF:No port

Address Offset	Data type	Interpretation	Description
0x1300 (Port 1) **0x1301 (Port 2)** **...** **Maximum Port (n)**	1 word	HEX	Port MDI/MDIX 0x0000: MDI 0x0001: MDIX 0xFFFD: Fiber Port 0xFFFE: Inactive Link 0xFFFF: No port
0x1400 (Port 1) **0x1420 (Port 2)** **...** **Maximum Port (n)**	32 words	ASCII	Port Media Type Ex: Port 1 Media Type = “100TX,RJ45.” Word 0 Hi byte =‘1’ 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
0x2000 (Port 1) **0x2002 (Port 2)** **...** **Maximum Port (n)** **0x2000 + (n * 2) (Channel Group 1)** **0x2000 + ((n + 1) * 2) (Channel Group 2)** **...**	2 words	HEX	Port Tx Packets Ex: port 1 Tx Packet Amount = 44332211 Received MODBUS response: 0x02A474B3 Word 0 = 0x02A4 Word 1 = 0x74B3

Address Offset	Data type	Interpretation	Description
0x2100 (Port 1) **0x2102 (Port 2)** **...** **Maximum Port (n)** **0x2100 + (n * 2) (Channel Group 1)** **0x2100 + ((n + 1) * 2) (Channel Group 2)** **...**	2 words	HEX	Port Rx Packets Ex: port 1 Tx Packet Amount = 44332211 Received MODBUS response: 0x02A474B3 Word 0 = 0x02A4 Word 1 = 0x74B3
0x2200 (Port 1) **0x2202 (Port 2)** **...** **Maximum Port (n)** **0x2200 + (n * 2) (Channel Group 1)** **0x2200 + ((n + 1) * 2) (Channel Group 2)** **...**	2 words	HEX	Port Tx Error Packets Ex: port 1 Tx Packet Amount = 44332211 Received MODBUS response: 0x02A474B3 Word 0 = 0x02A4 Word 1 = 0x74B3
0x2300 (Port 1) **0x2302 (Port 2)** **...** **Maximum Port (n)** **0x2300 + (n * 2) (Channel Group 1)** **0x2300 + ((n + 1) * 2) (Channel Group 2)** **...**	2 words	HEX	Port Rx Error Packets Ex: port 1 Tx Packet Amount = 44332211 Received MODBUS response: 0x02A474B3 Word 0 = 0x02A4 Word 1 = 0x74B3

Redundancy Information

Address Offset	Data type	Interpretation	Description
0x3000	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
0x3100	1 word	HEX	RSTP Root 0x0000: Not Root 0x0001: Root 0xFFFE: RSTP is Not Supported 0xFFFF: RSTP is Not Enabled
0x3200 (Port 1) **0x2301 (Port 2)** **...** **Maximum Port (n)** **0x3200 + n (Channel Group 1)** **0x3200 + n + 1 (Channel Group 2)** **...**	1 word	HEX	RSTP Port Status 0x0000: Port Disabled 0x0001: Not RSTP Port 0x0002: Link Down 0x0003: Blocked 0x0004: Learning 0x0005: Forwarding 0xFFFD: No Port 0xFFFE: RSTP is Not Supported 0xFFFF: RSTP is Not Enabled
0x3500	1 word	HEX	Turbo Ring V2 Coupling Mode 0x0000: None 0x0001: Coupling Backup 0x0002: Coupling Primary 0xFFFE: Turbo Ring V2 is Not Supported 0xFFFF: Turbo Ring V2 is Not Enabled

Address Offset	Data type	Interpretation	Description
0x3501	1 word	HEX	Turbo Ring V2 Coupling Port Primary Status 0x0000: Not Coupling Port 0x0001: Link Down 0x0002: Blocked 0x0003: Learning 0x0004: Forwarding 0xFFFD: Turbo Ring V2 Coupling is Not Enabled 0xFFFE: Turbo Ring V2 is Not Supported 0xFFFF: Turbo Ring V2 is Not Enabled
0x3502	1 word	HEX	Turbo Ring V2 Coupling Port Backup Status 0x0000: Not Coupling Port 0x0001: Link Down 0x0002: Blocked 0x0003: Learning 0x0004: Forwarding 0xFFFD: Turbo Ring V2 Coupling is Not Enabled 0xFFFE: Turbo Ring V2 is Not Supported 0xFFFF: Turbo Ring V2 is Not Enabled
0x3600	1 word	HEX	Turbo Ring V2 Ring 1 Status 0x0000: Healthy 0x0001: Break 0xFFFD: Turbo Ring V2 Ring 1 is Not Enabled 0xFFFE: Turbo Ring V2 is Not Supported 0xFFFF: Turbo Ring V2 is Not Enabled
0x3601	1 word	HEX	Turbo Ring V2 Ring 1 Master/Slave 0x0000: Slave 0x0001: Master 0xFFFD: Turbo Ring V2 Ring 1 is Not Enabled 0xFFFE: Turbo Ring V2 is Not Supported 0xFFFF:Turbo Ring V2 is Not Enabled

Address Offset	Data type	Interpretation	Description
0x3602	1 word	HEX	Turbo Ring V2 Ring 1's 1st Port Status 0x0000: Link Down 0x0001: Blocked 0x0002:Learning 0x0003:Forwarding 0xFFFD: Turbo Ring V2 Ring 1 is Not Enabled 0xFFFE: Turbo Ring V2 is Not Supported 0xFFFF:Turbo Ring V2 is Not Enabled
0x3603	1 word	HEX	Turbo Ring V2 Ring 1's 2nd Port Status 0x0000: Link Down 0x0001: Blocked 0x0002: Learning 0x0003: Forwarding 0xFFFD: Turbo Ring V2 Ring 1 is Not Enabled 0xFFFE: Turbo Ring V2 is Not Supported 0xFFFF:Turbo Ring V2 is Not Enabled
0x3680	1 word	HEX	Turbo Ring V2 Ring 2 Status 0x0000: Healthy 0x0001: Break 0xFFFD: Turbo Ring V2 Ring 2 is Not Enabled 0xFFFE: Turbo Ring V2 is Not Supported 0xFFFF: Turbo Ring V2 is Not Enabled
0x3681	1 word	HEX	Turbo Ring V2 Ring 2 Master/Slave 0x0000: Slave 0x0001: Master 0xFFFD: Turbo Ring V2 Ring 2 is Not Enabled 0xFFFE: Turbo Ring V2 is Not Supported 0xFFFF:Turbo Ring V2 is Not Enabled

Address Offset	Data type	Interpretation	Description
0x3682	1 word	HEX	Turbo Ring V2 Ring 2's 1st Port Status 0x0000: Link Down 0x0001: Blocked 0x0002: Learning 0x0003: Forwarding 0xFFFD: Turbo Ring V2 Ring 2 is Not Enabled 0xFFFE: Turbo Ring V2 is Not Supported 0xFFFF:Turbo Ring V2 is Not Enabled
0x3683	1 word	HEX	Turbo Ring V2 Ring 2's 2nd Port Status 0x0000: Link Down 0x0001: Blocked 0x0002: Learning 0x0003: Forwarding 0xFFFD: Turbo Ring V2 Ring 2 is Not Enabled 0xFFFE: Turbo Ring V2 is Not Supported 0xFFFF:Turbo Ring V2 is Not Enabled
0x3700	1 word	HEX	Turbo Chain Switch Role 0x0000: Head 0x0001: Member 0x0002: Tail 0xFFFE: Turbo Chain is Not Supported 0xFFFF: Turbo Chain is Not Enabled
0x3701	1 word	HEX	Turbo Chain 1st Port Status 0x0000: Link Down 0x0001: Blocked 0x0002: Listening 0x0003: Forwarding 0xFFFE: Turbo Chain is Not Supported 0xFFFF: Turbo Chain is Not Enabled

Address Offset	Data type	Interpretation	Description
0x3702	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
0x3800	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
0x3801	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
0x3802	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
0x3803	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
0x3804	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-bit)	Product code (32-bit)
EDS-4008	0x1100	0x11021000
EDS-4008-2GT-2GS	0x1104	0x11021004
EDS-4008-2MSC	0x1101	0x11021001
EDS-4008-2MST	0x1102	0x11021002
EDS-4008-2SSC	0x1103	0x11021003
EDS-4008-4P-2GT-GS	0x1105	0x11024005
EDS-4009-3MSC	0x1107	0X11022007
EDS-4009-3MST	0x1108	0X11022008
EDS-4009-3SSC	0x1109	0X11022009
EDS-4012-4GC	0x110B	0X1102300b
EDS-4012-4GC-HV-T	0x110D	0X1102300d
EDS-4012-4GS	0x110A	0X1102300a
EDS-4012-4GS-HV-T	0x110C	0X1102300c
EDS-4012-8P-4GS	0x110E	0x1102340e
EDS-4014-4GS-2QGS-HV-T	0x1112	0x11024012
EDS-G4008	0x1106	0x11021806
EDS-G4012-4GC	0x110F	0x1102380f
EDS-G4012-8P-4GS	0x1110	0x11023c10
EDS-G4014-4GS-2QGS	0x1111	0x11024011

Product name	Product code (16-bit)	Product code (32-bit)
EDS-G4014-4QGS-2XGS	0x1114	0x11024814
EDS-G4014-6QGS	0x1113	0x11024813
MDS-G4012	0x1081	0x11010001
MDS-G4012-4XGS-T	0x1281	0x11050001
MDS-G4012-L3	0x2081	0x12010001
MDS-G4012-L3-4XGS-T	0x2281	0x12050001
MDS-G4020	0x1082	0x11010002
MDS-G4020-4XGS-T	0x1282	0x11050002
MDS-G4020-L3	0x2082	0x12010002
MDS-G4020-L3-4XGS-T	0x2282	0x12050002
MDS-G4028	0x1083	0x11010003
MDS-G4028-4XGS-FM	0x2284	0x11050004
MDS-G4028-4XGS-T	0x1283	0x11050003
MDS-G4028-L3	0x2083	0x12010003
MDS-G4028-L3-4XGS-T	0x2283	0x12050003
MRX-G4064-L3-8XGS	0x2482	0x12090002
MRX-Q4064-L3-16XGS	0x2481	0x12090001
RKS-G4028-4GS-2HV-T	0x1304	0x11060004
RKS-G4028-4GS-2LV-T	0x1308	0x11060008
RKS-G4028-4GS-HV-T	0x1303	0x11060003
RKS-G4028-4GS-LV-T	0x1307	0x11060007
RKS-G4028-4GT-2HV-T	0x1302	0x11060002
RKS-G4028-4GT-2LV-T	0x1306	0x11060006

Product name	Product code (16-bit)	Product code (32-bit)
RKS-G4028-4GT-HV-T	0x1301	0x11060001
RKS-G4028-4GT-LV-T	0x1305	0x11060005
RKS-G4028-L3-4GS-2HV-T	0x2304	0x12060004
RKS-G4028-L3-4GS-2LV-T	0x2308	0x12060008
RKS-G4028-L3-4GS-HV-T	0x2303	0x12060003
RKS-G4028-L3-4GS-LV-T	0x2307	0x12060007
RKS-G4028-L3-4GT-2HV-T	0x2302	0x12060002
RKS-G4028-L3-4GT-2LV-T	0x2306	0x12060006
RKS-G4028-L3-4GT-HV-T	0x2301	0x12060001
RKS-G4028-L3-4GT-LV-T	0x2305	0x12060005
RKS-G4028-L3-PoE-4GS-2HV-T	0x230A	0x1206000A
RKS-G4028-L3-PoE-4GS-2LV-T	0x230C	0x1206000C
RKS-G4028-L3-PoE-4GS-HV-T	0x2309	0x12060009
RKS-G4028-L3-PoE-4GS-LV-T	0x230B	0x1206000B
RKS-G4028-PL-12XGS-T	0x1182	0x11030002
RKS-G4028-PL-L3-12XGS-T	0x2182	0x12030002
RKS-G4028-PL-L3-PoE-12XGS-T	0x2184	0x12030004
RKS-G4028-PL-PoE-12XGS-T	0x1184	0x11030004
RKS-G4028-PoE-4GS-2HV-T	0x130A	0x1106000A
RKS-G4028-PoE-4GS-2LV-T	0x130C	0x1106000C
RKS-G4028-PoE-4GS-HV-T	0x1309	0x11060009
RKS-G4028-PoE-4GS-LV-T	0x130B	0x1106000B
RKS-G4030-PL-8QGT-6XGS-T	0x1181	0x11030001

Product name	Product code (16-bit)	Product code (32-bit)
RKS-G4030-PL-L3-8QGT-6XGS-T	0x2181	0x12030001
RKS-G4030-PL-L3-PoE-8QGT-6XGS-T	0x2183	0x12030003
RKS-G4030-PL-PoE-8QGT-6XGS-T	0x1183	0x11030003

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
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256	ECDHE	RSA	CHACHA20-POLY1305	SHA256
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	ECDHE	ECDSA	AES128	SHA256
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDHE	RSA	AES128	SHA256
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDHE	RSA	AES256	SHA384
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	Ephemeral DH	RSA	AES128	SHA256
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	Ephemeral DH	RSA	AES256	SHA384
TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256	Ephemeral DH	RSA	CHACHA20-POLY1305	SHA256
TLS_ECDHE-RSA_WITH_AES256-SHA384	ECDHE	RSA	AES256	SHA384
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	ECDHE	RSA	AES128	SHA256
TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256	ECDHE	ECDSA	CHACHA20-POLY1305	SHA256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDHE	RSA	AES256	SHA384
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384	ECDHE	ECDSA	AES256	SHA384
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	ECDHE	ECDSA	AES128	SHA256

b. **TLS V1.3**

Cipher suite name	Key exchange	Encryption	Mode	Hash function
TLS_AES_256_GCM_SHA384	any	AES256	GCM	SHA384
TLS_CHACHA20_POLY1305_SHA256	any	CHACHA20-POLY1305	N/A	SHA256
TLS_AES_128_GCM_SHA256	any	AES128	GCM	SHA256

2. Below is a list of the recommended secure browsers that support TLS v1.2 or higher:

Browser	Version
Microsoft Edge	All
Microsoft Internet Explorer	v11 or above
Mozilla Firefox	v27 or above
Google Chrome	v38 or above
Apple Safari	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:
   a. **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.
   b. **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:
   a. **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.
   b. **Telnet / SSH**: We recommend that administrators use SSH with authentication and encryption to retrieve device properties.
   c. **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
SSH	22	Enabled	Y
Telnet	23	Disabled	Y
E-Mail Server (SMTP)	25	Disabled	Y
TACACS+	49	Disabled	Y
HTTP	80	Enabled	Y
MMS	102	Disabled	N
HTTPS	443	Enabled	Y
Moxa Service	443	Enabled	N
Modbus	502	Disabled	N

Service Type	Port Number	Default state	Port can be modified
Ethernet/IP	44818	Disabled	N

b. **Protocol: UDP**

Service Type	Port Number	Default state	Port can be modified
DHCP Server	67	Disabled	N
NTP	123	Disabled	N
SNMP	161	Disabled	Y
PTP (IP based)	319/320	Disabled	N
Syslog	514	Disabled	Y
RADIUS	1812	Disabled	Y
Ethernet/IP	2222	Disabled	N
PROFINET	34964/49152	Disabled	N
Moxa Service	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.

Syslog Severity	CEF Severity	Severity Name	Description
0	10	Emergency	System is unusable
1	8	Alert	Action must be taken immediately
2	7	Critical	Critical conditions
3	6	Error	Error conditions
4	5	Warning	Warning conditions
5	4	Notice	Normal but significant condition
6	1	Infomational	Informational messages
7	0	Debug	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
│       │   ├── mxPoee.mib
│       │   ├── mxPorte.mib
│       │   ├── mxProfinet.mib
```

```
|       |   ├── mxPtp.mib
|       |   ├── mxRelayC.mib
|       |   ├── mxSnmp.mib
|       |   ├── mxSwe.mib
|       |   ├── mxSysLoginPolicySvr.mib
|       |   ├── mxSyslogSvr.mib
|       |   ├── mxSysPasswordPolicySvr.mib
|       |   ├── mxSystemInfo.mib
|       |   ├── mxSysTrustAccessSvr.mib
|       |   ├── mxSysUtilSvr.mib
|       |   ├── mxTimeSetting.mib
|       |   ├── mxTimeZone.mib
|       |   ├── mxTrackinge.mib
|       |   ├── mxTrapC.mib
|       |   └── mxUiServiceMgmt.mib
|       ├── PoE     // PoE group
|       |   ├── mxPoe.mib
|       |   └── mxPoeBt.mib
|       ├── Product_Information        // Product group
|       |   ├── mxGeneralInfo.mib
|       |   └── mxProductInfo.mib
|       ├── Switching     // Switching group
|       |   ├── mxDai.mib
|       |   ├── mxDhcpSnp.mib
|       |   ├── mxDot1x.mib
|       |   ├── mxDualHoming.mib
|       |   ├── mxFiberCheck.mib
|       |   ├── mxIgmpSnp.mib
|       |   ├── mxIpsg.mib
|       |   ├── mxLa.mib
|       |   ├── mxLhc.mib
|       |   ├── mxLldp.mib
|       |   ├── mxLp.mib
|       |   ├── mxMab.mib
|       |   ├── mxMacsec.mib
|       |   ├── mxPort.mib
```

```
|       |    ├── mxPortMirror.mib
|       |    ├── mxPsms.mib
|       |    ├── mxPssp.mib
|       |    ├── mxQos.mib
|       |    ├── mxRadius.mib
|       |    ├── mxRlps.mib
|       |    ├── mxRmon.mib
|       |    ├── mxRstp.mib
|       |    ├── mxStcl.mib
|       |    ├── mxSwitching.mib
|       |    ├── mxTc.mib
|       |    ├── mxTcst.mib
|       |    ├── mxTrv2.mib
|       |    └── mxVlan.mib
|       ├── Routing    // Routing group
|           ├── mxArp.mib
|           ├── mxIpIf.mib
|           |── mxMulticastRouting.mib
|           ├── mxOspf.mib
|           ├── mxPimSm.mib
|           ├── mxRte.mib
|           ├── mxStaticRoute.mib
|           ├── mxUnicastRoutingTable.mib
|           └── mxVrrp.mib
|
├── Standard     // Standard MIB
|   ├── BRIDGE-MIB.mib
|   ├── EtherLike-MIB.mib
|   ├── IANA-ADDRESS-FAMILY-NUMBERS.mib
|   ├── IANAifType-MIB.mib
|   ├── IEC-62439-2.mib
|   ├── IEEE8021-PAE-MIB.mib
|   ├── IEEE8021-SPANNING-TREE-MIB.mib
|   ├── IEEE8021-TC-MIB.mib
|   ├── IEEE8023-LAG-MIB.mib
|   ├── IEEE8023-MSTP-MIB.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

6.SNMPv2-MIB.mib

7.IANAifType-MIB.mib

8.IEEE8023-LAG-MIB.mib

9.IF-MIB.mib

10.EtherLike-MIB.mib

11.IEEE8021-PAE-MIB.mib

12.BRIDGE-MIB.mib

13.P-BRIDGE-MIB.mib

14.RFC1271-MIB.mib

15.RMON-MIB.mib

16.TOKEN-RING-RMON-MIB.mib

17.RMON2-MIB.mib

18.Q-BRIDGE-MIB.mib

19.INET-ADDRESS-MIB.mib

20.IEEE8021-TC-MIB.mib

21.IEEE8021-SPANNING-TREE-MIB.mib

22.IEEE8021-MSTP-MIB.mib

23.IANA-ADDRESS-FAMILY-NUMBERS-MIB.mib

24.LLDP-MIB.mib

25.LLDP-EXT-DOT1-MIB.mib

26.LLDP-EXT-DOT3-MIB.mib

27.LLDP-EXT-ODVA-MIB.mib

28.OSPF-MIB.mib

29.PTPBASE-MIB.mib

30.IEEE8021-AS-MIB.mib

31.IEEE8021-BRIDGE-MIB.mib

32.IEEE8021-ST-MIB.mib

33.IEEE8021-Q-BRIDGE-MIB.mib

MIB Tree

iso(1)

|-std(0)-iso8802(8802)-ieee802dot1(1)-ieee802dot1mibs(1)

| |-ieee8021paeMIB(1) : IEEE8021-PAE-MIB.mib

| |-ieee8021SpanningTreeMib(3) : IEEE8021-SPANNING-TREE-MIB.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, mxPoee.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
   |      |      |      |- portInterfacce     : 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

| | | |- layer2Diagnosic : mxLldp.mib, mxTcst.mib, mxPortMirror.mib, mxRmon.mib, mxFiberCheck.mib, mxTracking.mib

| | | |- layer3Diagnosic

| | | |- layer2Multicast : mxIgmpSnp.mib

| | | |- layer3Multicast

| | |-routing(605)

| | | |- l3Genral : mxIpIf.mib, mxArp.mib

| | | |- unicastRouting : mxUnicastRoutingTable.mib, mxStaticRoute.mib, mxOspf.mib

| | | |- multicastRouting : mxMulticastRouting.mib, mxPimSm.mib

| | | |- l3Redundant : 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.
- **-**: 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
Locator	R/W	R/W	R
Reboot	R/W	R/W	-
Reset to Default Settings	R/W	-	-
Auto-save to Startup	R/W	R/W	-
Advanced Mode	R/W	R/W	R/W
Change Language	R/W	R/W	R/W
Log Out	R/W	R/W	R/W

System

Settings	Admin	Supervisor	User
Device Summary	R	R	R
System Management			
Information Settings	R/W	R/W	R
Firmware Upgrade	R/W	-	-
Config Backup and Restore	R/W	-	-
Account Management			
User Accounts	R/W	-	-
Online Accounts	R/W	-	-
Password Policy	R/W	-	-
Management Interface			
User Interface	R/W	-	-
Hardware Interfaces	R/W	R/W	R
SNMP	R/W	-	-
RMON1 (Only in CLI)	R/W	R/W	R
Time			
System Time	R/W	R/W	R
NTP Server	R/W	R/W	R
Time Synchronization	R/W	R/W	R

Port

Settings	Admin	Supervisor	User
Port Interface			
Port Settings	R/W	R/W	R
Linkup Delay	R/W	R/W	R
Link Aggregation	R/W	R/W	R
PoE **(for PoE models)**	R/W	R/W	R

Layer 2 Switching

Settings	Admin	Supervisor	User
VLAN	R/W	R/W	R
GARP	R/W	R/W	R
MAC			
Static Unicast	R/W	R/W	R
MAC Address Table	R/W	R/W	R
QoS			
Classification	R/W	R/W	R
Ingress Rate Limit	R/W	R/W	R
Scheduler	R/W	R/W	R
Egress Shaper	R/W	R/W	R
Multicast			
IGMP Snooping	R/W	R/W	R

Settings	Admin	Supervisor	User
GMRP	R/W	R/W	R
Static Multicast	R/W	R/W	R

IP Configuration

Settings	Admin	Supervisor	User
IP Configuration (for L2 models)	R/W	R/W	R

Network Interface

Settings	Admin	Supervisor	User
Network Interface (for L3 models)	R/W	R/W	R

Redundancy

Settings	Admin	Supervisor	User
Layer 2 Redundancy			
Spanning Tree	R/W	R/W	R
Turbo Ring v2	R/W	R/W	R
Turbo Chain	R/W	R/W	R
MRP	R/W	R/W	R
Multiple Dual Homing	R/W	R/W	R
Multiple Network Coupling	R/W	R/W	R

Settings	Admin	Supervisor	User
IEC 62439-3 (for MDS-G4000-L2 models)			
PRP / HSR	R/W	R/W	R
Supervision Frame	R/W	R/W	R
Layer 3 Redundancy (for L3 models)			
VRRP	R/W	R/W	R
Tracking	R/W	R/W	R

Network Service

Settings	Admin	Supervisor	User
DHCP Server (for L2 models)	R/W	R/W	R
DHCP Relay Agent	R/W	R/W	R
DNS Settings	R/W	R/W	R

Routing

Settings	Admin	Supervisor	User
Unicast Route			
Static Routing	R/W	R/W	R
RIP	R/W	R/W	R
OSPF	R/W	R/W	R

Settings	Admin	Supervisor	User
Routing Table	R	R	R
Multicast Route			
PIM-DM	R/W	R/W	R
PIM-SM	R/W	R/W	R
Multicast Local Route	R/W	R/W	R
Multicast Routing Table	R	R	R

Security

Settings	Admin	Supervisor	User
Device Security			
Login Policy	R/W	R	R
Trusted Access	R/W	R	R
SSH & SSL	R/W	R/W	-
Network Security			
IEEE 802.1X	R/W	R/W	R
MAC Authentication Bypass	R/W	R/W	R
MACsec	R/W	R/W	R
Port Security	R/W	R/W	R
Traffic Storm Control	R/W	R/W	R
Access Control List	R/W	R/W	R
Network Loop Protection	R/W	R/W	R
Binding Database	R/W	R/W	R

Settings	Admin	Supervisor	User
DHCP Snooping	R/W	R/W	R
IP Source Guard	R/W	R/W	R
Dynamic ARP Inspection	R/W	R/W	R
Authentication			
Login Authentication	R/W	-	-
RADIUS	R/W	-	-
TACACS+	R/W	-	-

Diagnostics

Settings	Admin	Supervisor	User
System Status			
Resource Utilization	R	R	R
Fiber Check	R/W	R/W	R
Module Information	R	R	R
Network Status			
Network Statistics	R	R	R
LLDP	R/W	R/W	R
ARP Table	R	R	R
Tools			
Port and VLAN Mirroring	R/W	R/W	R
Ping	R/W	R/W	R/W
Event Logs and Notifications			

Settings	Admin	Supervisor	User
Event Logs	R/W	R/W	R
Event Notifications	R/W	R/W	R
Syslog	R/W	R/W	-
SNMP Trap / Inform	R/W	-	-
Email Settings	R/W	R	R
Relay Alarm	R/W	R/W	R

Industrial Application

Settings	Admin	Supervisor	User
IEC 61850			
MMS	R/W	R/W	R
GOOSE Check	R/W	R/W	R
Modbus TCP	R/W	R/W	R
EtherNet / IP	R/W	R/W	R
PROFINET	R/W	R/W	R



Moxa Inc.
Copyright © 2026 Moxa, Inc. All rights reserved. Reproduction without permission is prohibited. Trademarks and logos are copyrights of their respective owners.

www.moxa.com/products