PT-G7728/G7828 Series User Manual

Version 1.7, February 2026

www.moxa.com/products

PT-G7728/G7828 Series User Manual

The software described in this manual is furnished under a license agreement and may be used only in accordance with the terms of that agreement.

Copyright Notice

Trademarks

Disclaimer

- Information in this document is subject to change without notice and does not represent a commitment on the part of Moxa.
- Moxa provides this document as is, without warranty of any kind, either expressed or implied, including, but not limited to, its particular purpose. Moxa reserves the right to make improvements and/or changes to this manual, or to the products and/or the programs described in this manual, at any time.
- Information provided in this manual is intended to be accurate and reliable. However, Moxa assumes no responsibility for its use, or for any infringements on the rights of third parties that may result from its use.
- This product might include unintentional technical or typographical errors. Changes are periodically made to the information herein to correct such errors, and these changes are incorporated into new editions of the publication.

Technical Support Contact Information

www.moxa.com/support

Table of Contents

1. About this Manual

Thank you for purchasing a Moxa managed Ethernet switch. Read this user's manual to learn how to connect your Moxa switch to Ethernet-enabled devices used for industrial applications.

A synopsis of chapters 2 and 3 are given below:

- **Chapter 2: Getting Started**

  In this chapter, we explain the initial installation process for a Moxa switch. Moxa switches provide three interfaces to access the configuration settings: serial console interface, command line interface, and web console interface.

- **Chapter 3: Featured Functions**

  In this chapter, we explain how to access a Moxa switch's various configuration, monitoring, and management functions. The functions can be accessed by serial console, Telnet console, and web console (web browser). We describe how to configure the switch functions via web console, which provides the most user-friendly way to configure a Moxa switch.

2. Getting Started

In this chapter, we explain how to install a Moxa switch for the first time. There are three ways to access the Moxa switch's configuration settings: serial console, command line interface, or web-based interface. If you do not know the Moxa switch's IP address, you can open the serial console by connecting the Moxa switch to a PC's RJ45 port with an RJ45 cable. You can open the Telnet or web-based console over an Ethernet LAN or over the Internet.

Serial Console Configuration (115200, None, 8, 1, VT100)

NOTE

A Moxa switch allows multi-session connections (up to 6) by connecting to the web console and another console (serial or Telnet) at the same time.

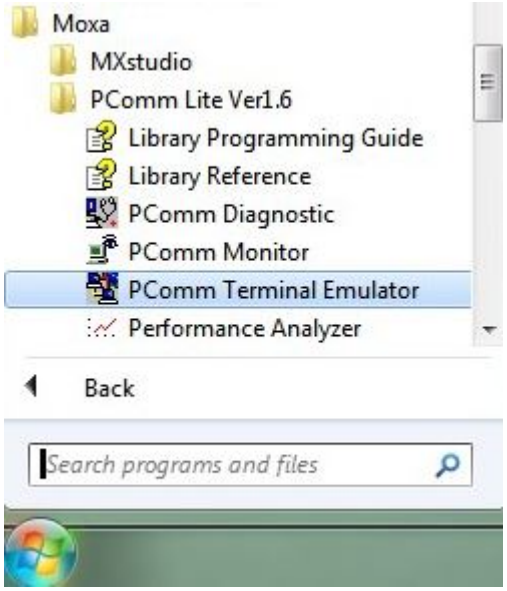
NOTE

We recommend using **PComm Lite** terminal emulator when opening the serial console. This software can be downloaded free of charge from the Moxa website.

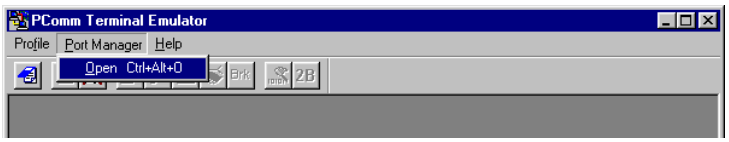
Before running the PComm Terminal Emulator software, install the serial console driver on your PC and then connect the Moxa switch's RJ45 console port to your PC's USB port with a RJ45-to-USB cable.

After installing PComm Terminal Emulator, open the Moxa switch's serial console as follows:

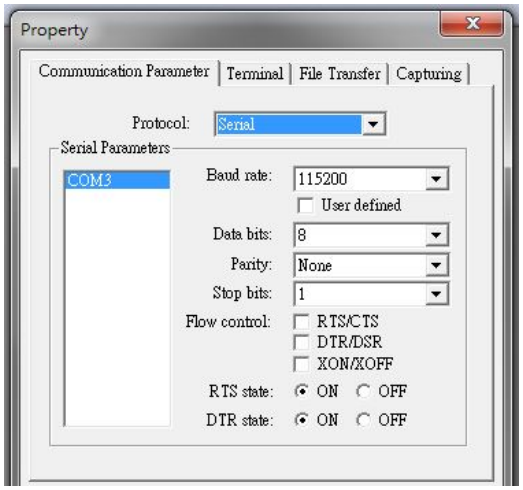
1. From the Windows desktop, click **Start > Moxa > PComm Lite Ver1.6 > Terminal Emulator**.



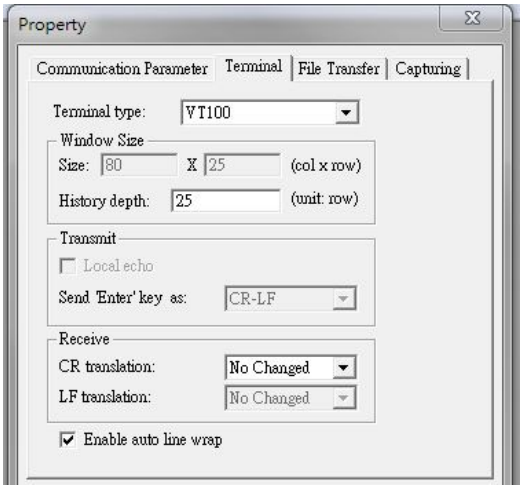
2. Select **Open** under the **Port Manager** menu to open a new connection.



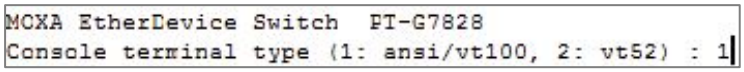
3. The **Property** window should open. On the **Communication Parameter** tab for **Ports**, select the COM port that is being used for the console connection. Set the other fields as follows: **115200** for **Baud Rate**, **8** for **Data Bits**, **None** for **Parity**, and **1** for **Stop Bits**.



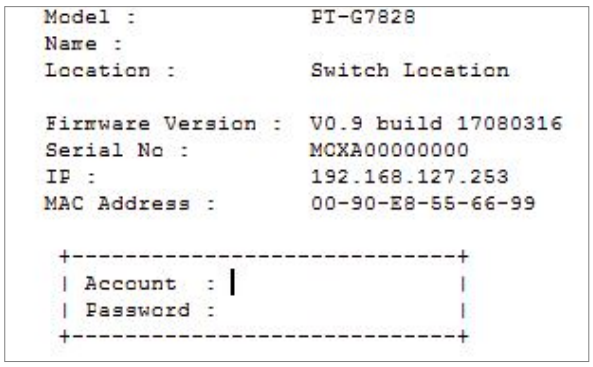
4. On the **Terminal** tab, select **VT100** for **Terminal Type**, and then click **OK** to continue.



5. In the terminal window, the Moxa switch will prompt you to select a terminal type. Enter **1** to select **ansi/vt100** and then press **Enter**.



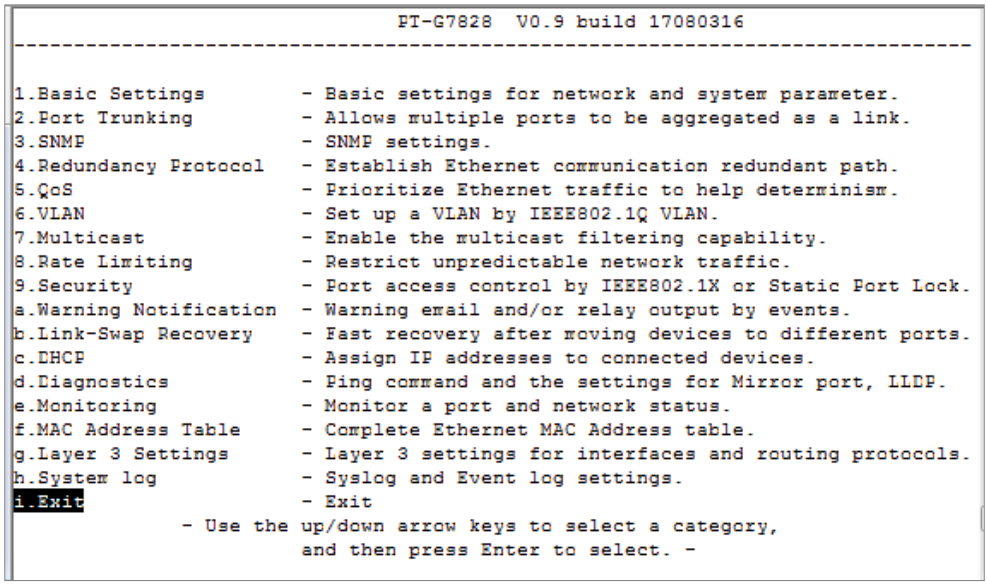
6. The serial console will prompt you to log in. Press **Enter** and select **admin** or **user**. Use the down arrow key on your keyboard to select the **Password** field and enter a password if desired. This password will be required to access any of the consoles (web, serial, Telnet).



NOTE

By default, the password assigned to the Moxa switch is **moxa**. Be sure to change the default password after you first log in to help keep your system secure.

7. The **Main Menu** of the Moxa switch's serial console will be displayed. (In PComm Terminal Emulator, you can adjust the font by selecting **Font...** from the **Edit** menu.)



8. Use the following keys on your keyboard to navigate the Moxa switch's serial console:

Key	Function
Up, down, right, left arrow keys, Tab	Move the onscreen cursor
Enter	Display and select options
Space	Toggle options
Esc	Previous menu

Configuration by Command Line Interface (CLI)

Opening the Moxa switch's Telnet or web console over a network requires that the PC host and Moxa switch are on the same logical subnet. You may need to adjust your PC host's IP address and subnet mask. By default, the Moxa switch's IP address is 192.168.127.253 and the Moxa switch's subnet mask is 255.255.255.0 (referred to as a Class B network). 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

To connect to the Moxa switch's Telnet or web console, your PC host and the Moxa switch must be on the same logical subnet.

NOTE

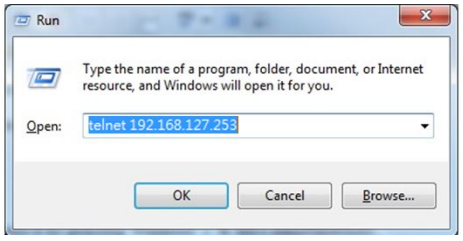
When connecting to the Moxa switch's Telnet or web console, first connect one of the Moxa switch's Ethernet ports to your Ethernet LAN, or directly to your PC's Ethernet port. You may use either a straight-through or cross-over Ethernet cable.

NOTE

The Moxa switch's default IP address is 192.168.127.253.

After making sure that the Moxa switch is connected to the same LAN and logical subnet as your PC, open the Moxa switch's Telnet console as follows:

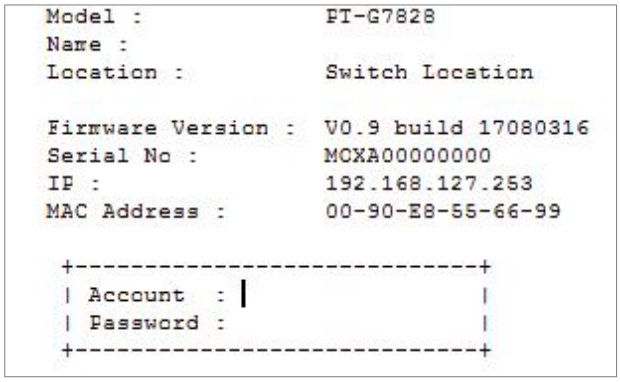
1. Click **Start > Run** from the Windows Start menu and then Telnet to the Moxa switch's IP address from the Windows **Run** window. You may also issue the Telnet command from a DOS prompt.



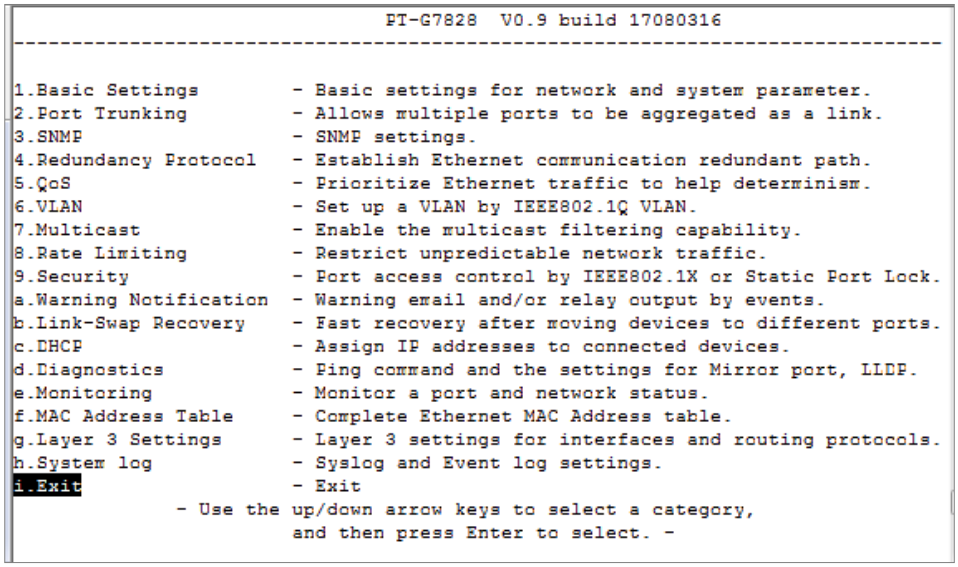
2. In the terminal window, the Telnet console will prompt you to select a terminal type. Type **1** to choose **ansi/vt100**, and then press **Enter**.

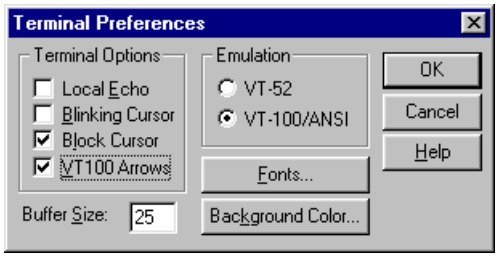
```
MOXA EtherDevice Switch  PT-G7828
Console terminal type (1: ansi/vt100, 2: vt52) : 1
```

3. The Telnet console will prompt you to log in. Press **Enter** and then select **admin** or **user**. Use the down arrow key on your keyboard to select the **Password** field and enter a password if desired. This password will be required to access any of the consoles (web, serial, Telnet). If you do not wish to create a password, leave the **Password** field blank and press **Enter**.



4. The **Main Menu** of the Moxa switch's Telnet console should appear.





5. Use the following keys on your keyboard to navigate the Moxa switch's Telnet console:

Key	Function
Up, down, right, left arrow keys, Tab	Move the onscreen cursor
Enter	Display and select options
Space	Toggle options
Esc	Previous menu

NOTE

The Telnet console looks and operates in precisely the same manner as the serial console.

Configuration by Web Console

The Moxa switch's web console is a convenient platform for modifying the configuration and accessing the built-in monitoring and network management functions. You can open the Moxa switch's web console using a standard web browser, such as Internet Explorer.

NOTE

When connecting to the Moxa switch's Telnet or web console, your PC host and the Moxa switch must be on the same logical subnet.

NOTE

If the Moxa switch is configured for other VLAN settings, you must make sure your PC host is on the management VLAN.

NOTE

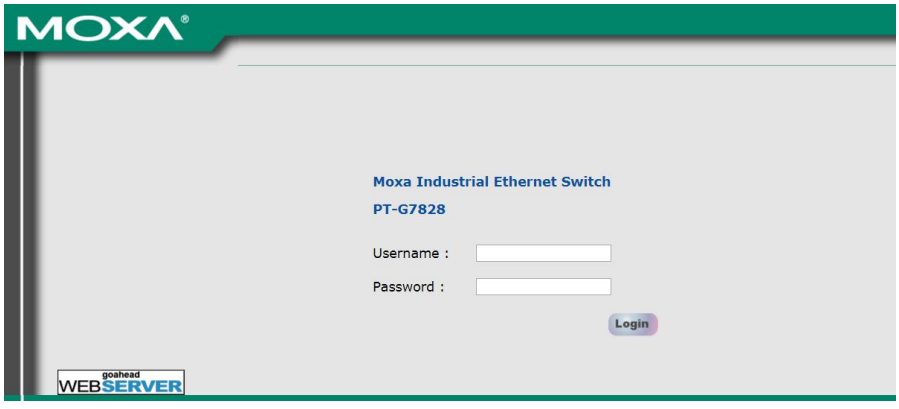
When connecting to the Moxa switch's Telnet or web console, first connect one of the Moxa switch's Ethernet ports to your Ethernet LAN, or directly to your PC's Ethernet port. You may use either a straight-through or cross-over Ethernet cable.

NOTE

The Moxa switch's default IP address is 192.168.127.253.

After making sure that the Moxa switch is connected to the same LAN and logical subnet as your PC, open the Moxa switch's web console as follows:

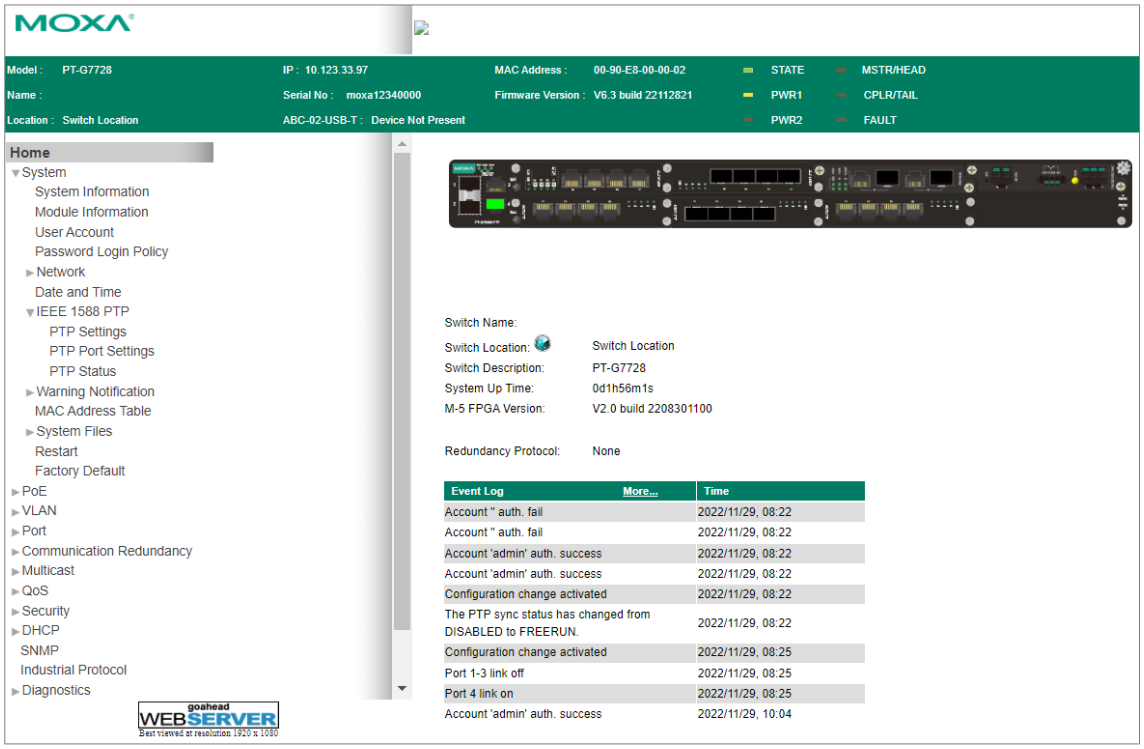
1. Connect your web browser to the Moxa switch's IP address by entering it in the **Address** or **URL** field.
2. The Moxa switch's web console will open, and you will be prompted to log in. Select the login account (admin or user) and enter the **Password**. This password will be required to access any of the consoles (web, serial, Telnet). If you do not wish to create a password, leave the **Password** field blank and press **Enter**.



NOTE

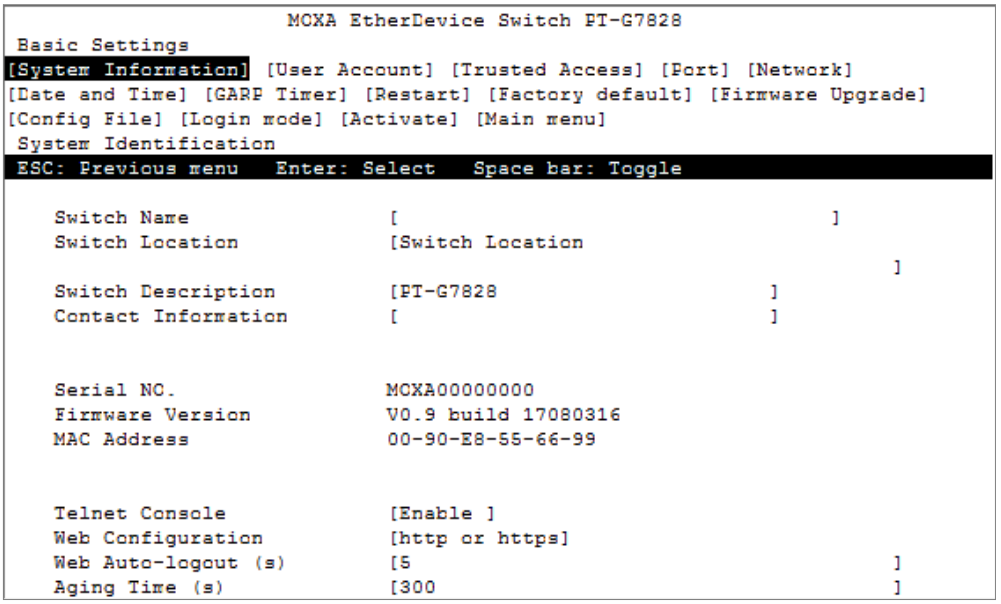
By default, the password assigned to the Moxa switch is moxa. Be sure to change the default password after you first log in to help keep your system secure.

3. After logging in, you may need to wait a few moments for the web console to appear. Use the folders in the left navigation panel to navigate between different pages of the configuration options.



Disabling Telnet and Browser Access

If you are connecting the Moxa switch to a public network but do not intend to manage it over the network, we suggest disabling both the Telnet and web consoles. This is done from the serial console by navigating to **System Identification** under **Basic Settings > System Information**. Disable or enable the **Telnet Console** and **Web Configuration** as shown below:



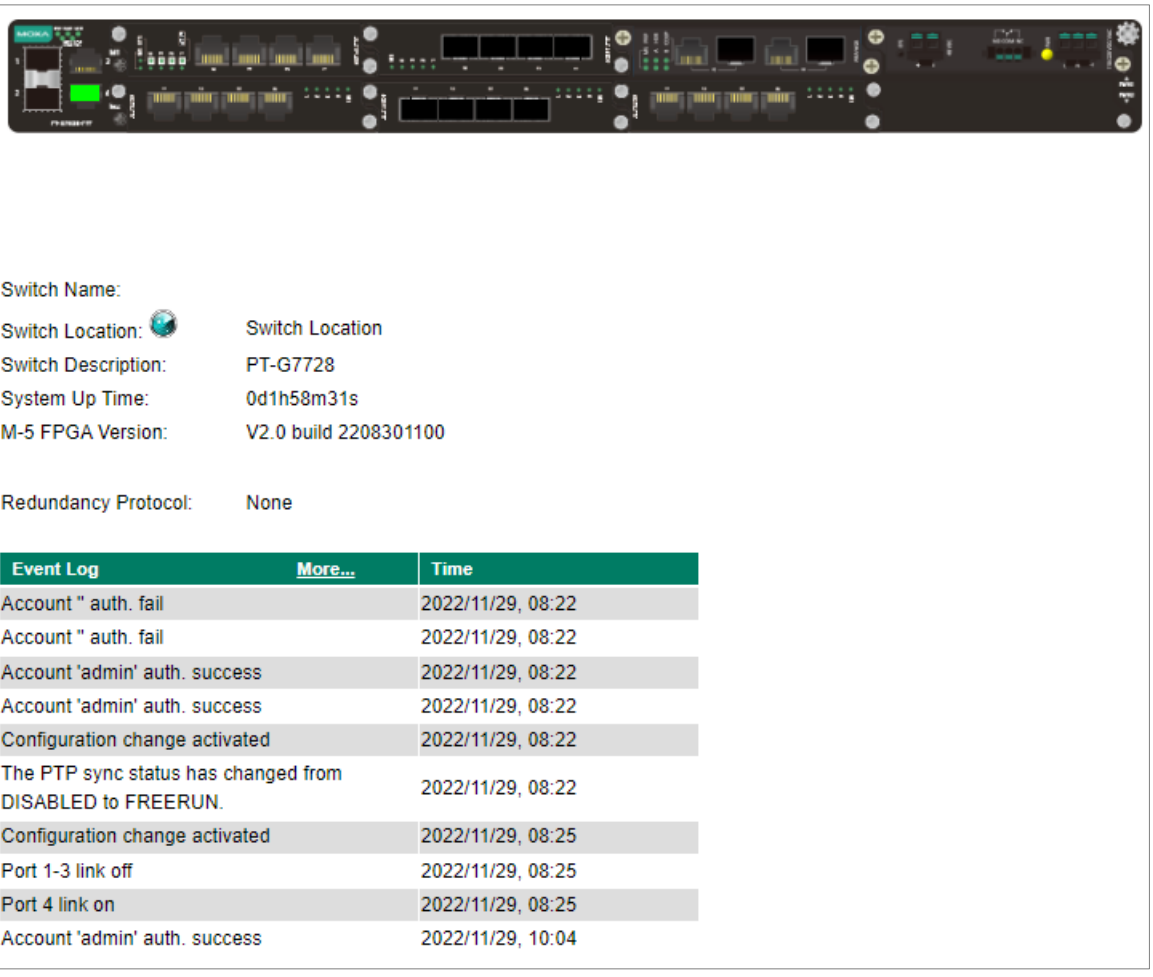
3. Featured Functions

In this chapter, we explain how to access the Moxa switch's various configuration, monitoring, and management functions. These functions can be accessed by serial console, Telnet console, or web console. The serial console can be used if you do not know the Moxa switch's IP address. To access the serial console, connect switch's USB port to your PC's COM port. The Telnet and web consoles can be opened over an Ethernet LAN or the Internet.

The web console is the most user-friendly interface for configuring a Moxa switch. In this chapter, we use the web console interface to introduce the console functions. There are only a few differences between the web console, serial console, and Telnet console.

Home

The **Home** page shows the summary of the Moxa switch information including System Information, Redundancy Protocol, Event Log, and Device virtualization panel. By showing the switch's information and event log, the operators can easily understand the system and port link status.

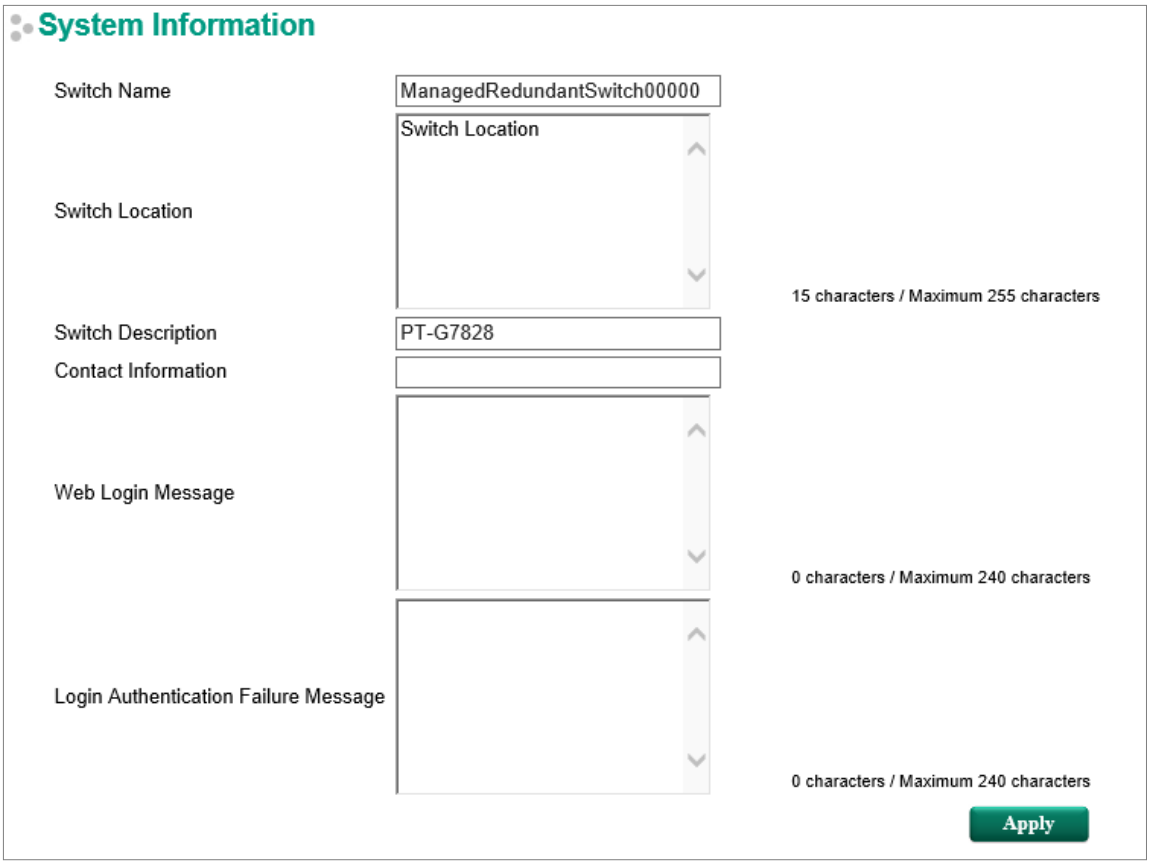


System Settings

The **System Settings** section includes the most common settings required by administrators to maintain and control a Moxa switch.

System Information

Define **System Information** items to make it easier to identify different switches that are connected to your network.



Switch Name

Setting	Description	Factory Default
Max. 30 characters	This option is useful for differentiating between the roles or applications of different units. Example: ManagedRedundantSwitch00000	none

NOTE

The Switch Name field does not allow spaces.

Switch Location

Setting	Description	Factory Default
Max. 255 characters	This option is useful for differentiating between the locations of different switches. Example: production line 1.	Switch Location

Switch Description

Setting	Description	Factory Default
Max. 30 characters	This option is useful for recording a more detailed description of the unit.	Switch Model name

Contact Information

Setting	Description	Factory Default
Max. 30 characters	This option is useful for providing information about who is responsible for maintaining this unit and how to contact this person.	None

Web Login Message

Setting	Description	Factory Default
Max. 240 characters	This option is useful as it shows a message when a user's login is successful	Switch Location

NOTE

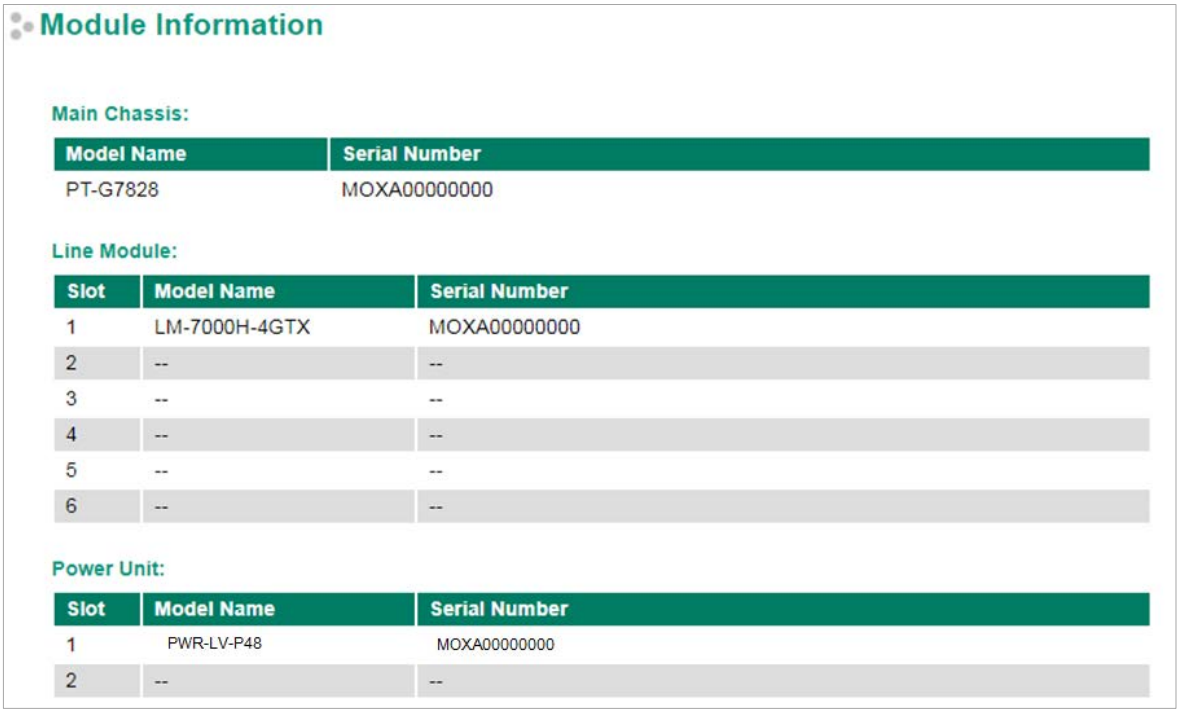
- If a message starts with a single quote and contains another single quote, the content within the single quotes will be extracted after import, and the initial single quote will disappear.
- Similarly, if a message starts with a double quote and contains another double quote, the content within the double quotes will be extracted after import, and the initial double quote will disappear.
- If a message starts with a single or double quote but does not contain another corresponding quote, the initial quote will disappear after import, and the rest of the message will remain unaffected.
- If a message starts with a single quote and contains double quotes, the initial single quote will disappear after import, and the rest of the message will remain unaffected.
- Similarly, if a message starts with a double quote and contains single quotes, the initial double quote will disappear after import, and the rest of the message will remain unaffected.

Login Authentication Failure Message

Setting	Description	Factory Default
Max. 240 characters	This option is useful as it shows a message when a user's login has failed	Switch Location

Module Information

This page displays the model name and serial number information of the device, including main chassis, line module, and power module. Below is an example of the information that will be displayed.

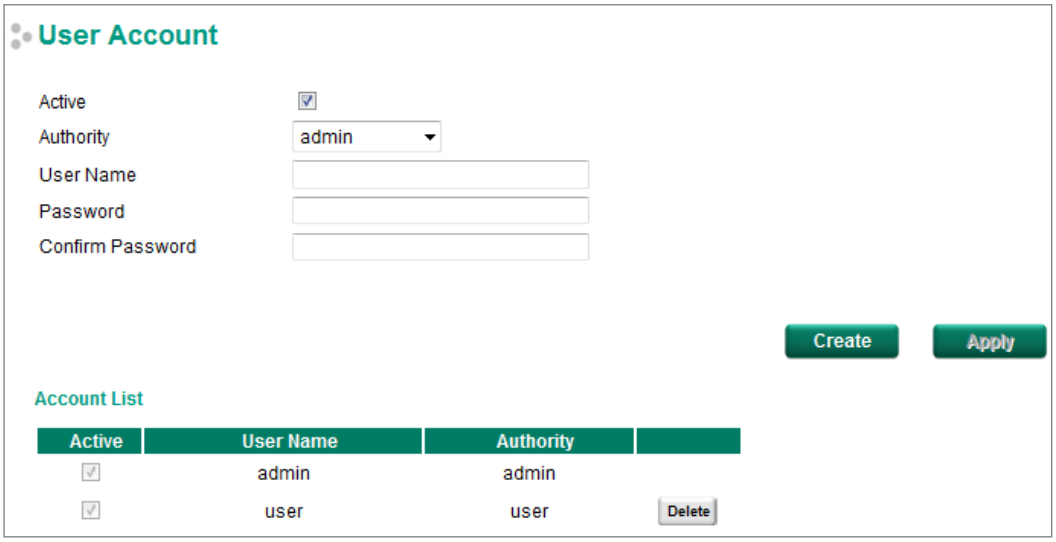


User Account

The Moxa switch supports the management of accounts, including establishing, activating, modifying, disabling, and removing accounts. There are two levels of configuration access: admin and user. Accounts with **admin** authority have read/write access of all configuration parameters, whereas accounts with **user** authority only have read access to view configuration items.

NOTE

1. In order to maintain a higher level of security, we strongly suggest that you change the password after you first log in.
2. By default, the **admin** user account cannot be deleted or disabled.



Active

Setting	Description	Factory Default
Checked	This account can access the switch's configuration settings.	Checked
Unchecked	This account cannot access the switch's configuration settings.	

Authority

Setting	Description	Factory Default
admin	This account has read/write access of all configuration parameters.	admin
User	This account can only view configuration parameters.	

Creating a New Account

Click Create, type in the username and password, and assign an authority to the new account. Click Apply to add the account to the Account List table.

Setting	Description	Factory Default
User Name (Max. of 30 characters)	User Name	None
Password	Password for the user account. (starting from v6.4 firmware, password length increased from 16 to 32 characters.)	None

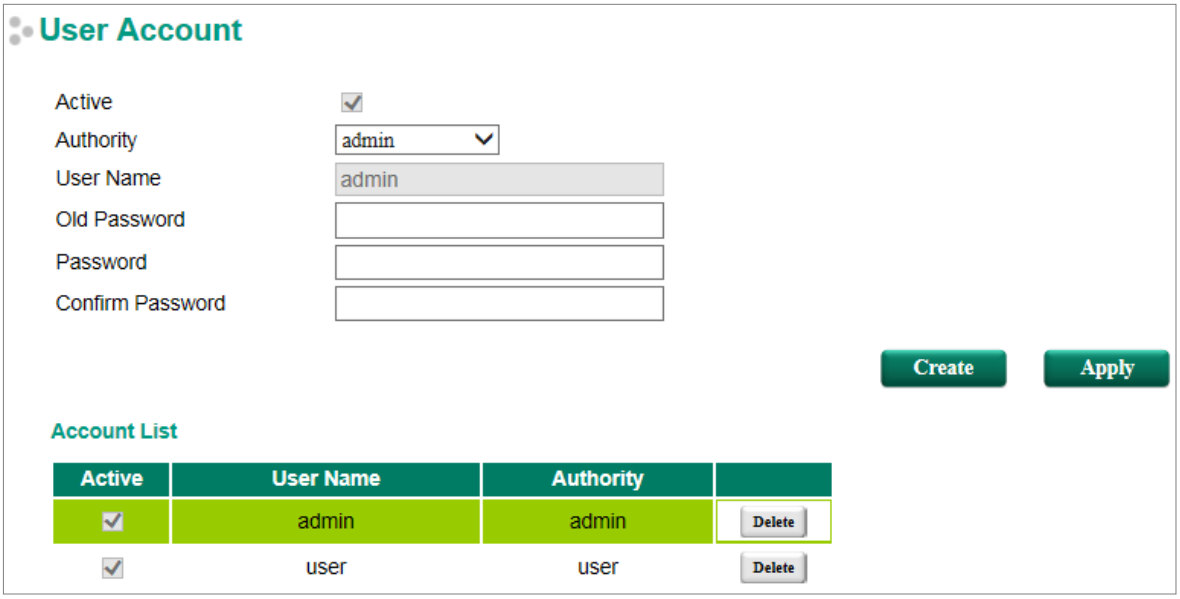
NOTE

- The password length has been increased from 16 to 32 bytes starting with firmware v6.4. Due to the difference in password length, we recommend upgrading directly to v6.5 from v6.3 and previous versions to avoid the following configurations from being reset to the default. This issue will be fixed in v6.5. When you upgrade to V6.4, the following will be reset; all other configuration settings will be retained.
  - Admin/User password
  - Account List
  - Login Authentication configuration
  - SNMP v3 account

  Due to the difference in password length, some upgrade/downgrade paths will result in above mentioned four configurations being reset to factory default values.
  - v6.3 and prior → v6.4 (above mentioned configurations set to factory default)
  - v6.4 → v6.3 (above mentioned configurations set to factory default)
  - v6.5 and later → v6.3 (above mentioned configurations set to factory default)
  - v6.3 and prior → v6.5 by export and import of configurations (above mentioned set to factory default)
- We recommend upgrading directly to firmware v6.5.
  v6.3 and prior → v6.5 and later (configuration setting Passwords with > 16 characters are only supported via the "unlock" function in MXconfig and can only be changed via the Web UI.

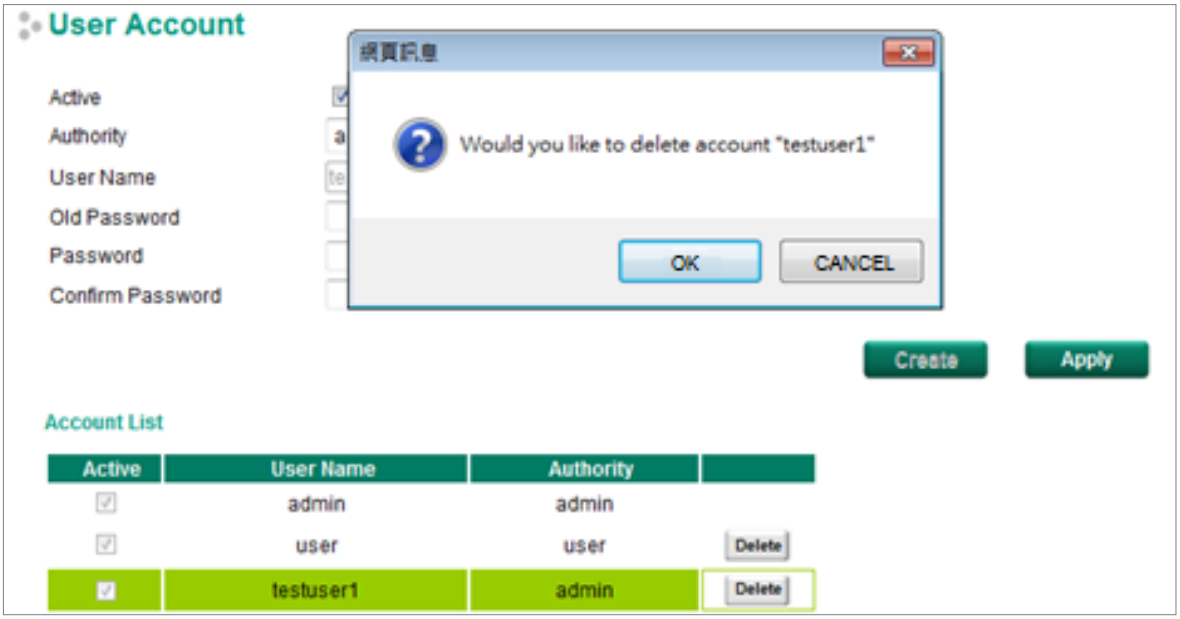
Modifying an Existing Account

Select an existing account from the Account List table, modify the account details, and then click **Apply** to save the changes.



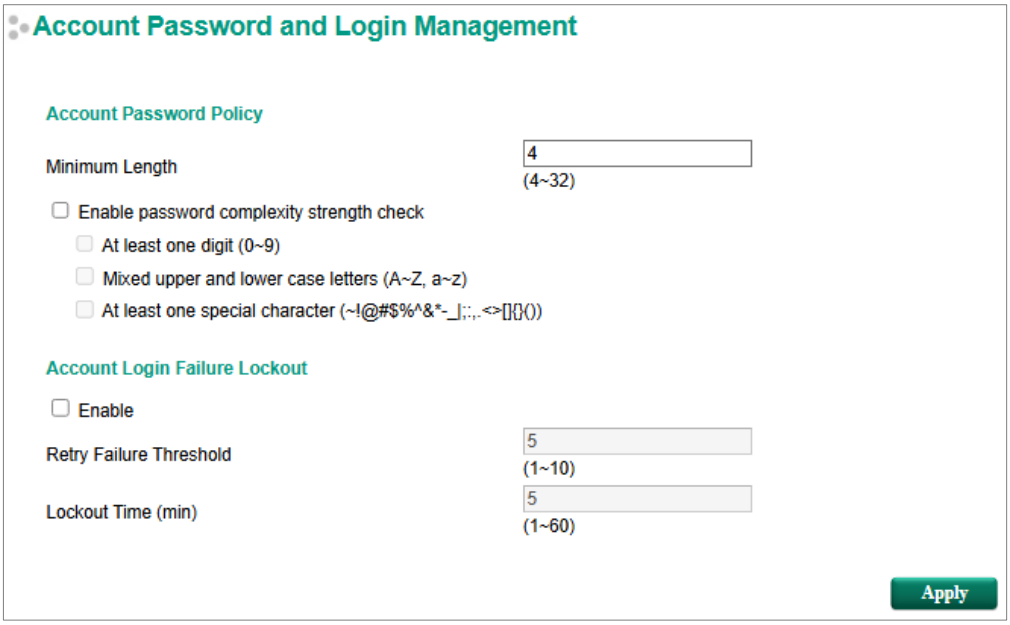
Deleting an Existing Account

Select an account from the Account List table and then click **Delete** to delete the account.



Password Login Policy

In order to prevent hackers from cracking the password, Moxa switches allow users to configure a password for their account and lock the account in the event that the wrong password is entered. The account password policy requires passwords to be of a minimum length and complexity with a strength check. If Account Login Failure Lockout is enabled, you will need to configure the Retry Failure Threshold and Lockout Time parameters. If the number of login attempts exceeds the Retry Failure Threshold, users will need to wait the number of minutes configured in Lockout Time before trying again.



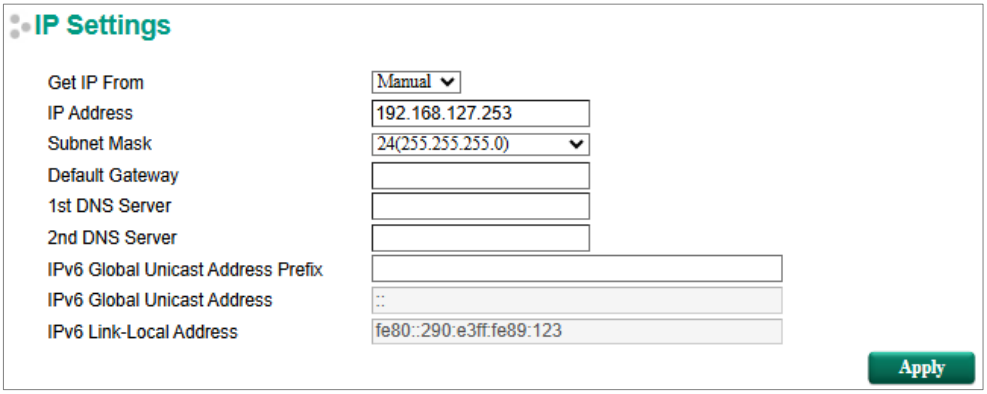
Network

Network configuration allows users to configure both IPv4 and IPv6 parameters for management access over the network. The Moxa switch supports both IPv4 and IPv6, and can be managed through either of these address types.

IP Settings

The IPv4 settings include the switch's IP address and subnet mask, as well as the IP address of the default gateway. In addition, input cells are provided for the IP addresses of a 1st and 2nd DNS server.

The IPv6 settings include two distinct address types—Link-Local Unicast addresses and Global Unicast addresses. A Link-Local address makes the switch accessible over IPv6 for all devices attached to the same local subnet. To connect to a larger network with multiple segments, the switch must be configured with a Global Unicast address.



Get IP From

Setting	Description	Factory Default
DHCP	The Moxa switch's IP address will be assigned automatically by the network's DHCP server.	Manual
BOOTP	The Moxa switch's IP address will be assigned automatically by the network's BootP server.	
Manual	The Moxa switch's IP address must be set manually.	

IP Address

Setting	Description	Factory Default
IP address for the Moxa switch	Assigns the Moxa switch's IP address on a TCP/IP network.	192.168.127.253

Subnet Mask

Setting	Description	Factory Default
Subnet mask for the Moxa switch	Identifies the type of network the Moxa switch is connected to (e.g., 255.255.0.0 for a Class B network, or 255.255.255.0 for a Class C network).	24(255.255.255.0)

Default Gateway

Setting	Description	Factory Default
IP address for gateway	Specifies the IP address of the router that connects the LAN to an outside network.	None

DNS Server IP Addresses

Setting	Description	Factory Default
1st DNS Server	Specifies the IP address of the DNS server used by your network. After specifying the DNS server's IP address, you can use the Moxa switch's URL (e.g., www.PT.company.com) to open the web console instead of entering the IP address.	None
2nd DNS Server	Specifies the IP address of the secondary DNS server used by your network. The Moxa switch will use the secondary DNS server if the first DNS server fails to connect.	None

IPv6 Global Unicast Address Prefix (Prefix Length: 64 bits) Default Gateway

Setting	Description	Factory Default
Global Unicast Address Prefix	The prefix value must be formatted according to RFC 2373 "IPv6 Addressing Architecture," using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields.	None

IPv6 Global Unicast Address

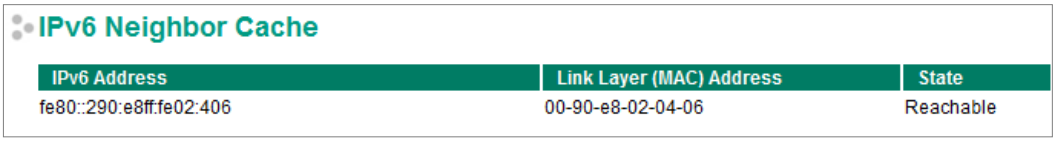
Setting	Description	Factory Default
None	Displays the IPv6 Global Unicast address. The network portion of the Global Unicast address can be configured by specifying the Global Unicast Prefix and using an EUI-64 interface ID in the low order 64 bits. The host portion of the Global Unicast address is automatically generated using the modified EUI-64 form of the interface identifier (Switch's MAC address).	None

IPv6 Link-Local Address

Setting	Description	Factory Default
None	The network portion of the Link-Local address is FE80, and the host portion of the Link-Local address is automatically generated using the modified EUI-64 form of the interface identifier (Switch's MAC address).	None

IPv6 Neighbor Cache

The IPv6 neighbor cache includes the neighboring node's IPv6 address, the corresponding Link-Layer address, and the current state of the entry.



NOTE

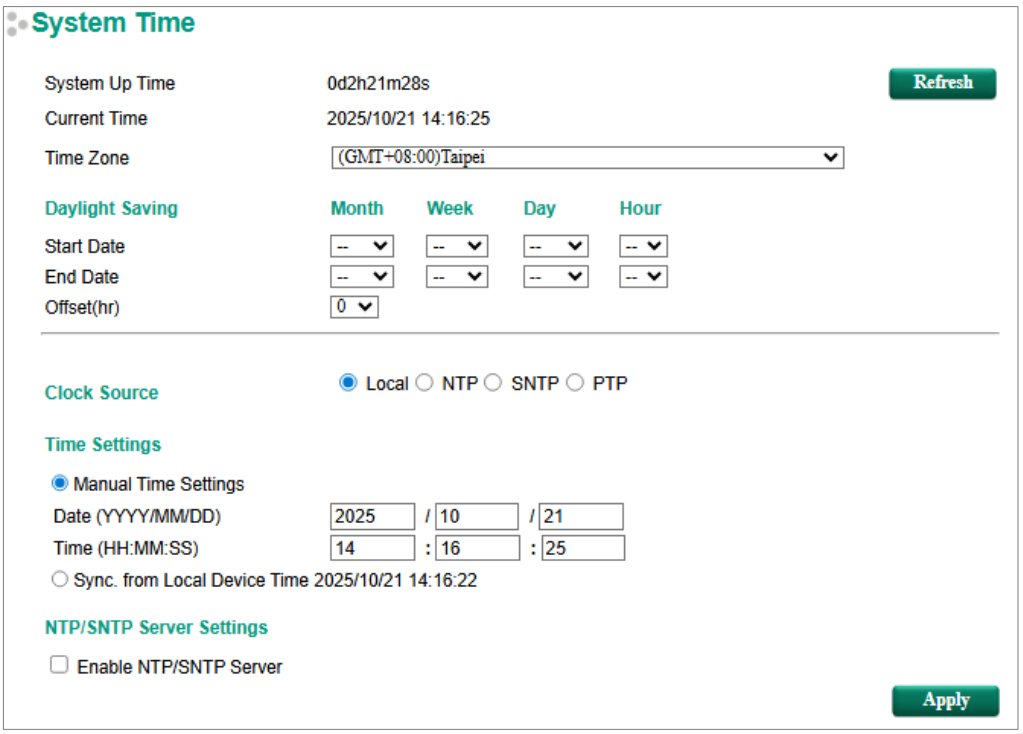
The IPv6 feature only works on the PT-G7728.

Date and Time

The Moxa switch has a time calibration function based on information from an NTP server or user specified time and date, allowing functions such as automatic warning emails to include a time and date stamp.

NOTE

The user must update the Current Time and Current Date after powering off the switch for a long period of time (for example a few days). The user must pay particular attention to this when there is no time server, LAN, or Internet connection.



System Up Time

Indicates how long the Moxa switch has been up and running since the last cold start.

Current Time

Setting	Description	Factory Default
User-specified time	Indicates time in yyyy-mm-dd format.	None

Clock Source

Setting	Description	Factory Default
Local	Configure clock source from local time	Local
NTP	Configure clock source from NTP	
SNTP	Configure clock source from SNTP	
PTP	Configure clock source from PTP	

Time Zone

Setting	Description	Factory Default
Time zone	Specifies the time zone, which is used to determine the local time offset from GMT (Greenwich Mean Time).	GMT (Greenwich Mean Time)

Daylight Saving Time

The Daylight Saving Time settings are used to automatically set the Moxa switch's time ahead according to national standards.

Start Date

Setting	Description	Factory Default
User-specified date	Specifies the date that Daylight Saving Time begins.	None

End Date

Setting	Description	Factory Default
User-specified date	Specifies the date that Daylight Saving Time ends.	None

Offset

Setting	Description	Factory Default
User-specified hour	Specifies the number of hours that the time should be set forward during Daylight Saving Time.	None

NOTE

Changing the time zone will automatically correct the current time. Be sure to set the time zone before setting the time.

If the NTP or SNTP options are enabled, you will also need to configure the following settings.

Time Server IP/Name

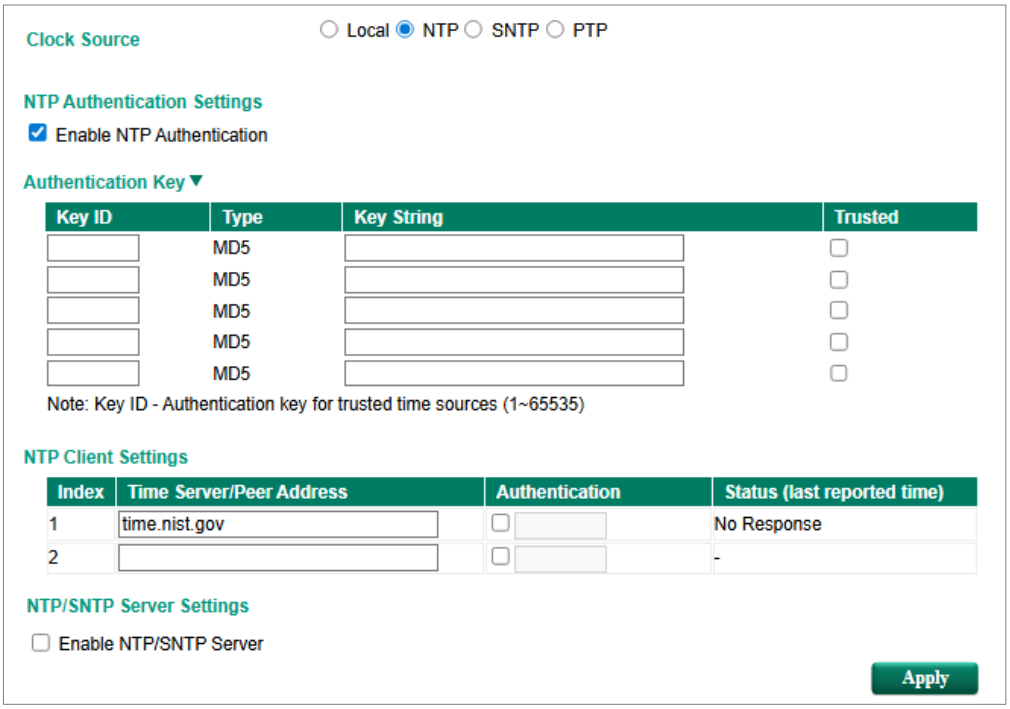
Setting	Description	Factory Default
1st address or name of IP server	The IP or domain address (e.g., 192.168.1.1, time.stdtime.gov.tw, or time.nist.gov).	None
IP address or name of secondary time server	The Moxa switch will try to locate the secondary SNTP server if the first SNTP server fails to connect.	
Query Period	The time period to sync with time server	600secs

Enable NTP/SNTP Server

Setting	Description	Factory Default
Enable/Disable	Enables SNTP/NTP server functionality for clients	Disabled

NTP Authentication Settings

NTP authentication is used to authenticate the NTP time synchronization packet. When you enable the NTP authentication, the device synchronizes to a time source/client/peer only if the packet carries the authentication key. The device will drop the packet that fails authentication and will not update at the local time.



Setting	Description
Enable NTP authentication	The NTP authentication will be enabled if the checkbox is selected

Authentication Key

This part indicates the key that can be recognized by this device, and a maximum of 5 keys can be stored in the device. Users can activate the key by selecting the 'Trusted' checkbox.

Setting	Description
Key ID	Indicate the ID of the key Range: 1 to 65535, Maximum of 5 key IDs can be stored
Key String	Defines the authentication key
Trusted	If selected, the key will be activated

NTP Client Settings

Setting	Description
Time Server/Peer Address	The time server or peer to sync to the NTP server
Authentication	Enter the key ID that you want to be used for authentication. The authentication key that user wants to be used to set the time
Status (Last Reported Time)	1. No Response: active or backup server is off for over 60 seconds 2. Active: shows active server last reported time (YYYY/MM/DD HH:MM:SS) 3. Backup: shows backup server last reported time (YYYY/MM/DD HH:MM:SS)

NTP/SNTP Server settings

Setting	Description	Default Value
Enable NTP/SNTP Server	The device will be the NTP server if the checkbox selected.	Disable

IEEE 1588

The following information is taken from the NIST website at http://ieee1588.nist.gov/intro.htm:

"Time measurement can be accomplished using the IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems (IEEE 1588-2008) to synchronize real-time clocks incorporated within each component of the electrical power system for power automation applications.

IEEE 1588, which was published in November 2002, expands the performance capabilities of Ethernet networks to control systems that operate over a communication network. In recent years an increasing number of electrical power systems have been using a more distributed architecture with network technologies that have less stringent timing specifications. IEEE 1588 generates a master-slave relationship between the clocks, and enforces the specific timing requirements in such power systems. All devices ultimately get their time from a clock known as the grandmaster clock. In its basic form, the protocol is intended to be administration free."

How Does an Ethernet Switch Affect 1588 Synchronization?

The following content is taken from the NIST website at http://ieee1588.nist.gov/switch.htm:

"An Ethernet switch potentially introduces multi-microsecond fluctuations in the latency between the 1588 grandmaster clock and a 1588 slave clock. Uncorrected, these fluctuations will cause synchronization errors. The magnitude of these fluctuations depends on the design of the Ethernet switch and the details of the communication traffic. Experiments with prototype implementations of IEEE 1588 indicate that with suitable care the effect of these fluctuations can be successfully managed. For example, use of appropriate statistics in the 1588 devices to recognize significant fluctuations and use suitable averaging techniques in the algorithms controlling the correction of the local 1588 clock will be good design means to achieve the highest time accuracy."

Can Ethernet switches be designed to avoid the effects of these fluctuations?

A switch can be designed to support IEEE 1588 while avoiding the effects of queuing. In this case two modifications to the usual design of an Ethernet switch are necessary:

Grandmaster Clock: Determines the time base for the system

Boundary Clock: Slave to the grandmaster clock and master to its slave

Ordinary Clock: Slave to its master

1. The **Boundary Clock and Transparent Clock** functionalities defined by IEEE 1588 must be implemented in the switch.
2. The switch must be configured so that it does not pass IEEE 1588 message traffic using the normal communication mechanisms of the switch.

Such an Ethernet switch will synchronize clocks directly connected to one of its ports to the highest possible accuracy.

PTP Settings

Enable IEEE 1588 PTP

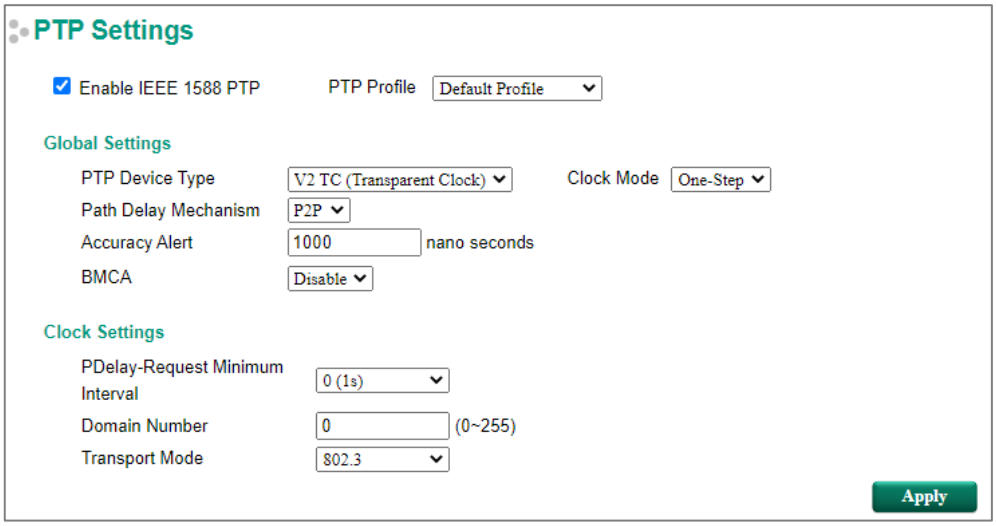
Setting	Description	Factory Default
Enable/Disable	Enable or disable the IEEE 1588 PTP feature globally.	Disabled

> **NOTE**
>
> When using IEEE 1588 PTP, you should first go to PTP port settings to enable the PTP feature on each port as well.

PTP Profile

Setting	Description	Factory Default
Default Profile	Configure as 'PTP default profile', which is defined in IEEE Std 1588-2008, Annex J.	Default Profile
Power Profile-2011	Configure as 'PTP power profile', which is defined in IEEE C37.238-2011.	
Power Profile-2017	Configure as 'PTP power profile', which is defined in IEEE C37.238-2017.	
IEC 61850-9-3	Configure as 'PTP power profile', which is defined in IEC 61850-9-3-2016.	

PTP Profile: Default Profile



Global Settings

PTP Device Type

Setting	Description	Factory Default
V2 BC (Boundary Clock)	Operates as an IEEE 1588 PTP v2 boundary clock.	V2 TC (Transparent Clock)
V2 TC (Transparent Clock)	Operates as an IEEE 1588 PTP v2 transparent clock.	

Clock Mode

Setting	Description	Factory Default
One-step	Configure as a one-step clock.	One-step
Two-step	Configure as a two-step clock.	

Path Delay Mechanism

Setting	Description	Factory Default
P2P	Configure as the peer-to-peer method. Power profile (C37.238) requires the peer-to-peer method.	P2P
E2E	Configure as the end-to-end method, which measures the propagation time between two PTP ports.	

Accuracy Alert

Setting	Description	Factory Default
50 to 250000000	Configure the time accuracy threshold.	1000

MCA

Setting	Description	Factory Default
Enable/Disable	Enable or disable Best Master Clock Algorithm (BMCA) Globally.	Disable

NOTE

Ensure all PTP devices are configured to the same PTP Delay Mechanism.

Clock Settings

PDelay-Request Minimum Interval

Setting	Description	Factory Default
1 (512ms) 0 (1 sec) 1 (2 sec) 2 (4 sec) 3 (8 sec) 4 (16 sec) 5 (32 sec)	Configure the minimum permitted mean time interval between successive Pdelay_Req messages of the P2P mode.	0 (1 sec)

Domain Number

Setting	Description	Factory Default
0 to 255	A domain defines the scope of communication, state, operations, data sets, and timescale of the PTP message.	0

Value(decimal)	Definition
0	Default domain
1	Alternate domain 1
2	Alternate domain 2
3	Alternate domain 3
4 to 127	User-defined domains
128 to 255	Reserved

NOTE

The switch and the grandmaster clock must be in the same PTP domain.

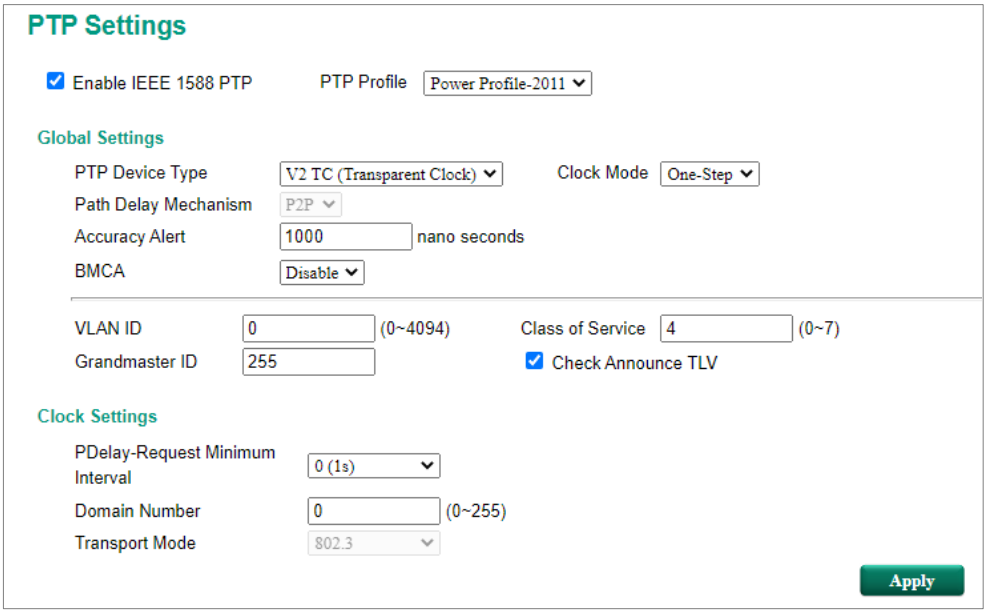
Transport Mode

Setting	Description	Factory Default
802.3	Configure PTP implementations directly using Ethernet format.	Default Profile: 802.3 Power Profile: fixed to 802.3 as C37.238 required
IPv4	Configure PTP implementations using UDP/IPv4 as a communication service.	

NOTE

Ensure all PTP devices are using the same communication service.

PTP Profile: Power Profile-2011/Power Profile-2017/IEC 61850-9-3



Global Settings

PTP Device Type

Setting	Description	Factory Default
V2 BC (Boundary Clock)	Operates as an IEEE 1588 PTP v2 boundary clock.	V2 TC (Transparent Clock)
V2 TC (Transparent Clock)	Operates as an IEEE 1588 PTP v2 transparent clock.	

Clock Mode

Setting	Description	Factory Default
One-step	Configure as a one-step clock.	One-step
Two-step	Configure as a two-step clock.	

Path Delay Mechanism

Setting	Description	Factory Default
P2P	Configure as the peer-to-peer method. Power profile (C37.238 or 61850-9-3) requires the peer-to-peer method.	P2P

Accuracy Alert

Setting	Description	Factory Default
50 to 250000000	Configure time accuracy threshold.	1000

MCA

Setting	Description	Factory Default
Enable/Disable	Enable or disable Best Master Clock Algorithm (BMCA) Globally.	Disable

VLAN ID

Setting	Description	Factory Default
0 to 4094	Only available in Power Profile-2011 mode. The reserved value 0 indicates that only the priority tag in 802.1Q is considered. This value should match the VLAN rules where the enabled PTP feature applies to the whole system. Take note of the VLAN settings of the device.	0

Class of Service

Setting	Description	Factory Default
0 to 7	Only available in Power Profile-2011 mode. Configure as an 802.1p priority tag. Lower values take precedence.	4

Grandmaster ID

Setting	Description	Factory Default
0 to 255	Only available in Power Profile-2011 and Power Profile-2017 mode. Configure the grandmaster ID to identify the grandmaster clock source.	255

Check Announce TLV

Setting	Description	Factory Default
Enable/Disable	Only available in Power Profile-2011 mode. When the profile type is the Power profile, the switch will not handle the PTP announce messages, which do not include length and value (TLV) extensions: Organization extension and Alternate timescale. Configure 'Check announce TLV' to enable or disable announce TLV checking.	Enabled

Clock Settings

PDelay-Request Minimum Interval

Setting	Description	Factory Default
1 (512ms) 0 (1 sec) 1 (2 sec) 2 (4 sec) 3 (8 sec) 4 (16 sec) 5 (32 sec)	Configure the minimum permitted mean time interval between successive Pdelay_Req messages of the P2P mode.	C37.238: 0 (1 sec) 61850-9-3: fixed to 0 (1 sec) as required.

Domain Number

Setting	Description	Factory Default
0 to 255	A domain defines the scope of communication, state, operations, data sets, and timescale of the PTP message. **Value(decimal) / Definition** 0 – Default domain 1 – Alternate domain 1 2 – Alternate domain 2 3 – Alternate domain 3 4 to 127 – User-defined domains 128 to 255 – Reserved	0

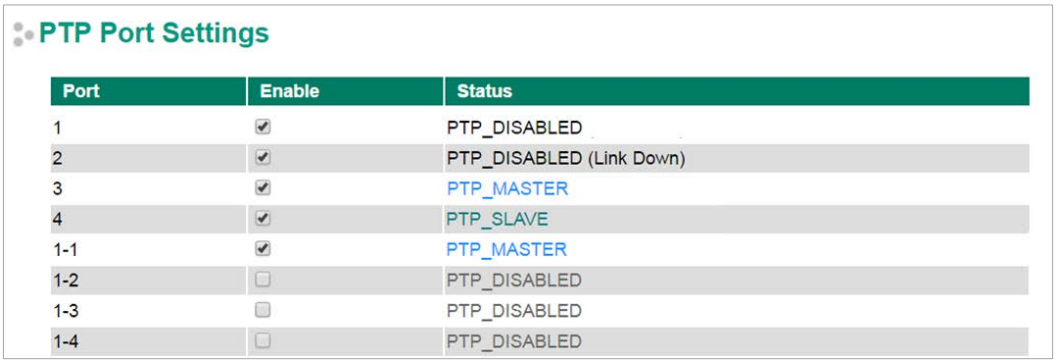
NOTE

The switch and the grandmaster clock must be in the same PTP domain.

Transport Mode

Setting	Description	Factory Default
802.3	Configure PTP implementations directly using Ethernet format.	Power Profile: fixed to 802.3 as C37.238 and 61850-9-3 required

PTP Port Settings



NOTE

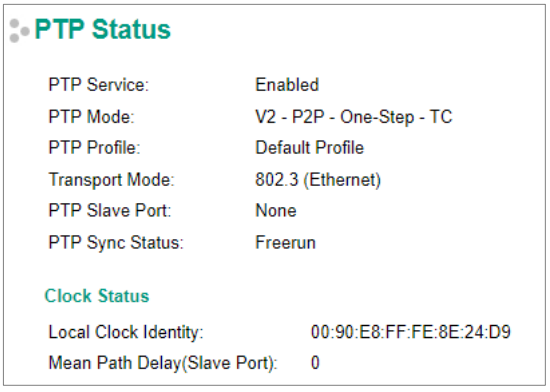
When enabling the PTP feature on each port, also enable the 'Enable IEEE 1588 PTP' on 'PTP settings.

PTP Port Settings

Setting	Description	Factory Default
Enable/Disable	PTP port status: • PTP_INITIALIZING: PTP port is initializing. No PTP messages on its communication path. • PTP_MASTER: The port is the source of time on the path served by the port. • PTP_DISABLED: A port in this state will not handle any PTP received messages except for management messages. • PTP_PASSIVE: The port is not the master on the path, nor does it synchronize to a master. • PTP_LISTENING: The port is waiting for the announce timeout interval to expire or to receive an Announce message from a master. • PTP_SLAVE: The port is synchronizing to the selected PTP master port.	PTP disabled

PTP Status

Indicates the current IEEE 1588 PTP status.

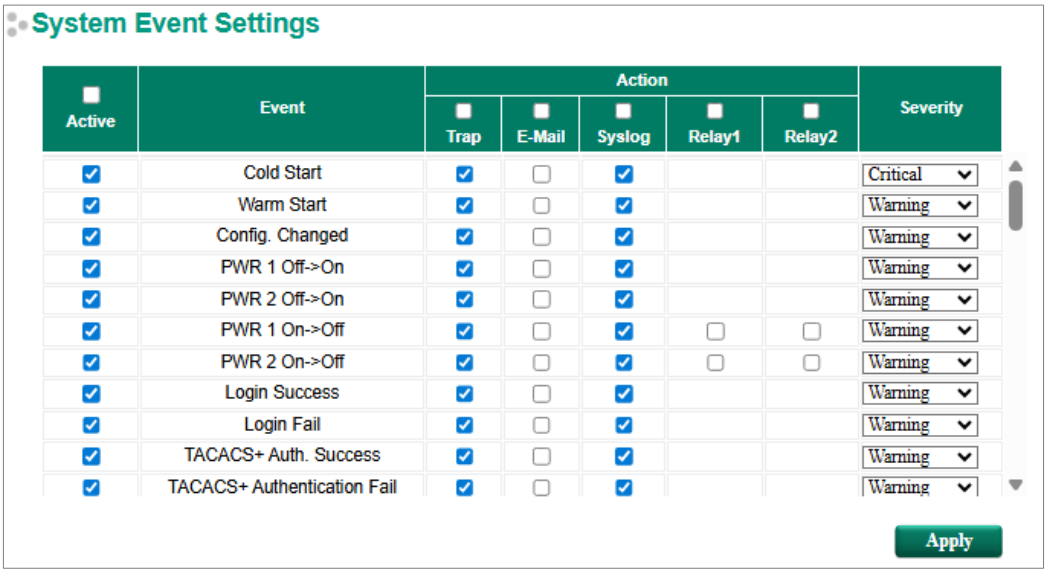


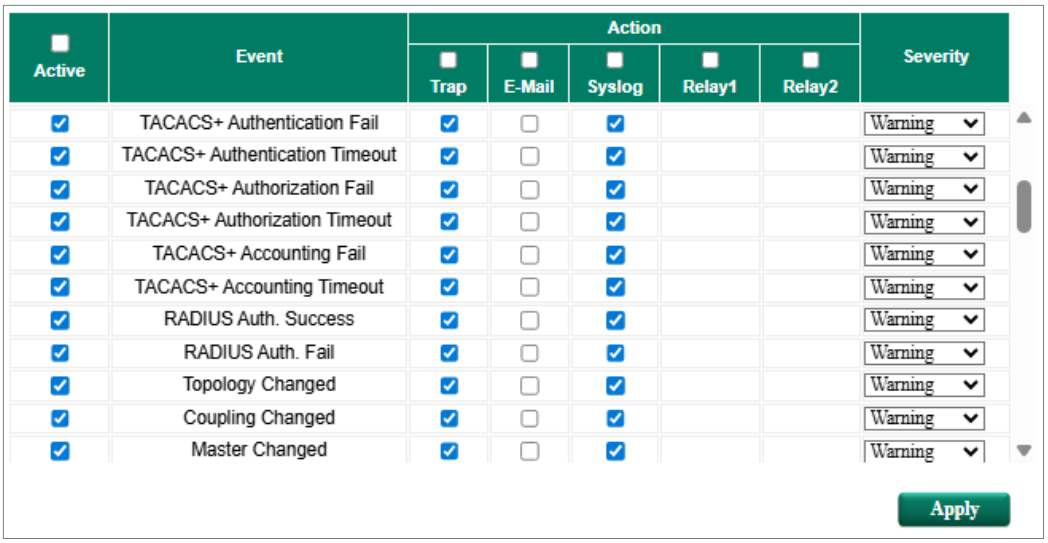
Warning Notification

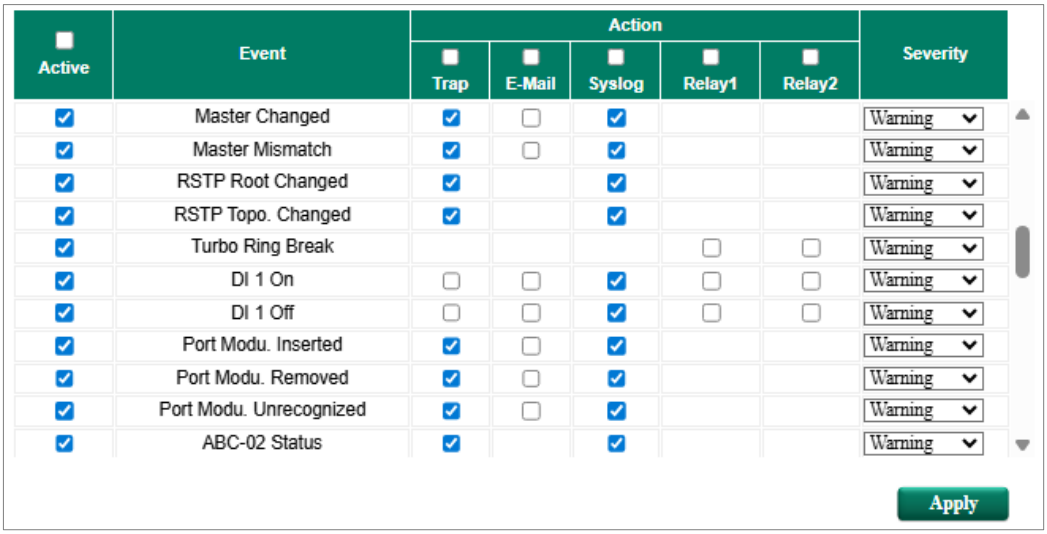
Since industrial Ethernet devices are often located at the endpoints of a system, these devices will not always know what is happening elsewhere on the network. This means that an industrial Ethernet switch that connects to these devices must provide system maintainers with real-time alarm messages. Even when control engineers are out of the control room for an extended period of time, they can still be informed of the status of devices almost instantaneously when exceptions occur. The Moxa switch supports different approaches to warn engineers automatically, such as email, trap, syslog and relay output. It also supports two digital inputs to integrate sensors into your system to automate alarms by email and relay output.

System Event Settings

System Events are related to the overall function of the switch. Each event can be activated independently with different warning approaches. The Administrator can decide the severity of each system event.

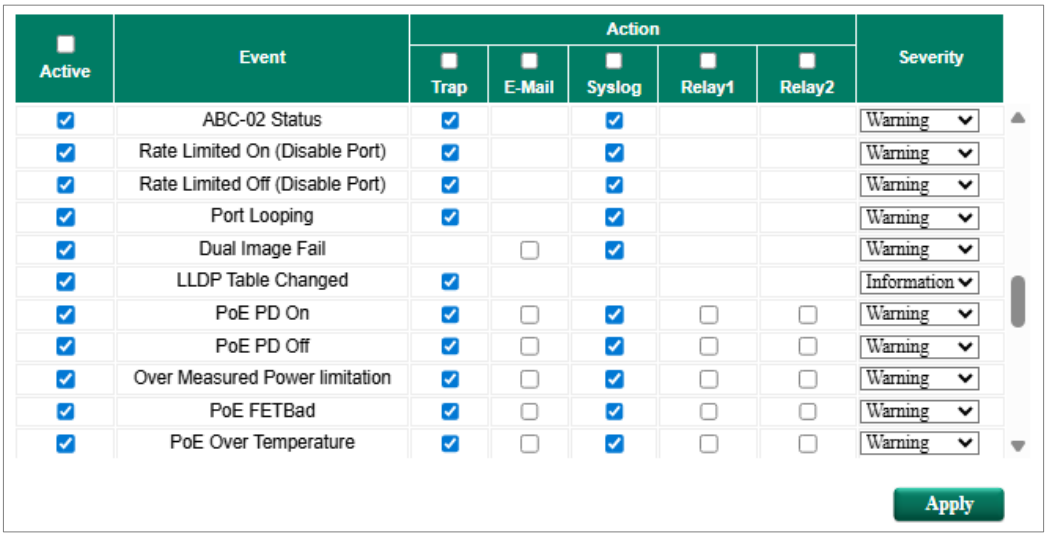






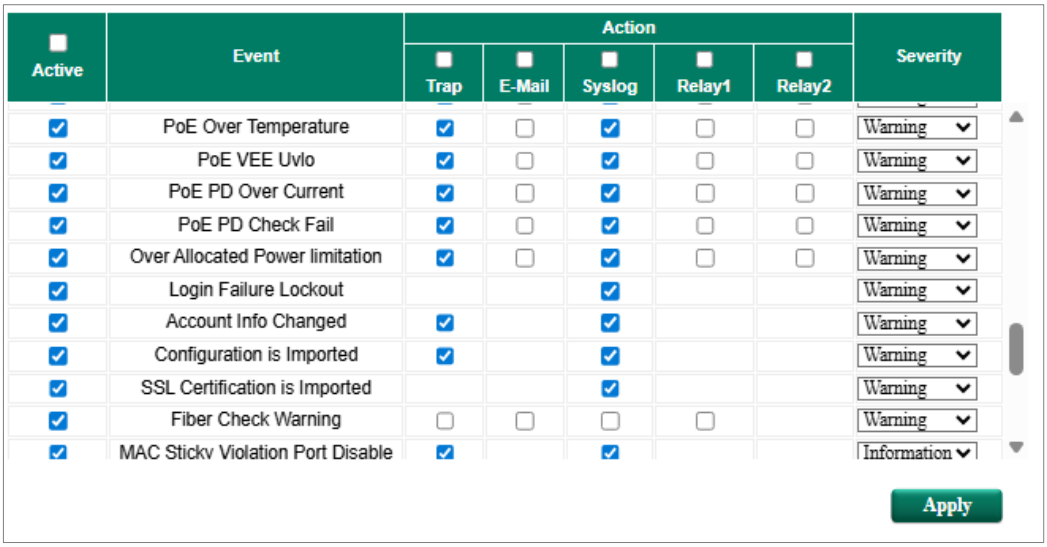
Active	Event	Action					Severity
		Trap	E-Mail	Syslog	Relay1	Relay2	
☑	Master Changed	☑	☐	☑			Warning
☑	Master Mismatch	☑	☐	☑			Warning
☑	RSTP Root Changed	☑		☑			Warning
☑	RSTP Topo. Changed	☑		☑			Warning
☑	Turbo Ring Break				☐	☐	Warning
☑	DI 1 On	☐	☐	☑	☐	☐	Warning
☑	DI 1 Off	☐	☐	☑	☐	☐	Warning
☑	Port Modu. Inserted	☑	☐	☑			Warning
☑	Port Modu. Removed	☑	☐	☑			Warning
☑	Port Modu. Unrecognized	☑	☐	☑			Warning
☑	ABC-02 Status	☑		☑			Warning

Apply



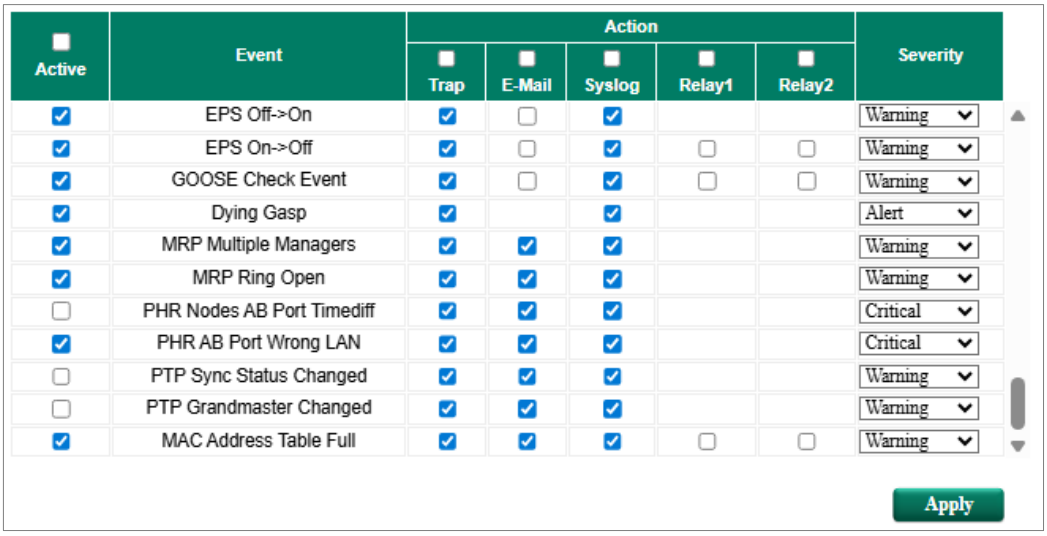
Active	Event	Action					Severity
		Trap	E-Mail	Syslog	Relay1	Relay2	
☑	ABC-02 Status	☑		☑			Warning
☑	Rate Limited On (Disable Port)	☑		☑			Warning
☑	Rate Limited Off (Disable Port)	☑		☑			Warning
☑	Port Looping	☑		☑			Warning
☑	Dual Image Fail		☐	☑			Warning
☑	LLDP Table Changed	☑					Information
☑	PoE PD On	☑	☐	☑	☐	☐	Warning
☑	PoE PD Off	☑	☐	☑	☐	☐	Warning
☑	Over Measured Power limitation	☑	☐	☑	☐	☐	Warning
☑	PoE FETBad	☑	☐	☑	☐	☐	Warning
☑	PoE Over Temperature	☑	☐	☑	☐	☐	Warning

Apply



Active	Event	Action					Severity
		Trap	E-Mail	Syslog	Relay1	Relay2	
☑	PoE Over Temperature	☑	☐	☑	☐	☐	Warning
☑	PoE VEE Uvlo	☑	☐	☑	☐	☐	Warning
☑	PoE PD Over Current	☑	☐	☑	☐	☐	Warning
☑	PoE PD Check Fail	☑	☐	☑	☐	☐	Warning
☑	Over Allocated Power limitation	☑	☐	☑	☐	☐	Warning
☑	Login Failure Lockout			☑			Warning
☑	Account Info Changed	☑		☑			Warning
☑	Configuration is Imported	☑		☑			Warning
☑	SSL Certification is Imported			☑			Warning
☑	Fiber Check Warning	☐	☐	☐	☐		Warning
☑	MAC Sticky Violation Port Disable	☑		☑			Information

Apply



System Events	Description
Cold Start	Power is cut off and then reconnected.
Warm Start	The Moxa switch is rebooted, such as when network parameters are changed (IP address, subnet mask, etc.).
Config. Changed	Any configuration item has been changed.
Power Transition (Off→On) • PWR 1 Off→On • PWR 2 Off→On	The Moxa switch is powered up.
Power Transition (On→Off) • PWR 1 On→Off • PWR 2 On→Off	The Moxa switch is powered down.
Login Success	The account logins to the switch
Login Fail	An incorrect password was entered.
TACACS+ Auth. Success	The account is authorized by a TACACS+ server
TACACS Auth. Fail	Incorrect authentication details were entered
TACACS+ Authentication Timeout	The switch couldn't reach the TACACS+ server to check a username/password before time ran out, so login couldn't complete.
TACACS+ Authorization Fail	The TACACS+ server replied that the logged-in user isn't allowed to perform the requested action, so access was blocked.
TACACS+ Authorization Timeout	The switch couldn't reach the TACACS+ server to confirm permissions before time ran out, so the action was blocked.
TACACS+ Accounting Fail	The switch tried to send activity records (who did what/when) to the TACACS+ server, and the server rejected it or couldn't record it.
TACACS+ Accounting Timeout	The switch tried to send activity records to the TACACS+ server but couldn't reach it before timing out.
TACACS+ Authentication Timeout	The switch couldn't reach the TACACS+ server to check a username/password before time ran out, so login couldn't complete.
RADIUS Auth. Success	The account is authorized by a RADIUS server
RADIUS Authentication Fail	Incorrect authentication details were entered
Password Change	User changes the account password
Topology Changed	• If the Master of the Turbo Ring has changed or the backup path is activated • If the Turbo Ring path is disconnected • If the MSTP topology has changed
Coupling Changed	Backup path is activated
Master Changed	Master of the Turbo Ring has changed
Master Mismatch	When the duplicate master (two or more) or non-master is set up, if any Turbo Ring path/switch fails, the duplicate master switches will automatically renegotiate to determine a new master.
RSTP Root Changed	If the RSTP root has changed
RSTP Topo. Changed	If any Rapid Spanning Tree Protocol switches have changed their position (applies only to the root of the tree)
Turbo Ring Break	Turbo Ring path is disconnected

System Events	Description
ABC-02 Status	Detects if the ABC-02-USB-T is connected or disconnected to the switch when the ABC-02-USB-T automatically imports/exports/backs-up the configuration
Rate Limited On (Disable Port)	When the port is disabled due to the ingress throughput exceeding the configured rate limit.
Rate Limited Off (Disable Port)	The port disable function is off because it exceeds the traffic duration, or the user changes "Port Disable" mode to "Drop Packet" mode.
Port Looping	Port looping event is triggered
LLDP Table Changed	Nearly connected devices are changed and shown in the LLDP table
PoE PD On	Power over Ethernet was turned on for a device connected to a port (the switch started supplying power).
PoE PD Off	Power over Ethernet was turned off for a device connected to a port (the switch stopped supplying power).
Over Measured Power limitation	Total PoE draw is above the configured system power threshold; the switch may deny new power requests or shed loads to stay within budget.
PoE FETBad	The PoE power control component on a port failed, so that port can't reliably supply PoE power.
PoE Over Temperature	The PoE power chip is too hot; the switch may reduce or cut PoE power on affected ports to protect the hardware.
PoE VEE Uvlo	The PoE input voltage dropped below the safe limit, so PoE power may be reduced or cut until voltage recovers.
PoE PD Over Current	A connected device is drawing too much PoE power (overload/short); the switch will cut or limit power on that port.
PoE PD Check Fail	The switch couldn't complete the safety/handshake check with the device, so PoE power wasn't applied or was removed.
Over Allocated Power limitation	The system's PoE power budget is over-committed; a port's power request was denied to keep within the total budget.
Login Failure Lockout	The attempt to log in exceeds the threshold
Account Info Changed	The account information has been changed
Configuration is Imported	When the configuration is successfully imported
SSL Certification is Imported	When SSL Certification is successfully imported
Fiber Check Warning	If the corresponding value of the fiber port status exceeds the threshold defined by the Fiber Check function
MAC Sticky Violation Port Disable	Any port with MAC sticky function is disabled because of a rule violation
Port module inserted	The module is inserted to the system
Port module removed	The module is removed from the system
Port module unrecognized	The module inserted is not recognized by the system
Dual image fail	One of the images has failed
Tracking Status Changed	The tracking status has changed
Port Enable Tracking Changed	The tracking status has changed and reacts on Port Enable
Static Route Tracking Changed	The tracking status has changed and reacts on Static Route
VRRP Tracking Changed	The tracking status has changed and reacts on VRRP priority
EPS Off→On	The external power supply for PoE is on
EPS On→Off	The external power supply for PoE is off
GOOSE Check Event	The GOOSE check status has changed
Dying Gasp	When the power input of power module is lower the system uptime threshold the dying gasp function will be activated. This event will only activate before the whole system powers off.
MRP Multiple Managers	The MRP ring has several MRM roles
MRP Ring Open	The MRP ring path is disconnected
PHR Nodes AB Port Timediff	The difference of time the packets were received from LAN A and LAN B is greater than 1 second
PHR AB Port Wrong LAN	Two redundant ports that should be on separate LAN segments are cabled into the wrong network
PTP Grandmaster Changed	Grandmaster clock has changed
PTP Synchronization Status Changed	The PTP synchronization status has changed
MAC Address Table Full	MAC Address reached max. 16,384 entries

Four response actions are available when events are triggered.

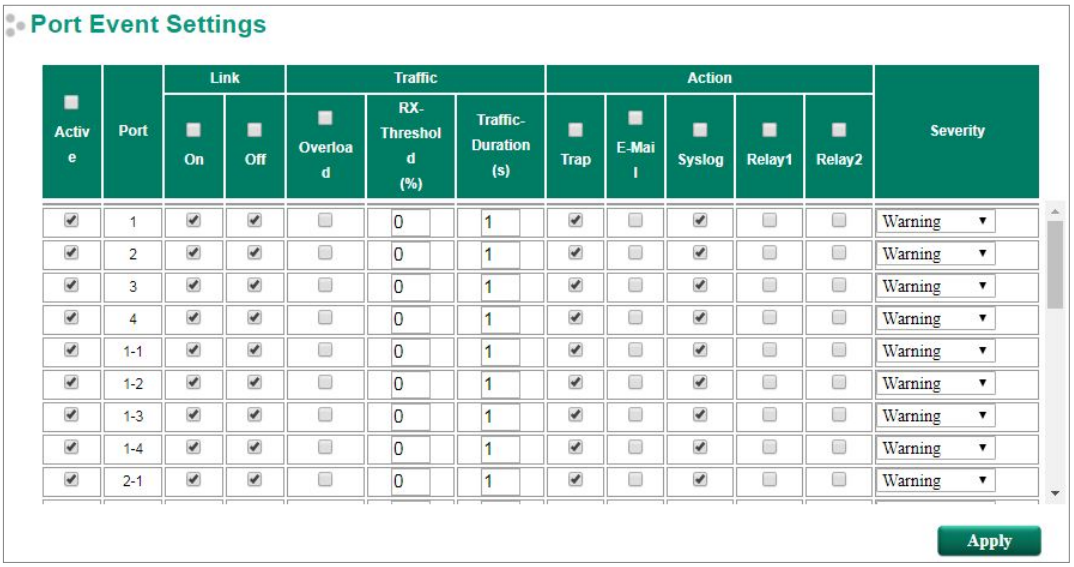
Action	Description
Trap	A notification will be sent to the trap server when an event is triggered.
E-Mail	A notification will be sent to the email server defined in the Email Setting.
Syslog	A notification will be sent to the syslog server defined in Syslog Server Setting.
Relay	Supports digital inputs to integrate sensors. When an event is triggered, the device will automate alarms through the relay output.

Severity

Severity	Description
Emergency	System is unusable
Alert	Action must be taken immediately
Critical	Critical conditions
Error	Error conditions
Warning	Warning conditions
Notice	Normal but significant condition
Information	Informational messages
Debug	Debug-level messages

Port Event Settings

Port Events are related to the activity of a specific port.



Port Events	Warning e-mail is sent when...
Link-ON	The port is connected to another device.
Link-OFF	The port is disconnected (e.g., the cable is pulled out, or the opposing device shuts down).
Traffic-Overload	The port's traffic surpasses the Traffic-Threshold for that port (provided this item is Enabled).
Traffic-Threshold (%)	Enter a nonzero number if the port's Traffic-Overload item is Enabled.
Traffic-Duration (sec.)	A Traffic-Overload warning is sent every Traffic-Duration second if the average Traffic-Threshold is surpassed during that time period.

Four response actions are available on the EDS E series when events are triggered.

Action	Description
Trap	A notification will be sent to the trap server when an event is triggered.
E-Mail	A notification will be sent to the email server defined in the Email Setting.
Syslog	A notification will be sent to the syslog server defined in Syslog Server Setting.
Relay	Supports digital inputs to integrate sensors. When an event is triggered, the device will automate alarms through the relay output.

Severity

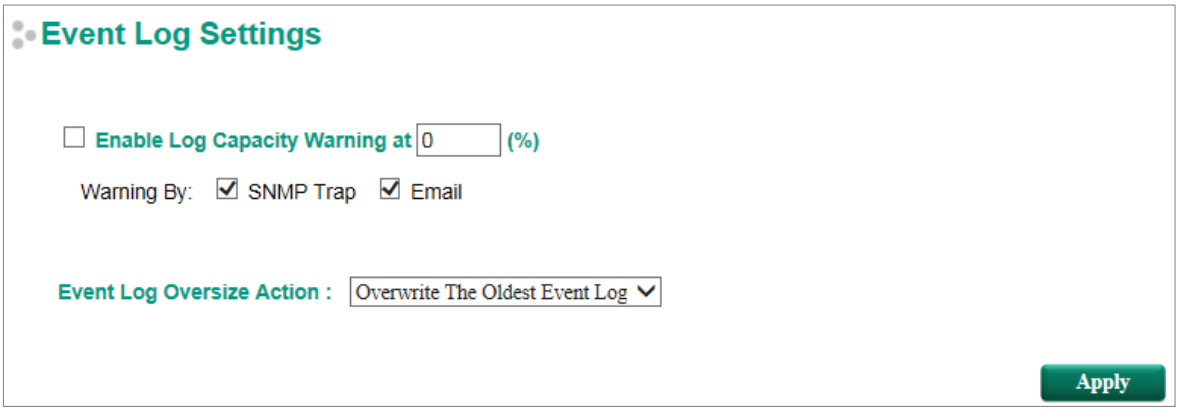
Severity	Description
Emergency	System is unusable
Alert	Action must be taken immediately
Critical	Critical conditions
Error	Error conditions
Warning	Warning conditions
Notice	Normal but significant condition
Information	Informational messages
Debug	Debug-level messages

NOTE

The Traffic-Overload, Traffic-Threshold (%), and Traffic-Duration (sec.) Port Event items are related. If you Enable the Traffic-Overload event, then be sure to enter a nonzero Traffic-Threshold percentage, as well as a Traffic-Duration between 1 and 300 seconds.

Event Log Settings

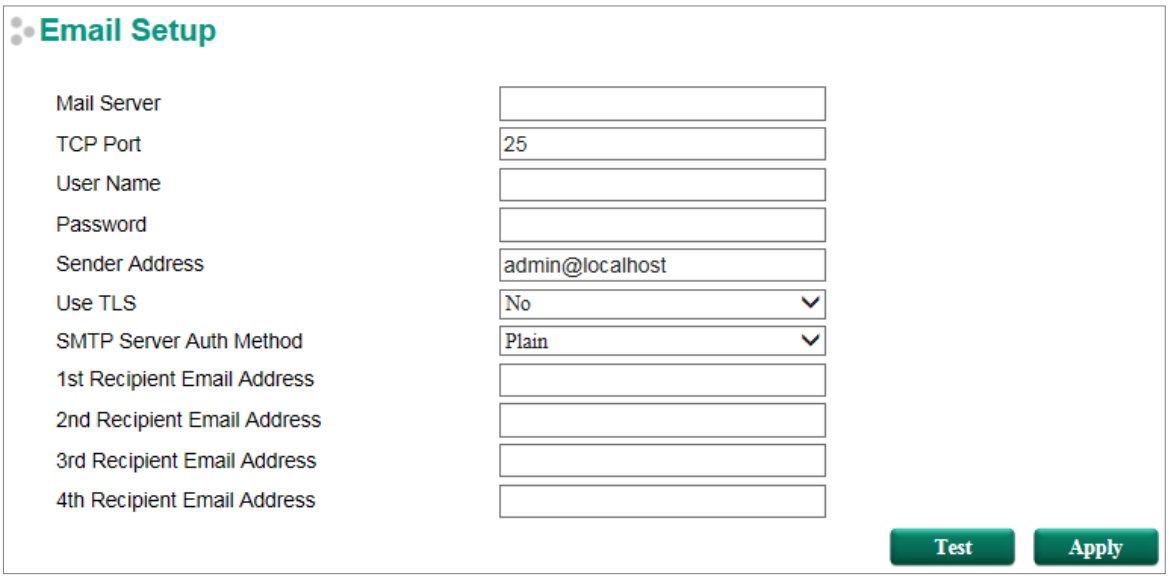
This function is used to inform the user what the event log capacity status is and decide what action to take when an event log is oversized. Select the **Enable Log Capacity Warning** checkbox to set the threshold percentage. When the event log capacity is over the percentage, the switch will send a warning message by SNMP Trap or Email.



Event Log Oversize Action

Setting	Description	Factory Default
Overwrite The Oldest Event Log	The oldest event log will be overwritten when the event log exceeds 1000 records.	Overwrite The Oldest Event Log
Stop Recording Event Log	Additional events will not be recorded when the event log exceeds 1000 records.	

Email Settings



Mail Server

Setting	Description	Factory Default
IP address or URL	The IP Address or URL of the email server.	None

TCP Port

Setting	Description	Factory Default
TCP Port number	The TCP port number of your email server.	25

User Name

Setting	Description	Factory Default
Max. of 45 characters	Your email account name	None

Password Setting

Setting	Description	Factory Default
Password	The email account password.	None

Email Address

Setting	Description	Factory Default
Max. of 30 characters	You can set up to 4 email addresses to receive alarm emails from the Moxa switch.	None

Sender Address

Setting	Description	Factory Default
Max. 30 characters	Sender Email Address	admin@localhost

User TLS

Setting	Description	Factory Default
Yes/No	Enables TLS(Transport Layer Security)	No

SMTP Server Auth Method

Setting	Description	Factory Default
Plain/Login/ CRAM-MD5	choose an authentication mechanism, PLAIN, LOGIN, and CRAM-MD5, to login SMTP Server	Plain

Sending a Test Email

After you complete the email settings, you should first click **Apply** to activate those settings, and then press **the** Test button to verify that the settings are correct.

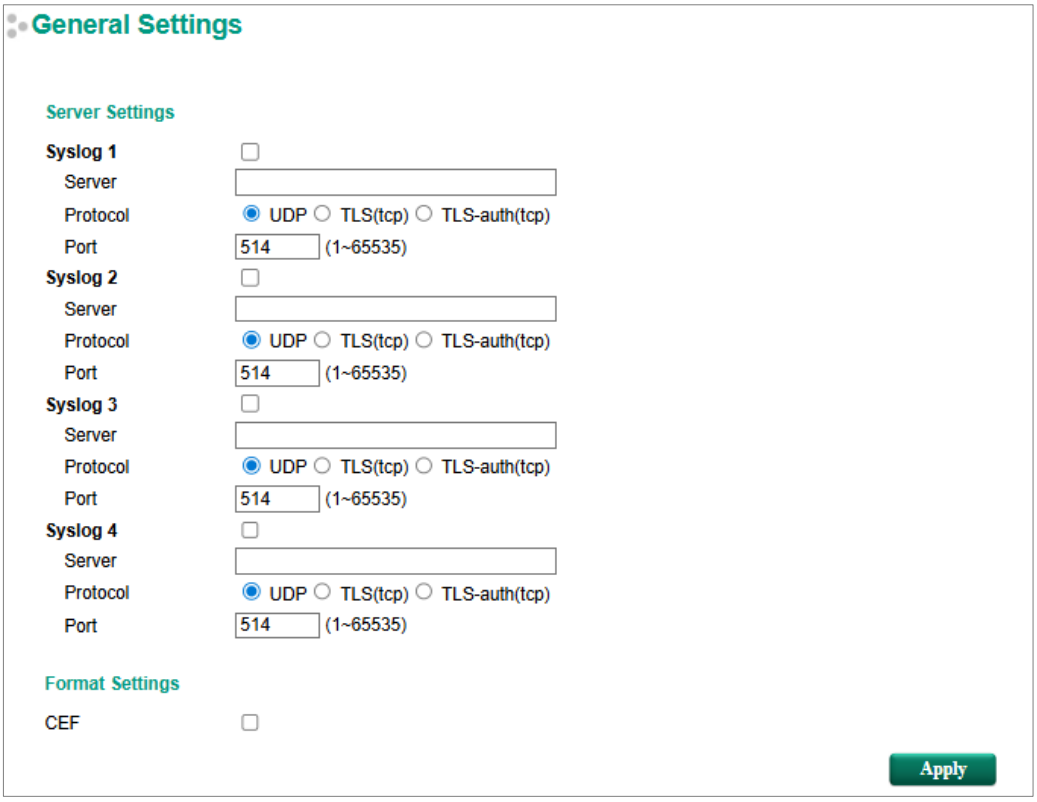
NOTE

Auto warning e-mail messages will be sent through an authentication protected SMTP server that supports the CRAM-MD5, LOGIN, and PAIN methods of SASL (Simple Authentication and Security Layer) authentication mechanism.

We strongly recommend not entering your Account Name and Account Password if auto warning e-mail messages can be delivered without using an authentication mechanism.

Syslog Server Settings

The Syslog function provides the event logs for the syslog server. The function supports 4 configurable syslog servers and syslog server UDP port numbers. When an event occurs, the event will be sent as a syslog UDP packet to the specified syslog servers. Each Syslog server can be activated separately by checking the appropriate checkbox to enable it.



Syslog Server 1/2/3/4

Setting	Description	Factory Default
IP Address	Enter the IP address of Syslog server 1/2/3, used by your network.	None
Port Destination (1 to 65535)	Enter the UDP port of Syslog server 1/2/3.	514

NOTE

The following events will be recorded into the Moxa switch's Event Log table, and will then be sent to the specified Syslog Server:

- Cold start
- Warm start
- Configuration change activated
- Power 1 or 2 transition: Off to On or On to Off
- Authentication fail
- Password change
- Redundancy protocol/topology change
- Master setting mismatch
- ABC-02 status
- Web log in
- Rate Limit on/off(Disable port)
- Port looping
- Port traffic overload
- dot1x Auth Fail
- Port link off/on
- The Grandmaster Clock has changed
- The PTP synchronization status has changed
- The external power supply for PoE transition: Off to On or On to Off

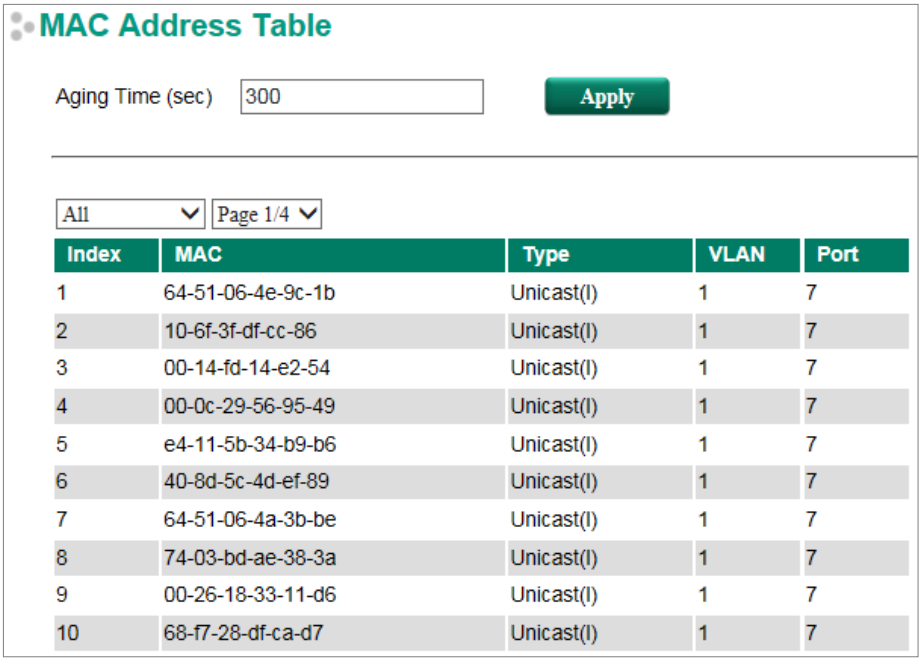
Relay Warning Status

When a relay warning is triggered by either the system or port events, the administrator can turn off the hardware warning buzzer by clicking the **Apply** button. The event will still be recorded in the event list.

MAC Address Table

The MAC address table shows the MAC address list passed through the Moxa switch. The Aging Time (15 to 3825 seconds) defines the length of time that a MAC address entry can remain in the Moxa switch. When an entry reaches its aging time, it "ages out" and is purged from the switch, effectively cancelling frame forwarding to that specific port.

The MAC Address table can be configured to display the following Moxa switch MAC address groups, which are selected from the drop-down list.



Drop Down List

ALL	Select this item to show all of the Moxa switch's MAC addresses.
ALL Learned	Select this item to show all of the Moxa switch's Learned MAC addresses.
ALL Static	Select this item to show all of the Moxa switch's Static, Static Lock, and Static Multicast MAC addresses.
ALL Multicast	Select this item to show all of the Moxa switch's Static Multicast MAC addresses.
Port x	Select this item to show all of the MAC address's dedicated ports.

The table displays the following information:

MAC	This field shows the MAC address.
Type	This field shows the type of this MAC address.
Port	This field shows the port that this MAC address belongs to.

System Files

Firmware Upgrade

There are four ways to update your Moxa switch's firmware: from a local *.rom file, by remote TFTP server, SCP, and with Auto Backup Configurator (ABC-02).

Local

1. Download the updated firmware (*.rom) file from Moxa's website (www.moxa.com).
2. Browse for the (*.rom) file, and then click the **Upgrade** button.

TFTP Server

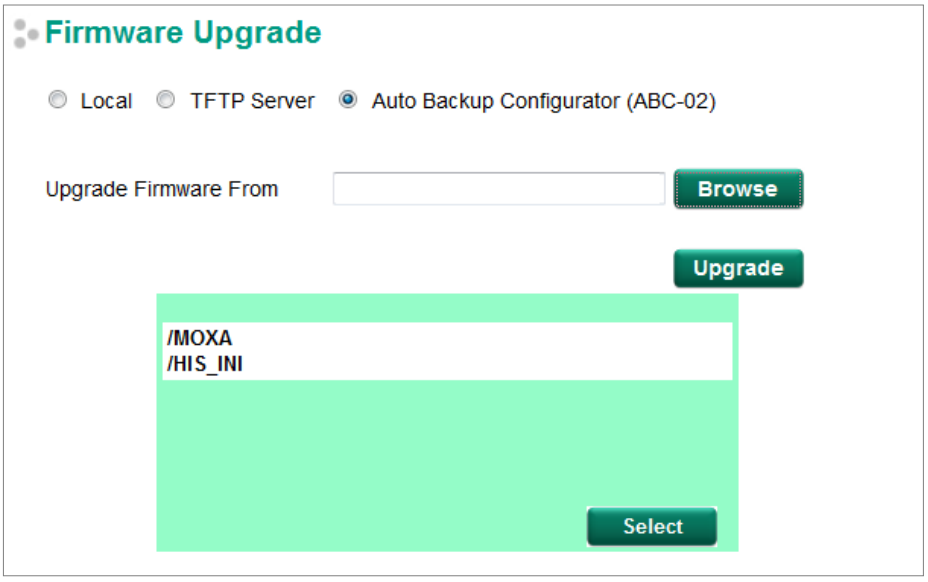
1. Enter the TFTP Server's IP address.
2. Input the firmware file name (*.rom) and click the **Upgrade** button.

SCP

1. Enter SCP IP address, Filename, Account and Password.
2. Click the **Upgrade** button.

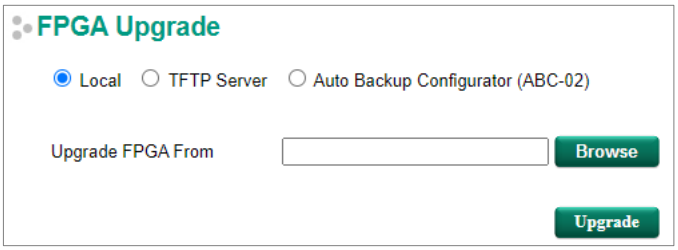
ackup Configurator (ABC-02)

1. Download the updated firmware (*.rom) file from Moxa's website (www.moxa.com).
2. Save the file to the ABC-02's **Moxa** folder. The file name cannot be longer than 8 characters, and the file extension must be **.rom**.
3. Browse for the firmware (*.rom) file from the ABC-02, and then click the **Upgrade** button.



FPGA Upgrade

There are three ways to update your Moxa switch's FPGA firmware from a local *.rom file; by remote TFTP server and with the Auto Backup Configurator (ABC-02).



Local

1. Download the updated FPGA firmware (*.rom) file from Moxa's website (www.moxa.com).
2. Browse for the (*.rom) file, and then click the **Upgrade** button.

TFTP Server

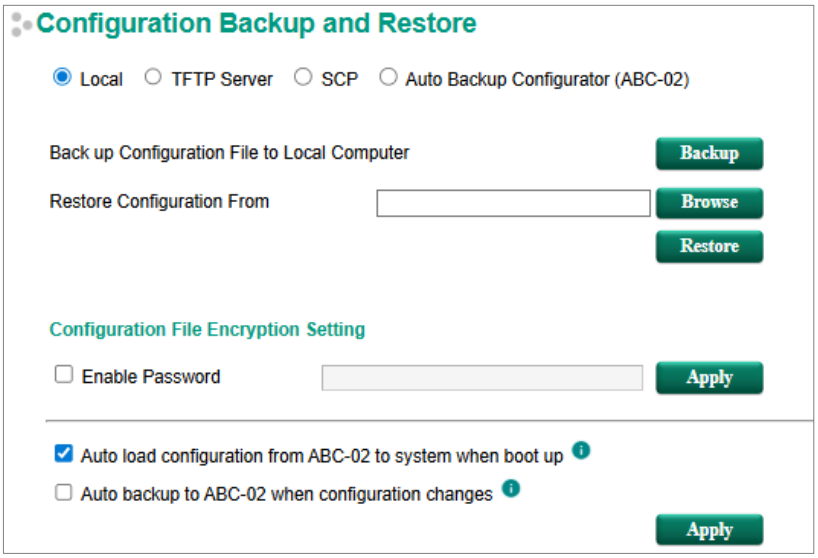
1. Enter the TFTP Server's IP address.
2. Input the FPGA firmware file name (*.rom) and click the **Upgrade** button.

Backup Configurator (ABC-02)

1. Download the updated FPGA firmware (*.rom) file from Moxa's website (www.moxa.com).
2. Save the file to the ABC-02's **Moxa** folder. The file name cannot be longer than 8 characters, and the file extension must be **.rom**.
3. Browse for the FPGA firmware (*.rom) file from the ABC-02, and then click the **Upgrade** button.

Configuration Backup and Restore

There are four ways to back up and restore your Moxa switch's configuration: from a local configuration file, by remote TFTP server, SCP and with Auto Backup Configurator (ABC-02).



Local

1. Click the **Backup** button to back up the configuration file to a local drive.
2. Browse for a configuration on a local disk, and then click the **Restore** button.

TFTP Server

1. Enter the TFTP Server's IP address.
2. Input the backup/restore file name (supports up to 54 characters, including the .ini file extension) and then click the **Backup/Restore** button.

SCP

1. Enter SCP IP address, Filename, Account and Password.
2. Click the **Upgrade** button.

Backup Configurator (ABC-02)

1. Click **Backup** to save the configuration file to the ABC-02. The file will be saved in the ABC-02's **Moxa** folder as a *.ini file (e.g., Sys.ini).

   Note that two files will be saved to the ABC-02-USB's **Moxa** folder: **Sys.ini** and **MAC.ini**. The purpose of saving the two files is to identify which file will be used when **Auto load configuration from ABC to system when boot up** is activated.

> **NOTE**
>
> MAC.ini is named using the last 6 digits of the switch's MAC address, without spaces.

2. Click **Browse** to select the configuration file, and then click **Restore** to start loading the configuration into your switch.
3. **Configuration File Encryption Setting**

   Select the **Configuration File Encryption Setting** checkbox, input the password, and then click **Apply**.
4. **Auto load configuration from ABC to system when boot up**

   Select the **Auto load configuration from ABC to system when boot up** checkbox and then click **Apply**. Note that this function is enabled by default.

   Power off your switch first, and then plug in the ABC-02. When you power on your switch, the system will detect the configuration file on the ABC-02 automatically. The switch will recognize the file name, with the following sequence priority:

   First priority: MAC.ini
   Second priority: Sys.ini

   If no matching configuration file is found, the fault LED light will turn on, and the switch will boot up normally.

> **NOTE**
>
> MAC.ini is named using the last 6 digits of the switch's MAC address, without spaces.

5. **Auto backup to ABC-02 when configuration changes**

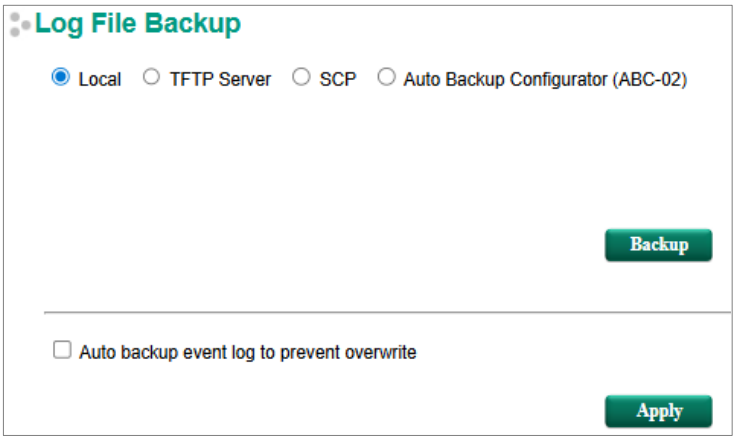
   Select the **Auto backup to ABC-02 when configuration change** checkbox and then click **Apply**. This function is disabled by default.

   The ABC-02 is capable of backing up switch configuration files automatically. While the ABC-02 is plugged into the switch, enable the **Auto backup to ABC-02 when configuration change** option, and then click **Apply**. Once this configuration is modified, the switch will back up the current configuration to the **/His_ini** folder on the ABC-02. The file name will be the system date/time (MMDDHHmm.ini).

> **NOTE**
>
> MM=month, DD=day, HH=hour, mm=minutes, from the system time.

Log File Backup

There are four ways to back up Moxa switch's log files: from a local drive, by remote TFTP server, or with Auto Backup Configurator (ABC-02).



Local

Click the **Backup** button to back up the log file to a local drive.

TFTP Server

Enter the TFTP Server's IP address and file name and then click the **Backup** button.

SCP

Enter SCP IP address, file name, account and password and click **Backup** button.

Backup Configurator (ABC-02)

Click **Backup** to save the configuration file to the ABC-02. The file will be saved in the ABC-02's **Moxa** folder with filename **Sys.ini**.

Auto backup of event log to prevent overwrite

This function is designed to maintain a long-term record of the switch's log files. Moxa Ethernet switches are capable of saving 1000 event log entries. When the 1000-entry storage limit is reached, the switch will delete the oldest saved event log. The ABC-02 can be used to back up these event logs. When the number of switch log entries reaches 1000, the ABC-02 will save the oldest 100 entries from the switch.

Enable the **Auto backup of event log to prevent overwrite**, and then click **Apply**. After that, when the ABC-02 is plugged into the switch, the event logs will always be saved to the ABC-02 automatically when the number of switch log entries reaches 1000. Each backup action saves the oldest 100 logs to the ABC-02 in one file, with the filename generated by the current system time as **MMDDHHmm.ini**. The file is saved to the **His_log** folder.

NOTE

MM=month, DD=day, HH=hour, mm=minutes, from the system time.

The log file includes the following information:

Index	An event index assigned to identify the event sequence.
Bootup Number	This field shows how many times the Moxa switch has been rebooted or cold started.
Date	The date is updated based on how the current date is set on the System Settings page.
Time	The time is updated based on how the current time is set on the System Settings page.
System Startup Time	The system startup time related to this event.
Event	Events that have occurred.

Switch Reset Button

The Moxa switch reset button can be used to perform two functions: quickly reset the switch's configuration and save the current configuration and log files to the ABC-02. For instructions on using the ABC-02 device refer to *QIG for ABC-02 Series on the Moxa website.*

NOTE

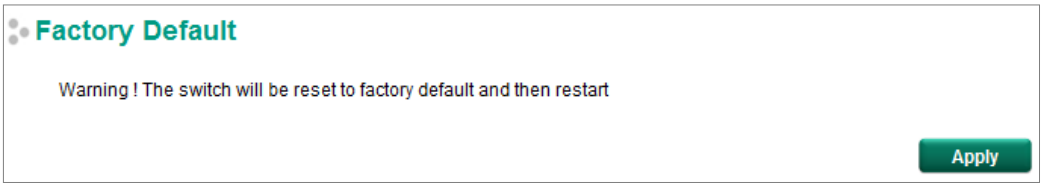
DO NOT remove the ABC-02 when performing an upgrade, backup, or restore.

Restart

The **Restart** function provides users with a quick way to restart the switch's operating system.

Factory Default

The **Factory Default** function provides users with a quick way of restoring the Moxa switch's configuration to factory defaults. The function can be activated from the USB serial interface, via Telnet, through the web-based console, or with the hardware reset button.



NOTE

After restoring the factory default configuration, you will need to use the default network settings to re-establish the web or Telnet console connection with the Moxa switch.

PoE (PoE models only)

NOTE

The PT-G7728 Series and PT-G7828 Series do not support LM-7000H-4GPoE/LM-7000H-4PoE HW Rev. 3.0.0. When LM-7000H-4GpoE/LM-7000H-4PoE HW Rev. 3.0.0 is inserted, the Module State LED will turn Red and EPS LED will turn off.

Power over Ethernet has become increasingly popular, due in large part to the reliability provided by PoE Ethernet switches that supply the power to Powered Devices (PD) when AC power is not available or is too expensive to provide locally.

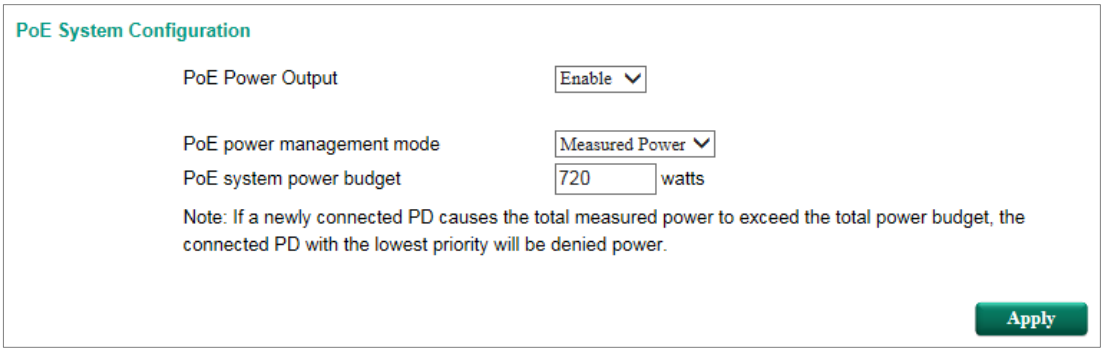
Power over Ethernet can be used with the following types of devices:

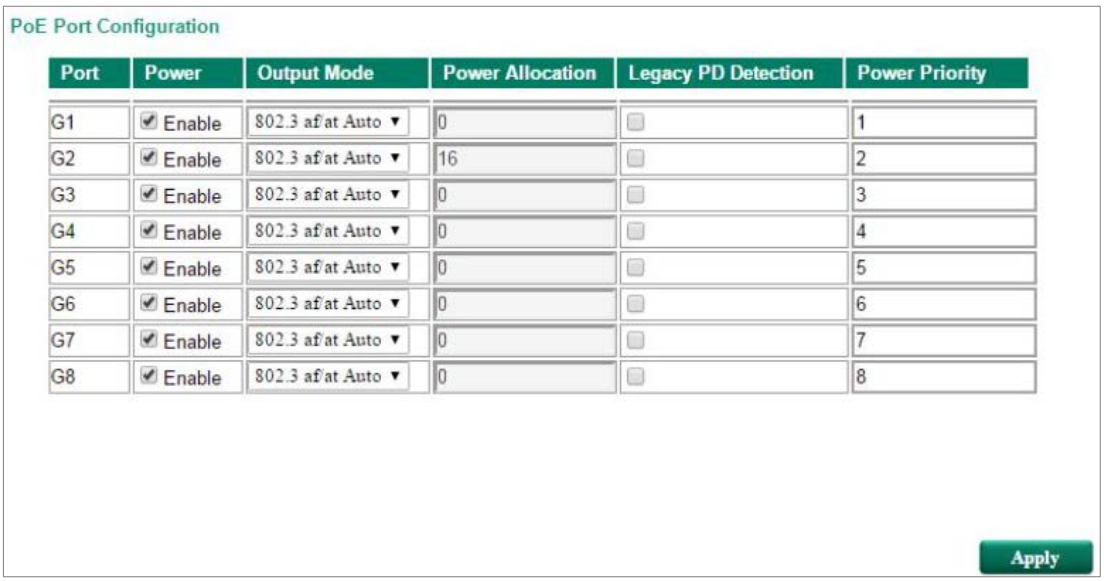
- Surveillance cameras
- Security I/O sensors
- Industrial wireless access points
- Emergency IP phones

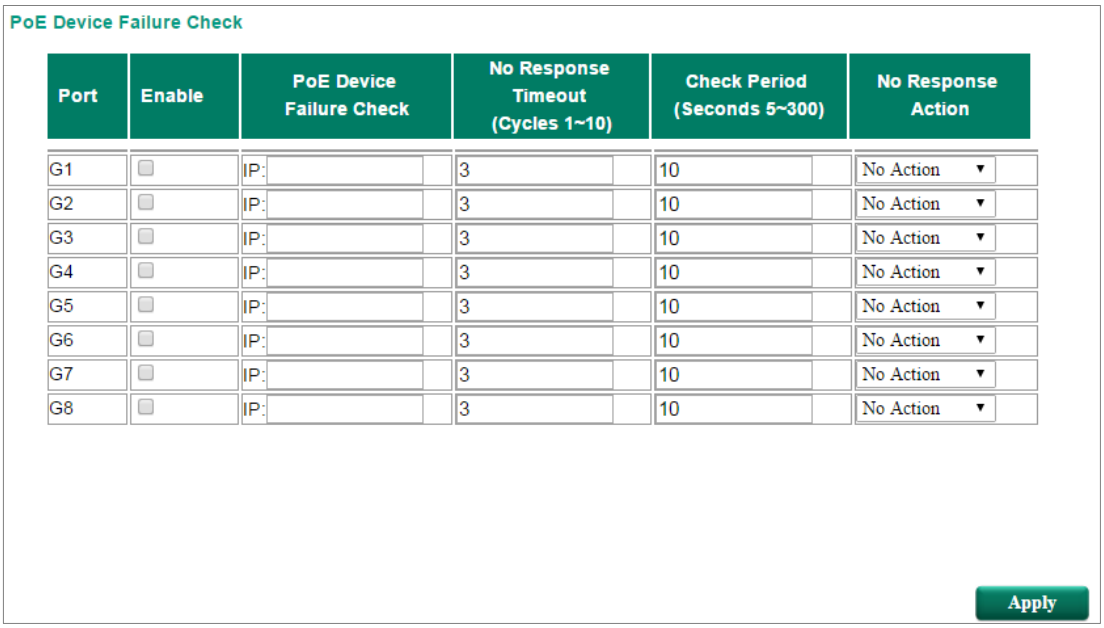
In fact, it's not uncommon for video, voice, and high-rate industrial application data transfers to be integrated onto one network. Moxa's PoE switches are equipped with many advanced PoE management functions, providing vital security systems with a convenient and reliable Ethernet network. Moreover, Moxa's advanced PoE switches support the high power PoE+ standard, a 24 VDC direct power input, and 20 ms fast recovery redundancy with Turbo Ring and Turbo Chain.

PoE Settings

The PoE settings interface gives users control over the system's PoE power output, PoE power threshold, PoE port configuration, and PD failure check. The PoE settings page is divided into three parts: **PoE System Configuration, PoE Port Configuration,** and **PoE Device Failure Check**. Each part is discussed separately below.





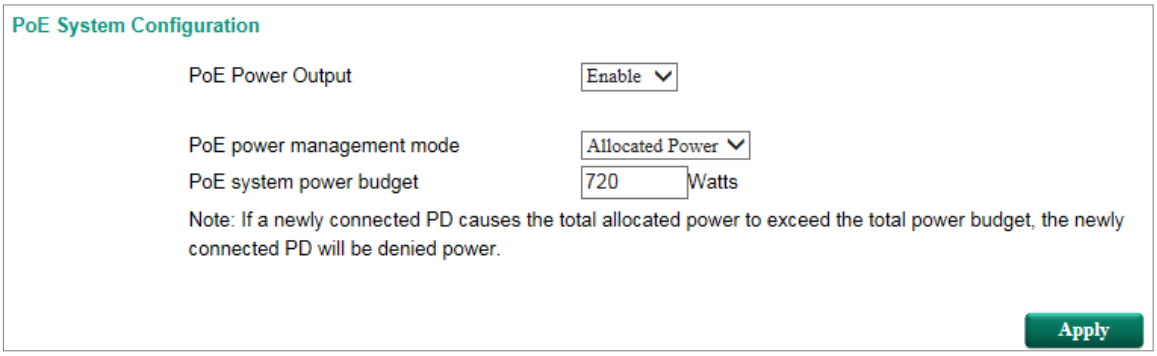


PoE System Configuration

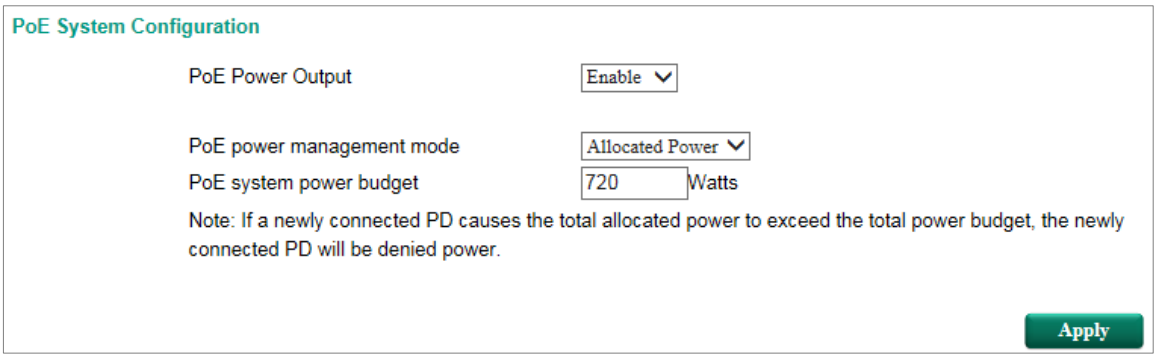
NOTE

The configuration is different, depending on whether the "PoE power output managed by" item is set to "Allocated Power" or "Measured Power."

PoE Power Management by Allocated Power



PoE Power Management by Measured Power



PoE System Configuration Settings

PoE Power Output

Setting	Description	Factory Default
Enable	Enables PoE power transmission to a PD	Enable
Disable	Disables PoE power transmission to a PD	

PoE power management Mode

Setting	Description	Factory Default
Allocated Power	If a powered device is connected that would cause the total amount of power needed by all connected devices to exceed the total allocated power limit, the switch will not power up the device.	Disable
Measured Power	If a powered device is connected that would cause the total amount of power needed by all connected devices to exceed the total measured power limit, the switch with will deny power to the device with the lowest priority.	Enable

Deny next port when exceed

This setting only appears when "PoE power output management mode" is set to "Allocated Power."

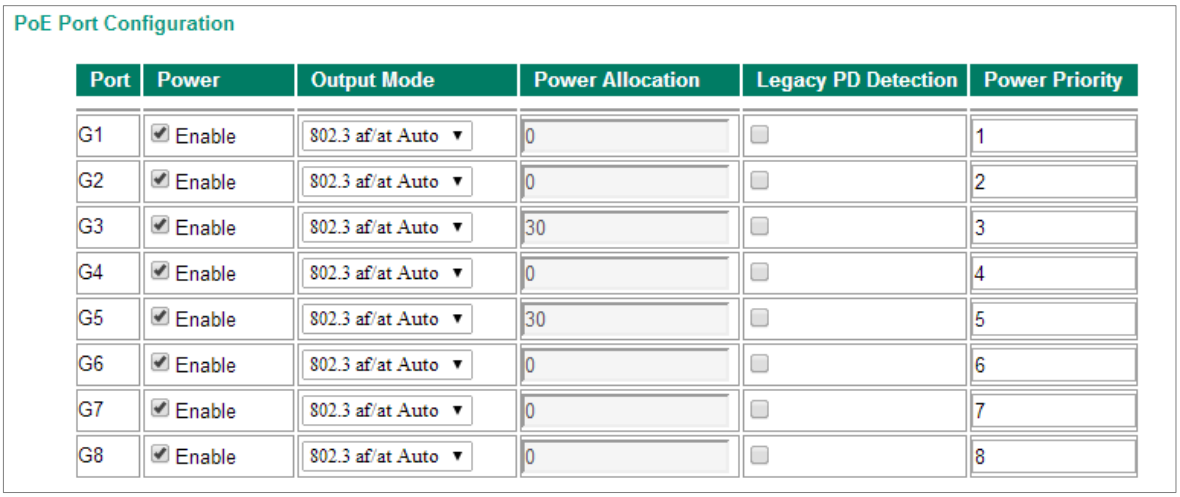
Setting	Description	Factory Default
wattage	Assigns the "Total allocated power" limit for all PoE ports combined.	720 W

Deny low priority port when exceed

This setting only appears when "PoE power output managed by" is set to "Measured Power."

Setting	Description	Factory Default
wattage	Assigns the "Total measured power" limit for all PoE ports combined.	720 W

PoE Port Configuration



Power

Setting	Description	Factory Default
Checked	Allows data and power to be transmitted through the port.	Checked
Unchecked	Immediately shuts off power to that port	

Output Mode

Setting	Description	Factory Default
802.3 af/at Auto	Power transmission follows the IEEE 802.3 af/at protocols. The acceptable PD resistance range is 17 kΩ to 29 kΩ.	802.3 af/at Auto
High Power	Provides a higher power output to the PD. The acceptable PD resistance range is 17 kΩ to 29 kΩ, and the power allocation of the port is automatically set to 36 W.	
Force	Provides power output to non-802.3 af/at PDs. The acceptable PD resistance range is over 2.4 kΩ, and the range of power allocation is 0 to 36 W.	

Power Allocation

Setting	Description	Factory Default
0 to 36	When the Output Mode is set to Force, the Power Allocation can be set from 0 to 36 W.	36

Legacy PD Detection

The PoE Ethernet Switch provides a **Legacy PD Detection** function. When the capacitance of the PD is higher than 2.7 μF, checking the **Legacy PD Detection** checkbox enables the system to output power to the PD. In this case, it will take 10 to 15 seconds for PoE power to be output through this port after the switch is turned on.

Setting	Description	Factory Default
Checked	Enables legacy PD detection	Unchecked
Unchecked	Disables legacy PD detection	

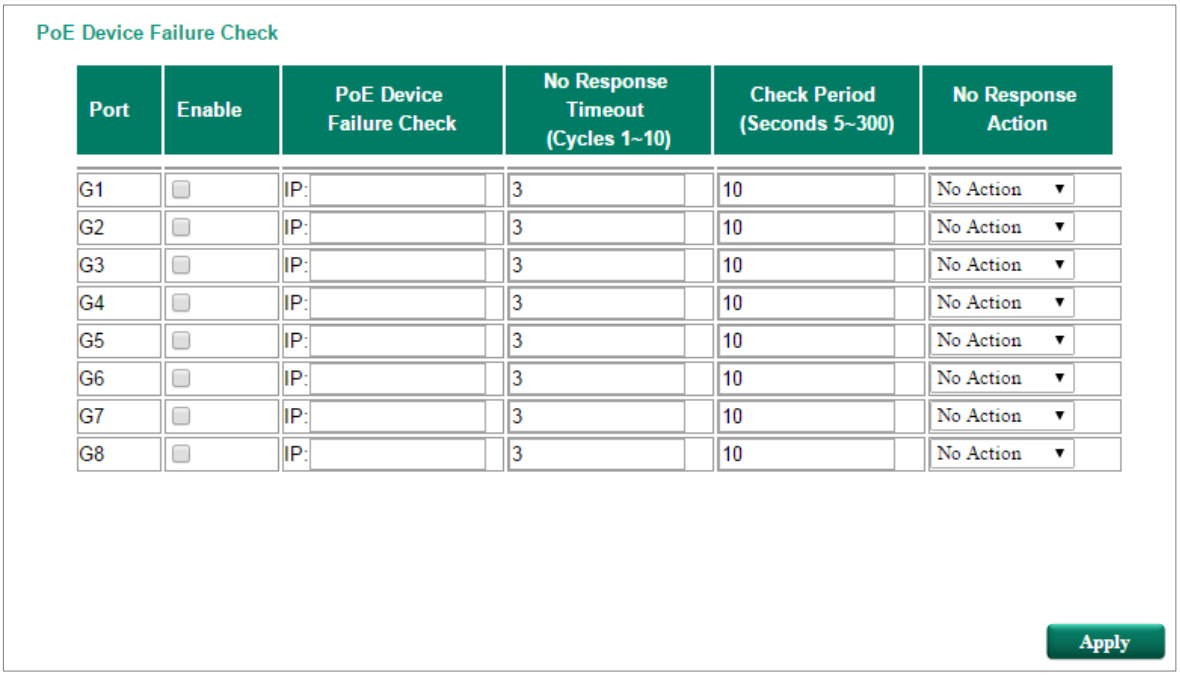
Power Priority

Use **Power Priority** when managing PoE power with measured power mode. The smaller the number, the higher the priority. You may set the same priority for different PoE ports, but if you configure two ports with the same priority, then the port with the lower port number has the higher priority. The setting can range from 1 up to the total number of ports. When the PoE measured power exceeds the assigned limit, the switch will disable the PoE port with the lowest priority.

Setting	Description	Factory Default
1 to "number of PoE ports"	The smaller the number, the higher the PoE port priority. When the PoE measured power exceeds the assigned limit, the switch will disable the PoE port with the lowest priority.	The PoE port index number

PoE Device Failure Check

The PoE Ethernet switch can monitor the status of a PD via its IP address. If the PD fails, the switch will not receive a PD response after the defined period, and the authentication process will be restarted. This function is extremely useful for ensuring your network's reliability and reducing your management burden.



Enable

Setting	Description	Factory Default
Checked	Enables the PD Failure Check function	Unchecked
Unchecked	Disables the PD Failure Check function	

PoE Device IP Address

Setting	Description	Factory Default
Max. 15 Characters	Enter the PD's IP address	None

No Response Timeout

Setting	Description	Factory Default
1 to 10	The maximum number of IP checking cycles.	3

Check Period

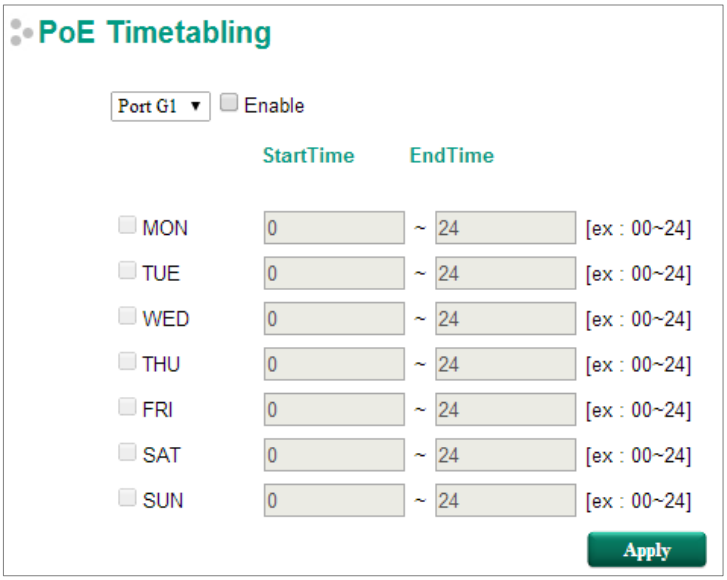
Setting	Description	Factory Default
5 to 300	Enter maximum time allowed for each IP checking cycle.	10

No Response Action

Setting	Description	Factory Default
No Action	The PSE has no action on the PD	No Action
Reboot PD	The PSE reboots the PD after the PD Failure Check	
Power Off PD	The PSE powers off the PD after the PD Failure Check	

PoE Timetabling

Powered devices usually do not need to be running 24 hours a day, 7 days a week. The PoE Ethernet switch provides a PoE timetabling mechanism that lets users economize the system's power burden by setting a flexible working schedule for each PoE port.



Port

Setting	Description	Factory Default
Port	Select which port you would like to configure.	The first port of the first PoE module

Enable

Setting	Description	Factory Default
Checked	Enables the PoE function of the port for the defined time period.	Unchecked
Unchecked	Enables the PoE function of the port all the time.	

MON, TUE, WED, THU, FRI, SAT, SUN

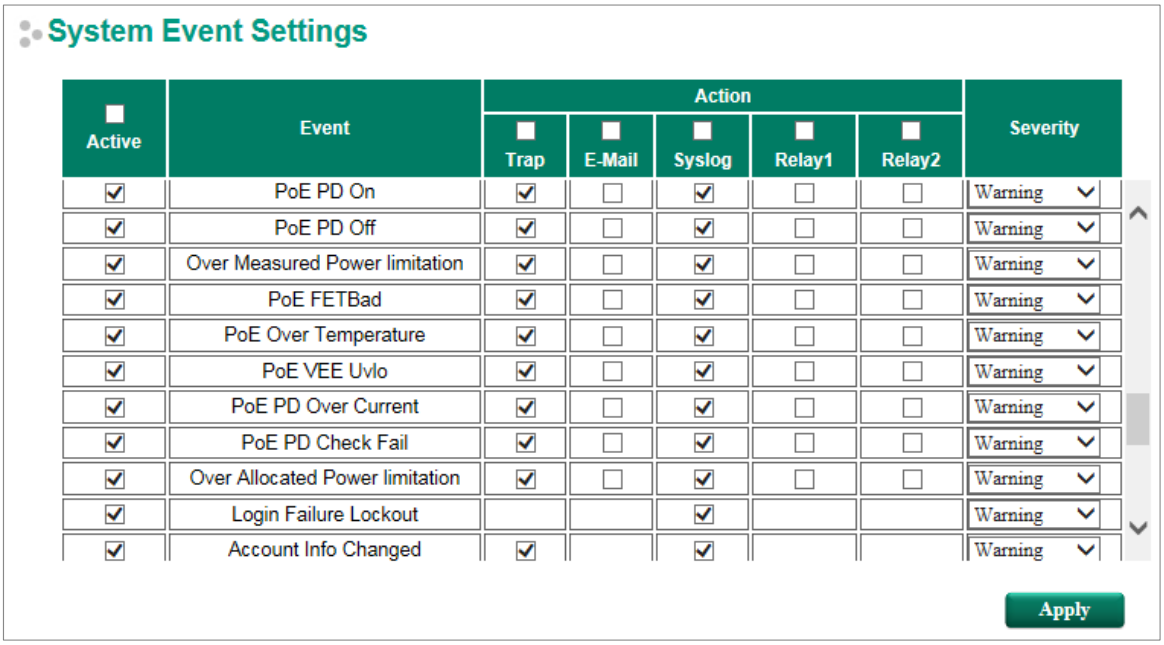
Setting	Description	Factory Default
Checked	Select those days on which you would like the port to be enabled (you will then be able to modify the StartTime and EndTime)	Disable
Unchecked	The port will not provide PoE power on days that are not check marked.	

Start/End Time

Setting	Description	Factory Default
Configured time period	Enter the hour of the day the configuration will be enabled, and the hour of the day the configuration will be disabled.	0 to 24

PoE Warning Event Settings

Since industrial Ethernet devices are often located at the endpoints of a system, these devices do not always know what is happening elsewhere on the network. This means that a PoE port connected to a PD must provide system administrators with real-time alarm messages. Even when control engineers are out of the control room for an extended period of time, they can still be informed of the status of the PD almost instantaneously when exceptions occur. The PoE Ethernet switch supports different methods for warning engineers automatically, including SNMP trap, email, and relay output. It also supports two digital inputs to integrate sensors into your system to automate alarms using email and relay output. The PoE warning event settings are on the **System Event Settings** page.



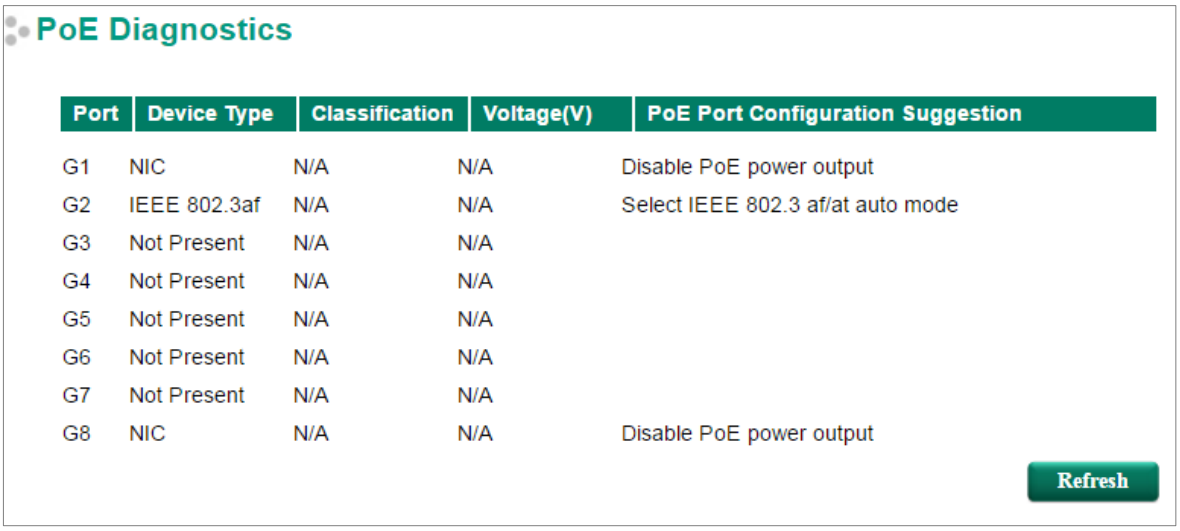
Warning Type

Action	Description
Trap	A notification will be sent to the trap server when an event is triggered.
E-Mail	A notification will be sent to the email server defined in Email Settings.
Syslog	Record a syslog to a syslog server defined in Syslog Server Settings.
Relay1/2	Supports digital inputs to integrate sensors. When an event is triggered, the device will automatically activate an alarm through the relay output.

Event Type

Port Events	Description
PoE PD on	Power is being output to the PD.
PoE PD off	The PoE power output is cut off.
PoE PD Over Current	When the current of the port exceeds the following limits: 802.3 af: 350 mA 802.3 at: 600 mA High Power: 720 mA Force: 600 mA
PoE PD Failure Check	When the switch does not receive a PD response after the defined period.
Over Measured Power Limitation	When the total PD power consumption exceeds the total measured power limit.
PoE FETBad	When the MOSFET of the port is out of order (Contact Moxa for technical service)
PoE over Temperature	Check the temperature of the environment. If you cannot keep the temperature under 75°C, contact Moxa for technical support.
PoE VEE Uvlo - VEE (PoE input voltage) under Voltage Lockout	The voltage of the power supply has dropped below 44 VDC. Adjust the voltage to between 46 and 57 VDC to eliminate this issue.
Over Allocated Power Limitation	When the total PD power consumption exceeds the total allocated power.

PoE Diagnose



PoE Diagnose helps users determine the PD conditions. The system provides the user with configuration options; select the best option for your PDs. Take the following steps to diagnose PD conditions:

Step 1: Check which port numbers will be diagnosed.

Step 2: Click **Activate**.

Step 3: The system will show the selected PD conditions.

Diagnose Configuration

Device Type

Item	Description
Not Present	No connection to the port
NIC	A NIC is connected to the port
IEEE 802.3af	An IEEE 802.3af PD is connected to the port
IEEE 802.3 at	An IEEE 802.3at PD is connected to the port
Legacy PoE Device	A legacy PD is connected to the port, and the PD's detected voltage is too high or low, or the PD's detected capacitance is too high.
Unknown	Unknown PD connected to the port

Classification

Item	Description
N/A	The port is not classified
0 to 4	Class 0 to 4
Unknown	Unknown class for the port; in this case it will usually be higher than class 4

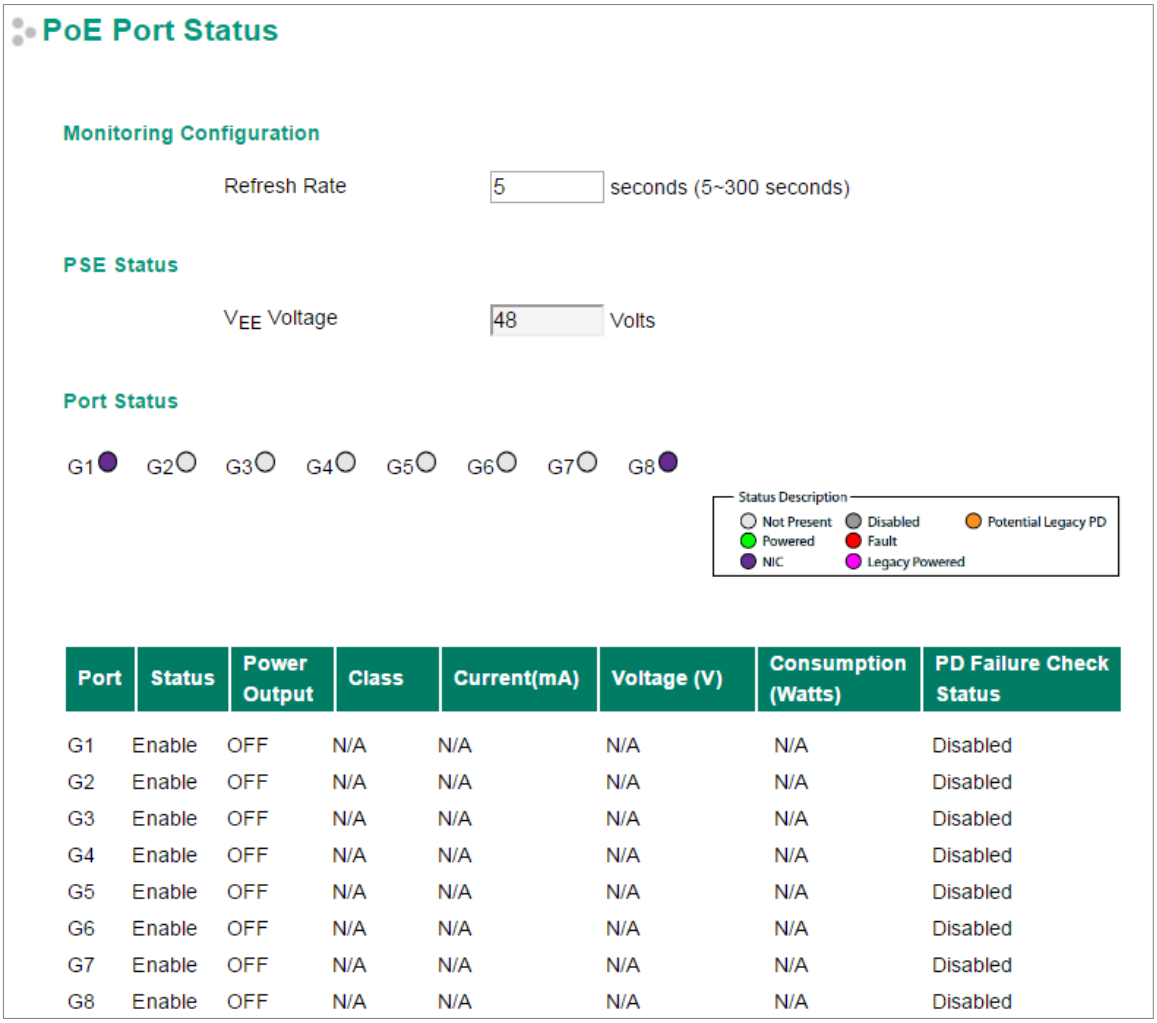
Voltage (V)

Item	Description
N/A	No voltage output on the port
Voltage	Display the voltage of the port

PoE Port Configuration Suggestion

Item	Description
Disable PoE power output	When detecting a NIC or unknown PD, the system suggests disabling PoE power output.
Enable "Legacy PD Detection"	When detecting a higher capacitance of PD, the system suggests enabling Legacy PD Detection.
Select Force Mode	When detecting higher/lower resistance or higher capacitance, the system suggests selecting Force Mode.
Select IEEE 802.3af/at auto mode	When detecting an IEEE 802.3 af/at PD, the system suggests selecting 802.3 af/at Auto mode.
Select high power output	When detecting an unknown classification, the system suggests selecting High Power output.
Raise the external power supply voltage to greater than 46 VDC	When the external supply voltage is detected at under 46 V, the system suggests raising the voltage.
Enable PoE function for detection	The system suggests enabling the PoE function.

PoE Port Status



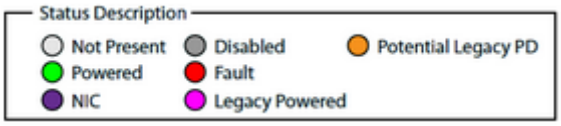
Port	Status	Power Output	Class	Current(mA)	Voltage (V)	Consumption (Watts)	PD Failure Check Status
G1	Enable	OFF	N/A	N/A	N/A	N/A	Disabled
G2	Enable	OFF	N/A	N/A	N/A	N/A	Disabled
G3	Enable	OFF	N/A	N/A	N/A	N/A	Disabled
G4	Enable	OFF	N/A	N/A	N/A	N/A	Disabled
G5	Enable	OFF	N/A	N/A	N/A	N/A	Disabled
G6	Enable	OFF	N/A	N/A	N/A	N/A	Disabled
G7	Enable	OFF	N/A	N/A	N/A	N/A	Disabled
G8	Enable	OFF	N/A	N/A	N/A	N/A	Disabled

Monitoring Configuration

Refresh Rate

Setting	Description	Factory Default
5 to 300	The period of time for the system to refresh the PoE Port Status (in seconds)	5

Port Status



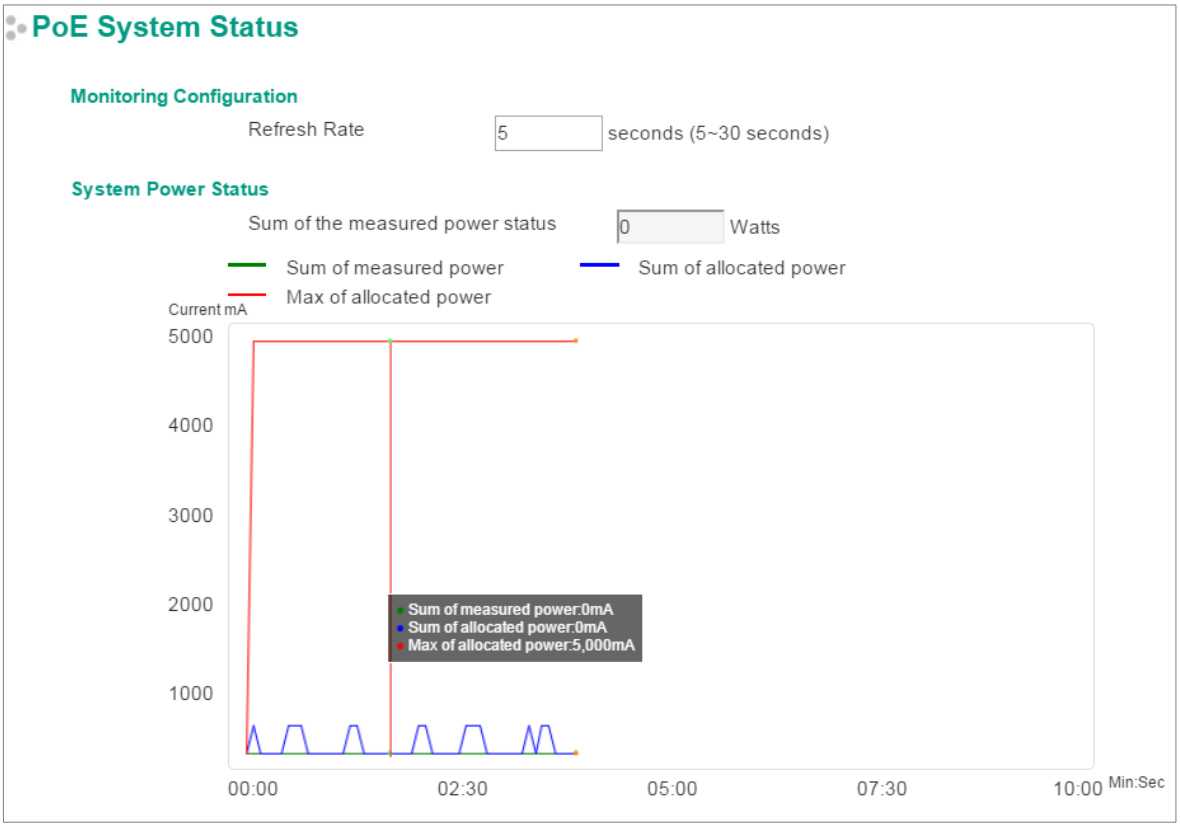
Status Description

Item	Description
Not Present	No connection to the port. PoE power is not being provided.
Powered	PoE power is being provided by the PSE.
NIC	System has detected a NIC connected to the port. PoE power is not being provided.
Disabled	The PoE function of the port is disabled. PoE power is not being provided.
Fault	In Force mode, the system has detected an out-of-range PD.
Legacy Powered	In Force mode, the system has detected a legacy PD.
Potential Legacy PD	In 802.3af/at or High Power mode; the system has detected a potential legacy PD. PoE power is not being provided.

Port Description

Item	Description
Status	Indicates if the PoE function is enabled or disabled.
Power Output	Indicates the power output of each PoE port.
Class	Indicates the classification of each PoE port.
Current (mA)	Indicates the actual current consumed by each PoE port.
Voltage (V)	Indicates the actual voltage consumed by each PoE port.
Consumption (Watts)	Indicates the actual Power consumed by each PoE port.
PD Failure Check Status	Indicates the PD Failure Check status of each PoE port. Alive: The system receives a response from all pings to the PD. Not Alive: The system receives no response from pings to the PD. Disabled: The PD Failure Check function is not activated.

PoE System Status



Monitoring Configuration

Refresh Rate

Setting	Description	Factory Default
5 to 300	If the Refresh Rate = T, then the PoE Port Status will be refreshed every T seconds.	5

System Power Status

System Power Status shows a graph of **Sum of measured power, Sum of allocated power,** and **Max of allocated power**. "Sum of measured power" (in green) shows the total measured power of all PDs, "Sum of allocated power" (in blue) shows the total allocated power, and "Max of allocated power" (in red) shows the threshold of total PoE power output. The graphs show **Current (mA)** versus **Sec. (second)** and are refreshed at the configured Refresh Rate.

Patent http://www.moxa.com/doc/operations/Moxa_Patent_Marking.pdf

VLAN

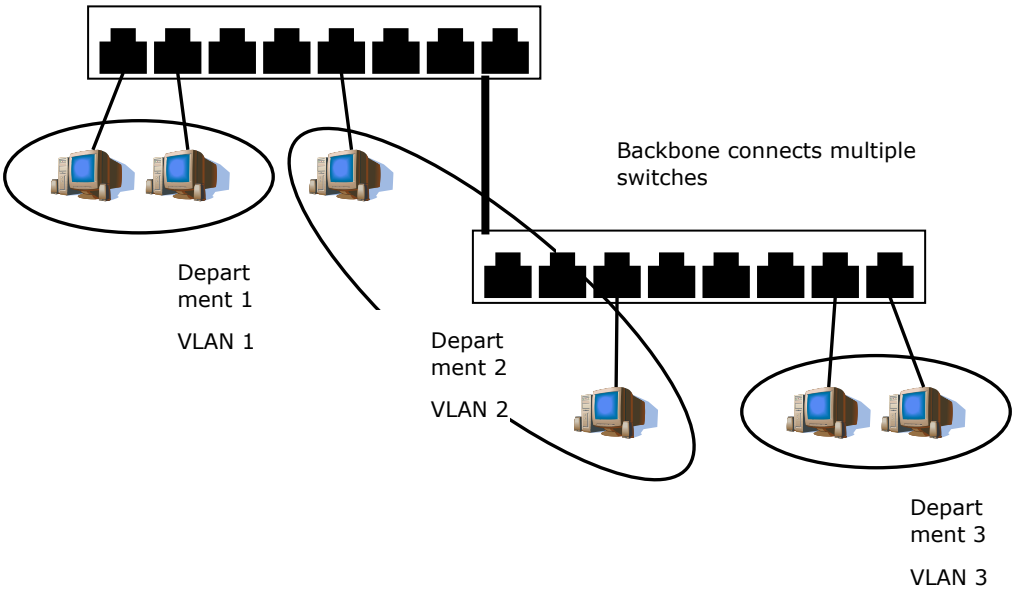
Setting up Virtual LANs (VLANs) on your Moxa switch increases the efficiency of your network by dividing the LAN into logical segments, as opposed to physical segments. In general, VLANs are easier to manage.

The Virtual LAN (VLAN) Concept

What is a VLAN?

A VLAN is a group of devices that can be located anywhere on a network, but which communicate as if they are on the same physical segment. With VLANs, you can segment your network without being restricted by physical connections—a limitation of traditional network design. With VLANs you can segment your network into:

- **Departmental groups—**You could have one VLAN for the marketing department, another for the finance department, and another for the product development department.
- **Hierarchical groups—**You could have one VLAN for directors, another for managers, and another for general staff.
- **Usage groups—**You could have one VLAN for email users and another for multimedia users.



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 ease the relocation of devices on networks:** With traditional networks, network administrators spend much of their time dealing with moves and changes. If users move to a different subnetwork, the addresses of each host must be updated manually. With a VLAN setup, if a host originally on the Marketing VLAN, is moved to a port on another part of the network, and retains its original subnet membership, you only need to specify that the new port is on the Marketing VLAN. You do not need to do any re-cabling.
- **VLANs provide extra security:** Devices within each VLAN can only communicate with other devices on the same VLAN. If a device on the Marketing VLAN needs to communicate with devices on the Finance VLAN, the traffic must pass through a routing device or Layer 3 switch.
- **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 and the Rackmount switch

Your Moxa switch provides support for VLANs using IEEE Std 802.1Q-1998. This standard allows traffic from multiple VLANs to be carried across one physical link. The IEEE Std 802.1Q-1998 standard allows each port on your Moxa switch to be placed as follows:

- On a single VLAN defined in the Moxa switch
- On several VLANs simultaneously using 802.1Q tagging

The standard requires that you define the 802.1Q VLAN ID for each VLAN on your Moxa switch before the switch can use it to forward traffic:

Managing a VLAN

A new or initialized Moxa switch contains a single VLAN—the Default VLAN. This VLAN has the following definition:

- *VLAN Name*—Management VLAN
- *802.1Q VLAN ID*—1 (if tagging is required)

All the ports are initially placed on this VLAN, and it is the only VLAN that allows you to access the management software of the Moxa switch over the network.

Between VLANs

If devices connected to a VLAN need to communicate with devices on a different VLAN, a router or Layer 3 switching device with connections to both VLANs needs to be installed. Communication between VLANs can only take place if they are all connected to a routing or Layer 3 switching device.

VLANs: Tagged and Untagged Membership

The Moxa switch supports 802.1Q VLAN tagging, a system that allows traffic for multiple VLANs to be carried on a single physical link (backbone, trunk). When setting up VLANs you need to understand when to use untagged or tagged membership of VLANs. Simply put, if a port is on a single VLAN it can be an untagged member, but if the port needs to be a member of multiple VLANs, a tagged membership must be defined.

A typical host (e.g., clients) will be an untagged member of one VLAN, defined as an **Access Port** in a Moxa switch, while an inter-switch connection will be a tagged member of all VLANs, defined as a **Trunk Port** in a Moxa switch.

The IEEE Std 802.1Q-1998 defines how VLANs operate within an open packet-switched network. An 802.1Q compliant packet carries additional information that allows a switch to determine which VLAN the port belongs to. If a frame is carrying the additional information, it is known as a tagged frame.

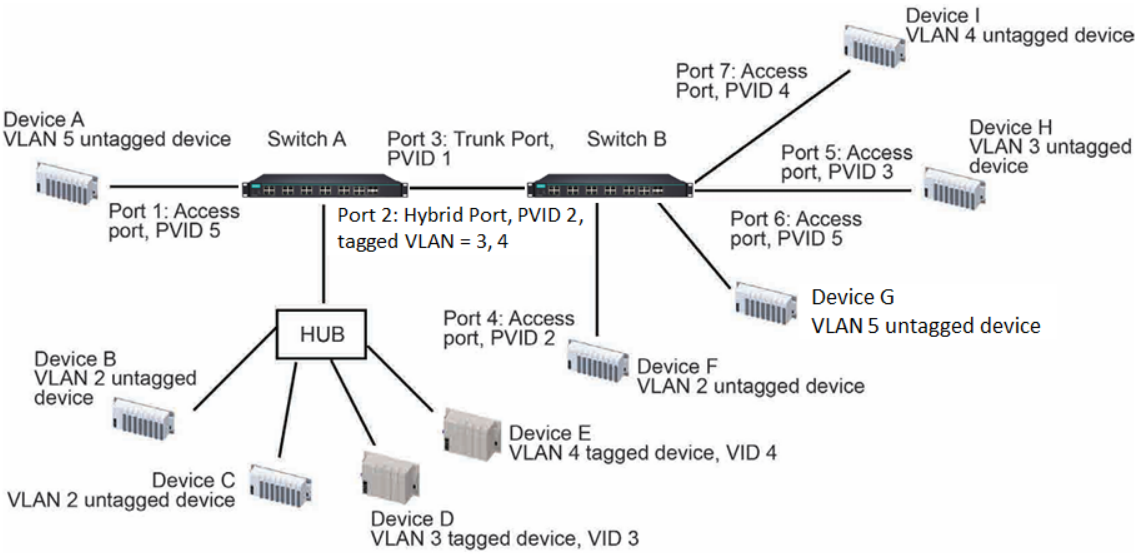
To carry multiple VLANs across a single physical link (backbone, trunk), each packet must be tagged with a VLAN identifier so that the switches can identify which packets belong in which VLAN. To communicate between VLANs, a router must be used.

The Moxa switch supports three types of VLAN port settings:

- **Access Port:** The port connects to a single device that is not tagged. The user must define the default port PVID that assigns which VLAN the device belongs to. Once the ingress packet of this Access Port egresses to another Trunk Port (the port needs all packets to carry tag information), the Moxa switch will insert this PVID into this packet so the next 802.1Q VLAN switch can recognize it.
- **Trunk Port:** The port connects to a LAN that consists of untagged devices, tagged devices, and/or switches and hubs. In general, the traffic of the Trunk Port must have a Tag. Users can also assign a PVID to a Trunk Port. The untagged packet on the Trunk Port will be assigned the default port PVID as its VID.
- **Hybrid Port:** The port is similar to a Trunk port, except users can explicitly assign tags to be removed from egress packets.

The following section illustrates how to use these ports to set up different applications.

Sample Applications of VLANs Using Moxa Switches



In this application:

- Port 1 connects a single untagged device and assigns it to VLAN 5; it should be configured as an **Access Port** with PVID 5.
- Port 2 connects a LAN with two untagged devices belonging to VLAN 2. One tagged device with VID 3 and one tagged device with VID 4. It should be configured as a **Hybrid Port** with PVID 2 for untagged devices and Fixed VLAN (Tagged) with 3 and 4 for tagged devices. Since each port can only have one unique PVID, all untagged devices on the same port must belong to the same VLAN.
- Port 3 connects with another switch. It should be configured as a **Trunk Port**. GVRP protocol will be used through the Trunk Port.
- Port 4 connects a single untagged device and assigns it to VLAN 2; it should be configured as an **Access Port** with PVID 2.
- Port 5 connects a single untagged device and assigns it to VLAN 3; it should be configured as an **Access Port** with PVID 3.
- Port 6 connects a single untagged device and assigns it to VLAN 5; it should be configured as an **Access Port** with PVID 5.
- Port 7 connects a single untagged device and assigns it to VLAN 4; it should be configured as an **Access Port** with PVID 4.

After the application is properly configured:

- Packets from Device A will travel through **Trunk Port 3** with tagged VID 5. Switch B will recognize its VLAN, pass it to port 6, and then remove tags received successfully by Device G, and vice versa.
- Packets from Devices B and C will travel through **Hybrid Port 2** with tagged VID 2. Switch B recognizes its VLAN, passes it to port 4, and then removes tags received successfully by Device F, and vice versa.
- Packets from Device D will travel through **Trunk Port 3** with tagged VID 3. Switch B will recognize its VLAN, pass to port 5, and then remove tags received successfully by Device H. Packets from Device H will travel through **Trunk Port 3** with PVID 3. Switch A will recognize its VLAN and pass it to port 2, but will not remove tags received successfully by Device D.
- Packets from Device E will travel through **Trunk Port 3** with tagged VID 4. Switch B will recognize its VLAN, pass it to port 7, and then remove tags received successfully by Device I. Packets from Device I will travel through **Trunk Port 3** with tagged VID 4. Switch A will recognize its VLAN and pass it to port 2, but will not remove tags received successfully by Device E.

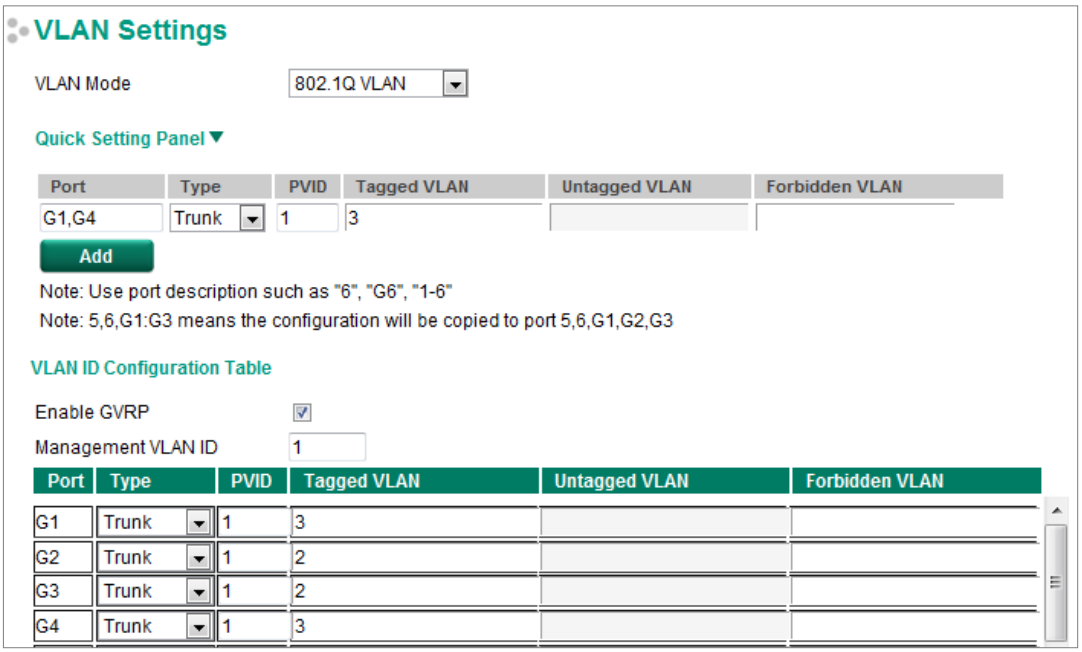
Configuring a Virtual LAN

To configure 802.1Q VLAN and Unaware VLANs on the Moxa switch, use the **VLAN Settings** page to configure the ports for either an **802.1Q VLAN** or **Unaware VLAN**.

VLAN Mode

Setting	Description	Factory Default
802.1Q VLAN	Sets VLAN mode to 802.1Q VLAN	802.1Q VLAN
Unaware VLAN	Sets VLAN mode to unaware VLAN	

VLAN Settings: 802.1Q



When VLAN Mode is set to 802.1Q VLAN, the configuration options will be divided into the **Quick Setting Panel** and **VLAN ID Configuration Table**. The Quick Setting Panel is generally used to configure VLAN settings for groups of ports, with the settings pushed down to the VLAN ID Configuration Panel when the user clicks the Add button. The VLAN ID Configuration Table can be used to configure the settings for individual ports.

Quick Setting Panel

Administrators can use the **Quick Setting Panel** to quickly configure VLAN settings for single ports or groups of ports. To configure a group of ports, type the port names in the **Port** column, separated commas (,) for individual port names, or colons (:) to indicate a range of ports. For example, typing "G1,G3" applies the settings to ports G1 and G3, whereas typing "G1:G3" applies the settings to ports G1, G2, and G3. Next, if necessary, configure **Type, PVID, Tagged VLAN, Untagged VLAN,** and **Forbidden VLAN**, and then click the **Add** button to move the settings down to the table at the bottom of the window.

VLAN ID Configuration Table

Enable GVRP

Setting	Description	Factory Default
Checked/Unchecked	Check the checkbox to enable the GVRP function. Remove the checkmark to disable the GVRP function.	Checked

Management VLAN ID

Setting	Description	Factory Default
1 to 4094	Assigns the VLAN ID to this Moxa switch.	1

NOTE

Some of the following settings can be modified in the Quick Setting Panel.

Port

Setting	Description	Factory Default
Port name	Read only	N/A

Type

Setting	Description	Factory Default
Access	When this port is connected to a single device, without tags.	Access
Trunk	When this port is connected to another 802.1Q VLAN aware switch.	
Hybrid	When this port is connected to another Access 802.1Q VLAN aware switch or another LAN that combines tagged and/or untagged devices and/or other switches/hubs.	

WARNING

For communication redundancy in the VLAN environment, set **Redundant Port Coupling Ports** and **Coupling Control Ports** to **Trunk Port**, since these ports act as the **backbone** for transmitting packets from different VLANs to different Moxa switch units.

PVID

Setting	Description	Factory Default
1 to 4094	Sets the default VLAN ID for untagged devices connected to the port.	1

Tagged VLAN

Setting	Description	Factory Default
1 to 4094	This field will be active only when selecting the Trunk or Hybrid port type. Set the other VLAN ID for tagged devices that connect to the port. Use commas to separate different VIDs.	None

Untagged VLAN

Setting	Description	Factory Default
VID range from 1 to 4094	This field is only active when the Hybrid port type is selected. Set the other VLAN ID for tagged devices that connect to the port and tags that need to be removed in egress packets. Use commas to separate different VIDs.	None

Forbidden VLAN

Setting	Description	Factory Default
1 to 4094	This field is only active when Trunk or Hybrid port type is selected. Set the other VLAN IDs that will not be supported by this port. Use commas to separate different VIDs.	None

NOTE

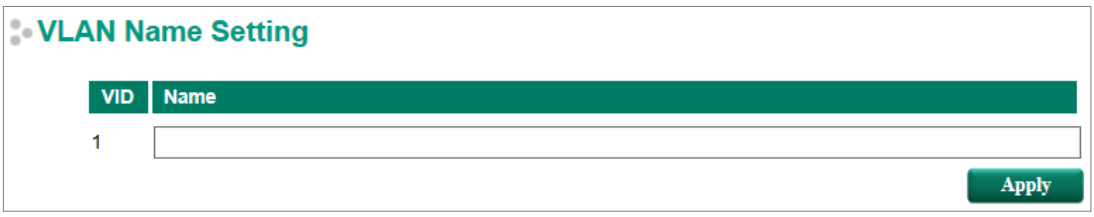
The **Quick Setting Panel** provides a quick way of configuring multiple VLAN ports with the same setting.

VLAN Settings: Unaware VLAN

The switch ignores VLAN tags in frames or packets even for VLAN ID 0. Any VLAN tagging that exists is ignored and remains in the frame. The switch does not strip the tag from the frames, so if the switch receives a tagged frame, the frame is delivered tagged to the destination MAC. Some Intelligent Electronic Device (IED) vendors might use VLAN ID 0 as the default value when a VLAN ID value is not explicitly configured. It is recommended that you avoid the 0 value when configuring a default VLAN ID value.

VLAN Name Setting

For the 802.1Q VLAN, the user is able to set the VLAN name of each VLAN ID (VID).



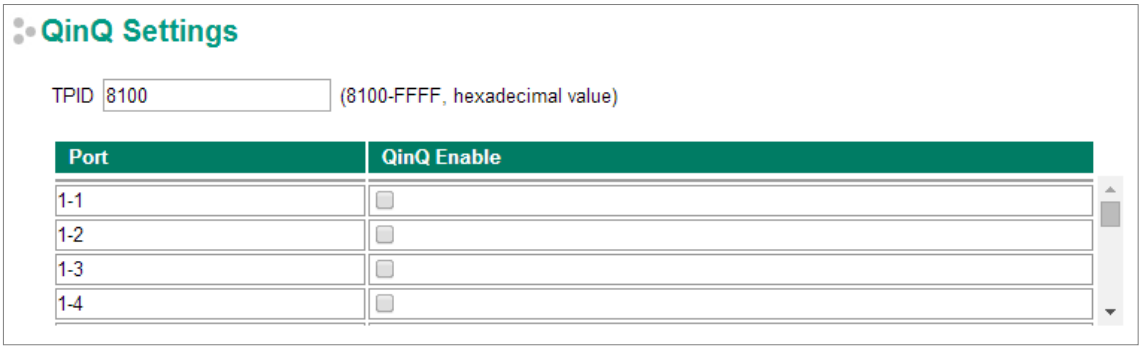
VLAN Name Setting

Setting	Description	Factory Default
Name	The VLAN name can only include these characters, a-z/A-Z/0-9/-/_/	Null

QinQ Settings

NOTE

Moxa's layer 3 switches support the IEEE 802.1ad QinQ function, which allows users to tag double VLAN headers into a single Ethernet frame.



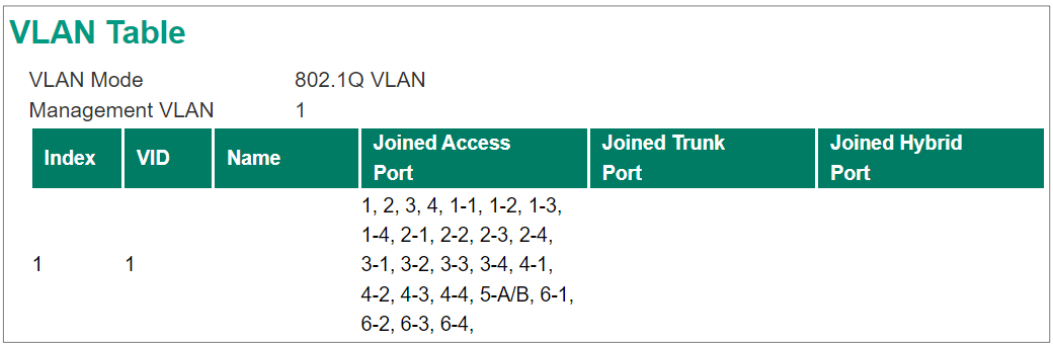
TPID

Setting	Description	Factory Default
8100 to FFFF	Assign the TPID of the second VLAN tag	8100

QinQ Enable

Setting	Description	Factory Default
Enable/Disable	Enable VLAN QinQ function	Disable

VLAN Table

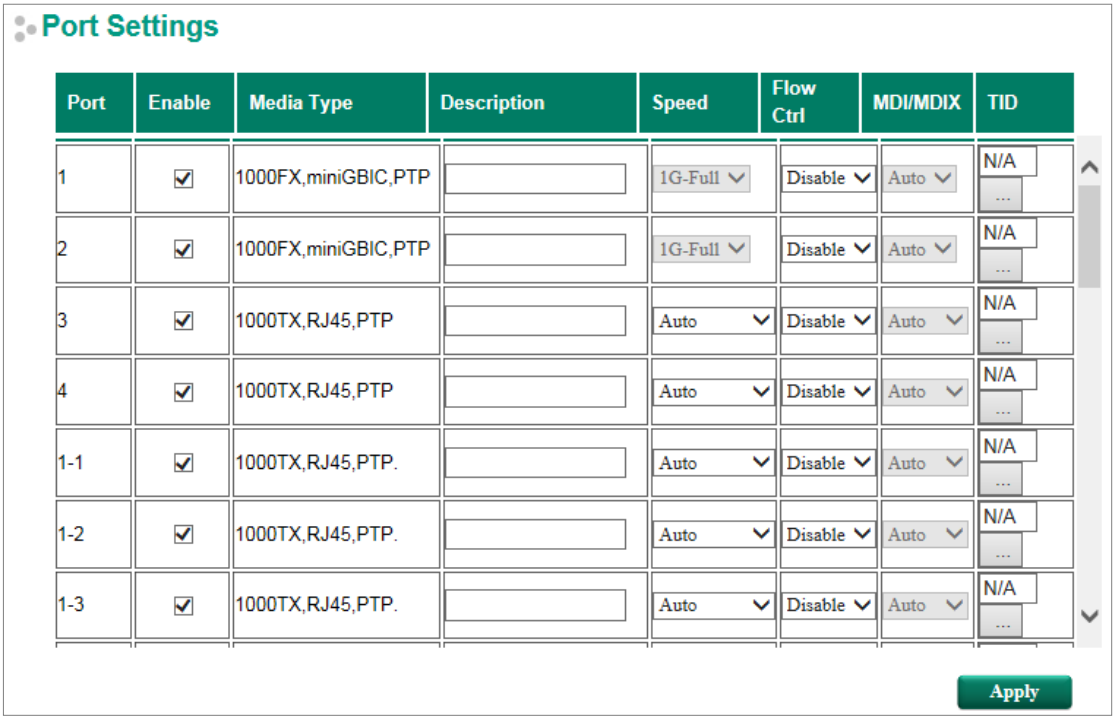


Use the 802.1Q VLAN table to review the VLAN groups that were created, VLAN Name, Joined Access Ports, Trunk Ports, and Hybrid Ports.

Port

Port Settings

Port settings are included to give the user control over port access, port transmission speed, flow control, and port type (MDI or MDIX).



Enable

Setting	Description	Factory Default
Checked	Allows data transmission through the port.	Checked
Unchecked	Immediately shuts off port access.	

Media Type

Setting	Description	Factory Default
Media type	Displays the media type for each module's port	N/A

Description

Setting	Description	Factory Default
Max. 63 characters	Specifies an alias for the port to help administrators differentiate between different ports. Example: PLC 1	None

Speed

Setting	Description	Factory Default
Auto	Allows the port to use the IEEE 802.3u protocol to negotiate with connected devices. The port and connected devices will determine the best speed for that connection.	Auto
100M-Full	Choose one of these fixed speed options if the connected Ethernet device has trouble auto-negotiating for line speed.	
100M-Half		
10M-Full		
10M-Half		

FDX Flow Ctrl

This setting enables or disables flow control for the port when the port's Speed is set to Auto. The final result will be determined by the Auto process between the Moxa switch and connected devices.

Setting	Description	Factory Default
Enable	Enables flow control for this port when the port's Speed is set to Auto.	Disabled
Disable	Disables flow control for this port when the port's Speed is set to Auto.	

MDI/MDIX

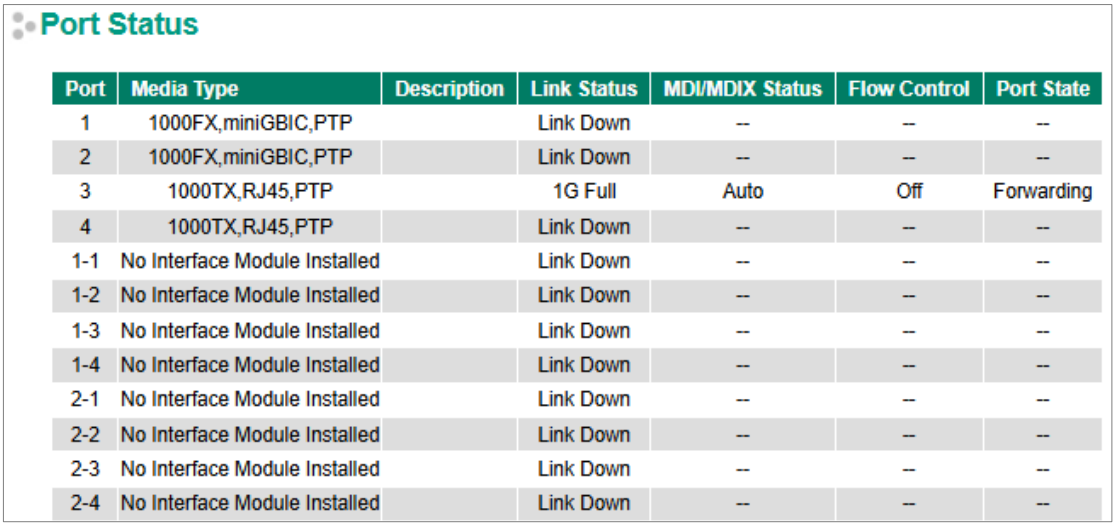
Setting	Description	Factory Default
Auto	Allows the port to auto-detect the port type of the connected Ethernet device and change the port type accordingly.	Auto
MDI	Choose MDI or MDIX if the connected Ethernet device has trouble auto-negotiating for port type.	
MDIX		

NOTE

For the Gigabit ports, MDI/MDIX is only Auto mode.

Port Status

The following table shows the status of each port, including the media type, link status, flow control, and port state.



Port	Media Type	Description	Link Status	MDI/MDIX Status	Flow Control	Port State
1	1000FX,miniGBIC,PTP		Link Down	--	--	--
2	1000FX,miniGBIC,PTP		Link Down	--	--	--
3	1000TX,RJ45,PTP		1G Full	Auto	Off	Forwarding
4	1000TX,RJ45,PTP		Link Down	--	--	--
1-1	No Interface Module Installed		Link Down	--	--	--
1-2	No Interface Module Installed		Link Down	--	--	--
1-3	No Interface Module Installed		Link Down	--	--	--
1-4	No Interface Module Installed		Link Down	--	--	--
2-1	No Interface Module Installed		Link Down	--	--	--
2-2	No Interface Module Installed		Link Down	--	--	--
2-3	No Interface Module Installed		Link Down	--	--	--
2-4	No Interface Module Installed		Link Down	--	--	--

Link Aggregation

Link aggregation involves grouping links into a link aggregation group. A MAC client can treat link aggregation groups as if they were a single link.

The Moxa switch's port trunking feature allows devices to communicate by aggregating up to 4 trunk groups, with a maximum of 8 ports for each group. If one of the 8 ports fails, the other seven ports will automatically provide backup and share the traffic.

Port trunking can be used to combine up to 8 ports between two Moxa switches. If all ports on both switches are configured as 100BaseTX and they are operating in full duplex, the potential bandwidth of the connection will be 1600 Mbps.

The Port Trunking Concept

Moxa has developed a port trunking protocol that provides the following benefits:

- Greater flexibility in setting up your network connections, since the bandwidth of a link can be doubled, tripled, or quadrupled.
- Redundancy—if one link is broken, the remaining trunked ports share the traffic within this trunk group.
- Load sharing—MAC client traffic can be distributed across multiple links.

To avoid broadcast storms or loops in your network while configuring a trunk, first disable or disconnect all ports that you want to add to the trunk or remove from the trunk. After you finish configuring the trunk, enable or re-connect the ports.

If all ports on both switch units are configured as 100BaseTX and they are operating in full duplex mode, the potential bandwidth of the connection will be up to 1.6 Gbps. This means that users can double, triple, or quadruple the bandwidth of the connection by port trunking between two Moxa switches.

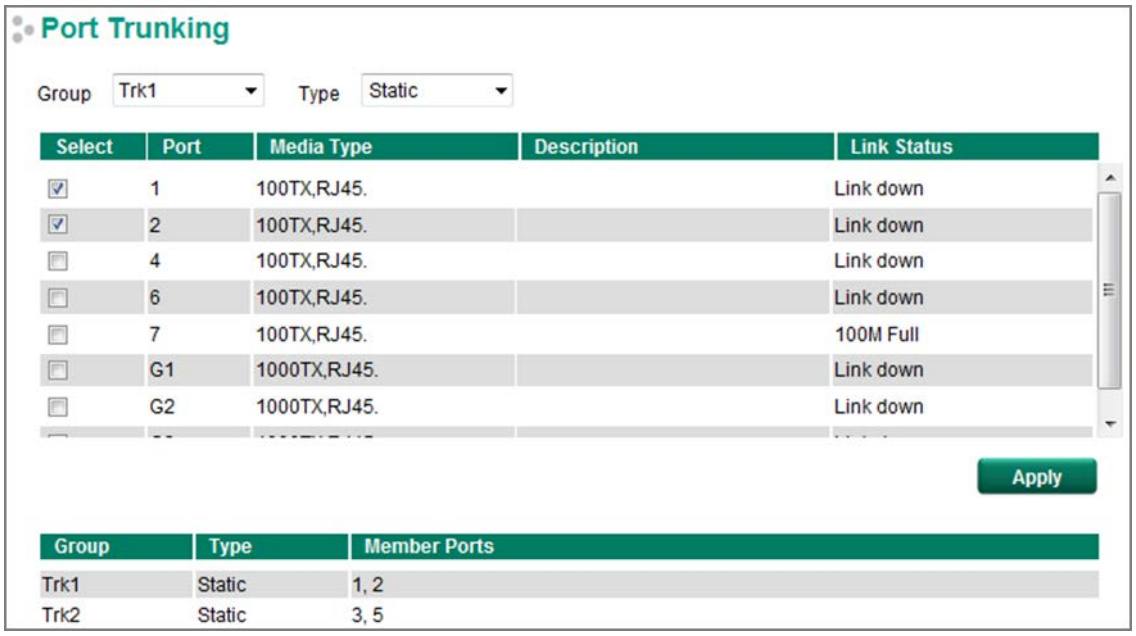
Each Moxa switch can set a maximum of 3 port trunking groups. When you activate port trunking, certain settings on each port will be reset to factory default values or disabled:

- Communication redundancy will be reset.
- 802.1Q VLAN will be reset.
- Multicast Filtering will be reset.
- Port Lock will be reset and disabled.
- Set Device IP will be reset.
- Mirror will be reset.

After port trunking has been activated, you can configure these items again for each trunking port.

Port Trunking

The **Port Trunking Settings** page is where ports are assigned to a trunk group.



Step 1: Select the desired **Trunk Group**.

Step 2: Select the **Trunk Type** (Static or LACP).

Step 3: Select the Trunk Group to modify the desired ports if necessary.

Trunk Group (maximum of 4 trunk groups)

Setting	Description	Factory Default
Trk1, Trk2, Trk3, Trk4 (Depends on switching chip capability; some Moxa switches only support 3 trunk groups)	Specifies the current trunk group.	Trk1

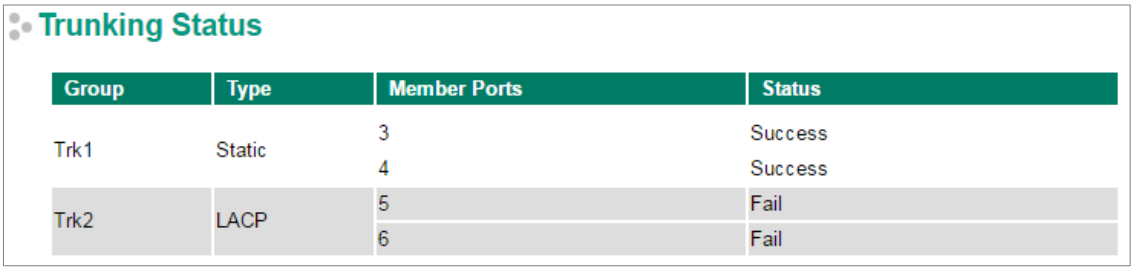
The PT-G7728/G8728 supports 4 Trunk Groups

Trunk Type

Setting	Description	Factory Default
Static	Selects Moxa's static trunking protocol.	Static
LACP	Selects LACP (IEEE 802.3ad, Link Aggregation Control Protocol).	Static

Trunking Status

The **Trunking Status table** shows the Trunk Group configuration status.



Link-Swap Fast Recovery

The Link-Swap Fast Recovery function, which is enabled by default, allows the Moxa switch to return to normal operation extremely quickly after devices are unplugged and then re-plugged into different ports. The recovery time is in the order of a few milliseconds (compare this with standard commercial switches for which the recovery time could be on the order of several minutes). To disable the Link-Swap Fast Recovery function, or to re-enable the function after it has already been disabled, access either the Console utility's **Link-Swap recovery** page, or the Web Browser interface's **Link-Swap fast recovery** page, as shown below.

Link-Swap-Fast-Recovery

Setting	Description	Factory Default
Enable/Disable	Select the checkbox to enable the Link-Swap-Fast-Recovery function	Enable

STP/RSTP/MSTP

The STP/RSTP/MSTP Concept

Spanning Tree Protocol (STP) was designed to help reduce link failures on a network, and provide an automatic means of avoiding 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 RSTP/STP on every Moxa switch connected to your network.

Rapid Spanning Tree Protocol (RSTP) implements the Spanning Tree Algorithm and Protocol defined by IEEE 802.1D-2004. RSTP provides the following benefits:

- The topology of a bridged network will be determined much more quickly compared to STP.
- RSTP is backwards compatible with STP, making it relatively easy to deploy. For example:
  - Defaults to sending 802.1D style BPDUs if packets with this format are received.
  - STP (802.1D) and RSTP (802.1w) can operate on different ports of the same switch, which is particularly helpful when switch ports connect to older equipment such as legacy switches.

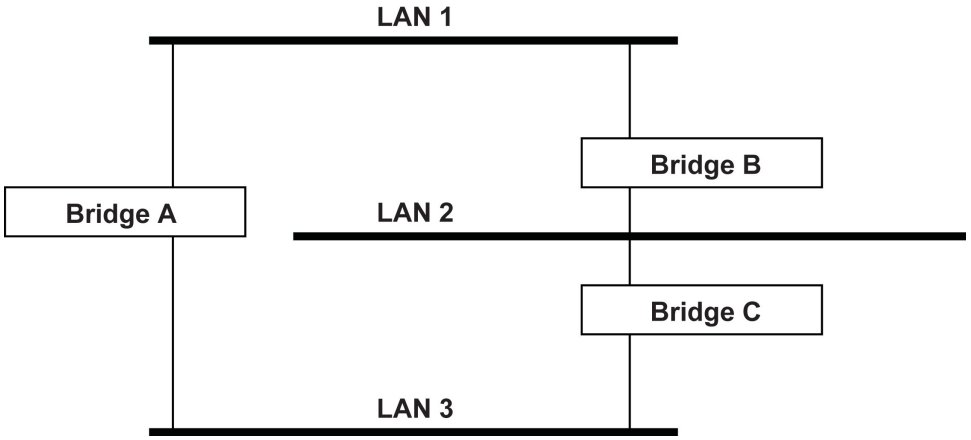
You get essentially the same functionality with RSTP and STP. To see how the two systems differ, see the Differences between STP, RSTP, and MSTP section in this chapter.

What is STP?

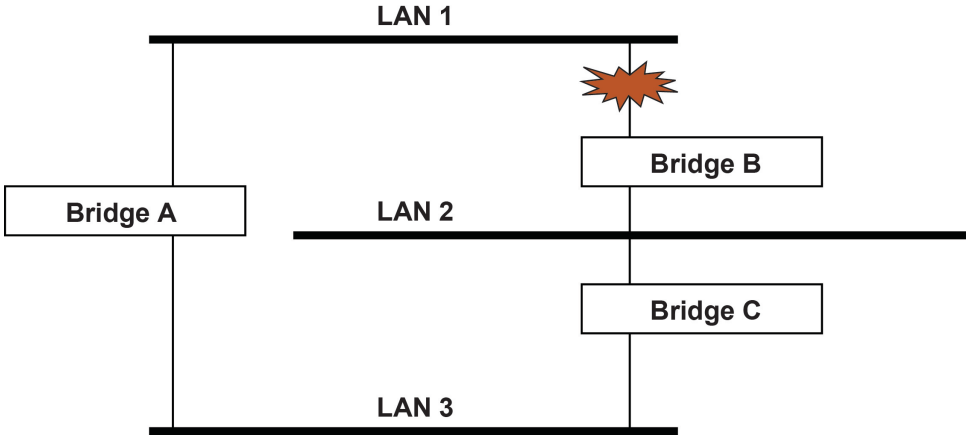
STP (802.1D) is a bridge-based system that is used to implement parallel paths for network traffic. STP uses a loop-detection process to:

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

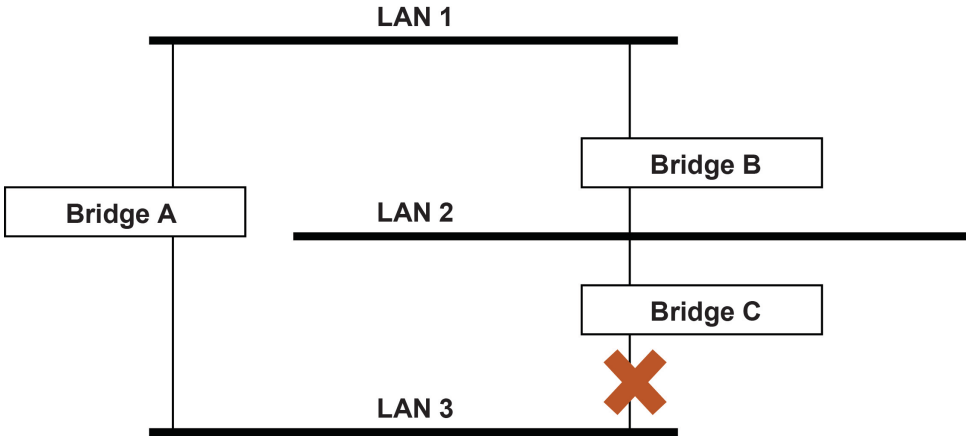
The figure below shows a network made up of three LANs separated by three bridges. Each segment uses at most two paths to communicate with the other segments. Since this configuration can give rise to loops, the network will overload if STP is NOT enabled.



If STP is enabled, it will detect duplicate paths and prevent, or block, one of the paths from forwarding traffic. In the following example, STP determined that traffic from LAN segment 2 to LAN segment 1 should flow through bridges C and A since this path has a greater bandwidth and is therefore more efficient.



What happens if a link failure is detected? As shown in next figure, the STP process reconfigures the network so that traffic from LAN segment 2 flows through bridge B.



STP will determine which path between each bridged 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 3 figures, STP first determined that the path through bridge C was the most efficient, and as a result, blocked the path through bridge B. After the failure of bridge C, STP re-evaluated the situation and opened the path through Bridge B.

How STP Works

When enabled, STP determines the most appropriate path for traffic through a network. The way it does this is outlined in the sections below.

STP Requirements

Before STP can configure the network, the system must satisfy the following requirements:

- All bridges must be able to communicate with each other. The communication is carried out using Bridge Protocol Data Units (BPDUs), which are transmitted in packets with a known multicast address.
- Each bridge must have a Bridge Identifier that specifies which bridge acts as the central reference point, or Root Bridge, for the STP system—bridges with a lower Bridge Identifier are more likely to be designated as the Root Bridge. The Bridge Identifier is calculated using the MAC address of the bridge and a priority defined for the bridge. For example, the default priority setting of Moxa switches is 32768.
- Each port has a cost that specifies the efficiency of each link. The efficiency cost is usually determined by the bandwidth of the link, with less efficient links assigned a higher cost.

STP Calculation

The first step of the STP process is to perform calculations. During this stage, each bridge on the network transmits BPDUs. The following items will be calculated:

- Which bridge should be the **Root Bridge**. The Root Bridge is the central reference point from which the network is configured.
- The **Root Path Costs** for each bridge. This is the cost of the paths from each bridge to the Root Bridge.
- The identity of each bridge's **Root Port**. The Root Port is the port on the bridge that connects to the Root Bridge via the most efficient path. In other words, the port connected to the Root Bridge via the path with the lowest Root Path Cost. The Root Bridge, however, does not have a Root Port.
- The identity of the **Designated Bridge** for each LAN segment. The Designated Bridge is the bridge with the lowest Root Path Cost from that segment. If several bridges have the same Root Path Cost, the one with the lowest Bridge Identifier becomes the Designated Bridge. Traffic transmitted in the direction of the Root Bridge will flow through the Designated Bridge. The port on this bridge that connects to the segment is called the **Designated Bridge Port**.

STP Configuration

After all of the bridges on the network agree on the identity of the Root Bridge, and all other relevant parameters have been established, each bridge is configured to forward traffic only between its Root Port and the Designated Bridge Ports for the respective network segments. All other ports are blocked, which means that they will not be allowed to receive or forward traffic.

STP Reconfiguration

Once the network topology has stabilized, each bridge listens for Hello BPDUs transmitted from the Root Bridge at regular intervals. If a bridge does not receive a Hello BPDU after a certain interval (the Max Age time), the bridge assumes that the Root Bridge, or a link between itself and the Root Bridge, has ceased to function. This will trigger the bridge to reconfigure the network to account for the change. If you have configured an SNMP trap destination, the first bridge to detect the change will send out an SNMP trap when the topology of your network changes.

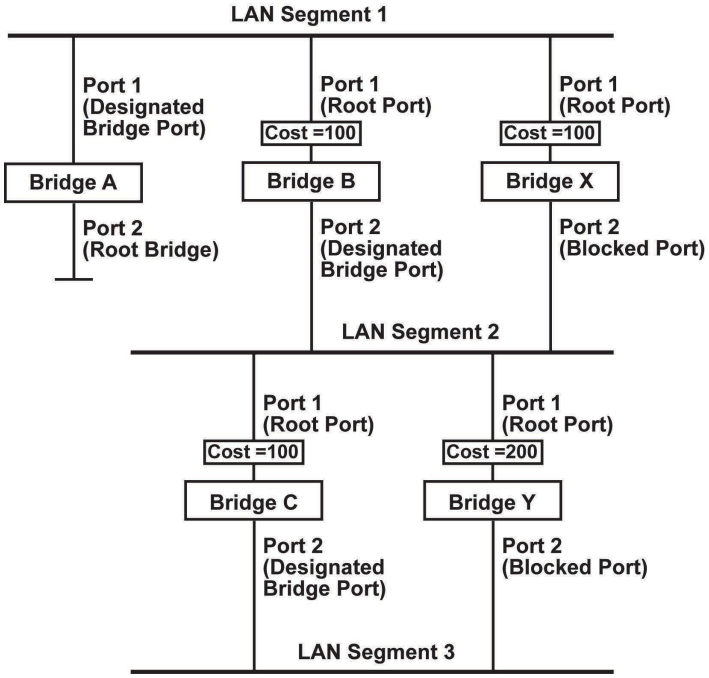
Differences between STP, RSTP, and MSTP

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. MSTP uses VLANs to create multiple spanning trees in a network, which significantly improves network resource utilization while maintaining a loop-free environment.

STP Example

The LAN shown in the following figure has three segments, with adjacent segments connected using two possible links. The various STP factors, such as Cost, Root Port, Designated Bridge Port, and Blocked Port are shown in the figure.

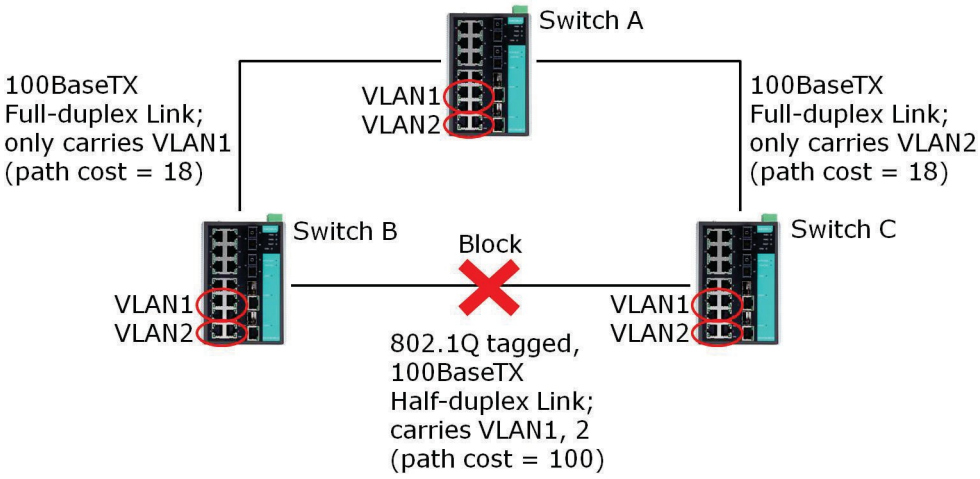


- Bridge A has been selected as the Root Bridge, since it was determined to have the lowest Bridge Identifier on the network.
- Since Bridge A is the Root Bridge, it is also the Designated Bridge for LAN segment 1. Port 1 on Bridge A is selected as the Designated Bridge Port for LAN Segment 1.
- Ports 1 of Bridges B, C, X, and Y are all Root Ports since they are nearest to the Root Bridge, and therefore have the most efficient path.
- Bridges B and X offer the same Root Path Cost for LAN segment 2. However, Bridge B was selected as the Designated Bridge for that segment since it has a lower Bridge Identifier. Port 2 on Bridge B is selected as the Designated Bridge Port for LAN Segment 2.
- Bridge C is the Designated Bridge for LAN segment 3, because it has the lowest Root Path Cost for LAN Segment 3:
  - The route through bridges C and B costs 200 (C to B=100, B to A=100)
  - The route through bridges Y and B costs 300 (Y to B=200, B to A=100)
- The Designated Bridge Port for LAN Segment 3 is port 2 on bridge C.

Using STP on a Network with Multiple VLANs

IEEE Std 802.1D, 1998 Edition, does not take into account VLANs when calculating STP information—the calculations only depend on the physical connections. Consequently, some network configurations will result in VLANs being subdivided into a number of isolated sections by the STP system. You must ensure that every VLAN configuration on your network takes into account the expected STP topology and alternative topologies that may result from link failures.

The following figure shows an example of a network that contains VLANs 1 and 2. The VLANs are connected using the 802.1Q-tagged link between switch B and Switch C. By default, this link has a port cost of 100 and is automatically blocked because the other switch-to-switch connections have a port cost of 36 (18+18). This means that both VLANs are now subdivided—VLAN 1 on switches A and B cannot communicate with VLAN 1 on switch C, and VLAN 2 on switches A and C cannot communicate with VLAN 2 on switch B.



To avoid subdividing VLANs, all inter-switch connections should be made members of all available 802.1Q VLANs. This will ensure connectivity at all times. For example, the connections between switches A and B, and between switches A and C, should be 802.1Q tagged and carrying VLANs 1 and 2 to ensure connectivity.

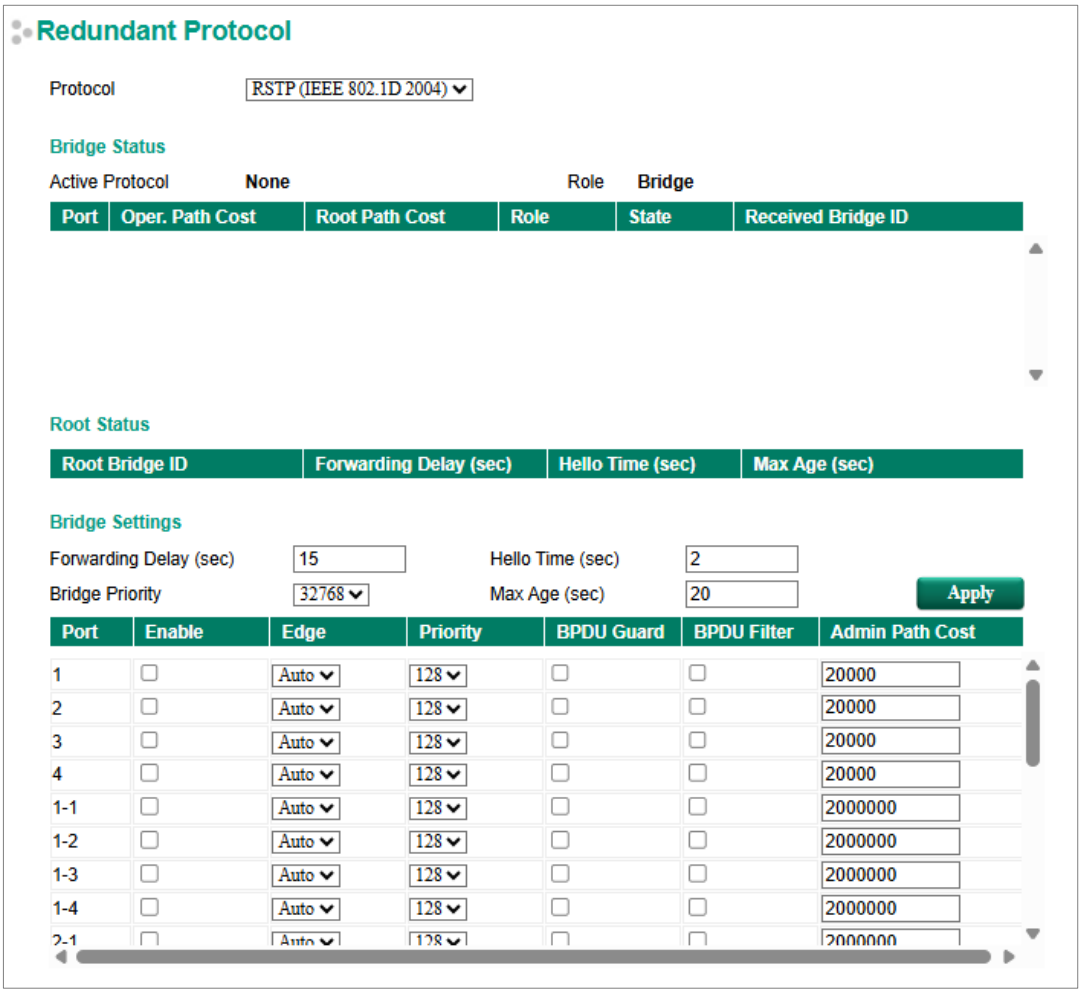
Configuring STP/RSTP

Use the scrolling bar at the top of the Redundancy Protocol page to select among **Turbo Ring**, **Turbo Ring V2**, **Turbo Chain**, **RSTP**, or **MSTP**. Note that configuration pages for these five protocols are different.

Protocol

Setting	Description	Factory Default
Turbo Ring	Select this item to change to the Turbo Ring configuration page.	None
Turbo Ring V2	Select this item to change to the Turbo Ring V2 configuration page.	
Turbo Chain	Select this item to change to the Turbo Chain configuration page.	
RSTP (IEEE 802.1D-2004)	Select this item to change to the RSTP configuration page.	
MSTP (IEEE 802.1s)	Select this item to change to the MSTP configuration page.	

The following figure indicates which Spanning Tree Protocol parameters can be configured. A more detailed explanation of each parameter follows.



Explanation of "Status" Items

Active Protocol

Shows which redundancy protocol is in use: **Turbo Ring**, **Turbo Ring V2**, **Turbo Chain**, **RSTP**, **MSTP**, or **None**.

Role

This field only appears when RSTP mode is selected. The field indicates whether or not this switch is the ***Root*** of the Spanning Tree (the root is determined automatically).

Explanation of "Settings" Items

Forwarding delay (sec.)

Setting	Description	Factory Default
Numerical value input by user	The amount of time this device waits before checking to see if it should change to a different state.	15

Bridge priority

Setting	Description	Factory Default
Numerical value selected by user	Increase this device's bridge priority by selecting a lower number. A device with a higher bridge priority has a greater chance of being established as the root of the Spanning Tree topology.	32768

Hello time (sec.)

Setting	Description	Factory Default
Numerical value input by user	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. The "hello time" is the amount of time the root waits between sending hello messages.	2

Max. Age (sec.)

Setting	Description	Factory Default
Numerical value input by user	If this device is not the root, and it has not received a hello message from the root in an amount of time equal to "Max. Age," 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.	20

Enable STP per Port

Setting	Description	Factory Default
Enable/Disable	Select to enable the port as a node on the Spanning Tree topology.	Disabled

NOTE

We suggest not enabling the Spanning Tree Protocol once the port is connected to a device (PLC, RTU, etc.) as opposed to network equipment. The reason is that it will cause unnecessary negotiation.

Edge

Setting	Description	Factory Default
Auto	If the port does not receive a BPDU within 3 seconds, the port will be in the forwarding state. Once the port receives a BPDU, it will start the RSTP negotiation process.	Auto
True	The port is an edge port. Once the port receives a BPDU, it will start the RSTP negotiation process.	
False	The port is set as the normal RSTP port.	

Priority

Setting	Description	Factory Default
Numerical value selected by user	Increase this port's priority as a node on the Spanning Tree topology by entering a lower number.	128

PDU Guard

Setting	Description	Factory Default
BPDU Guard	Unchecked: Disable BPDU Guard	Unchecked
	Checked: Enable BPDU Guard	

BPDU Guard is a protection mechanism that prevents looping caused from misconnection or wrong setting of edge ports. Edge ports aren't supposed to connect to devices that are capable of sending BPDUs. 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. By default, this function is disabled.

PDU Filter

Setting	Description	Factory Default
BPDU Filter	Unchecked: Disable BPDU Filter	Unchecked
	Checked: Enable BPDU Filter	

BPDU filter prevents a port from sending and processing BPDUs. A BPDU filter enabled port cannot transmit any BPDUs and will drop all received BPDUs. If edge port is disabled, BPDU filter cannot be enabled on this port. By default, this function is disabled.

Cost

Setting	Description	Factory Default
Numerical value input by user	Input a higher cost to indicate that this port is less suitable as a node for the Spanning Tree topology.	200000

Status

Indicates the current Spanning Tree status of this port. **Forwarding** for normal transmission, **Blocking** for block transmission, or Link down for no connection.

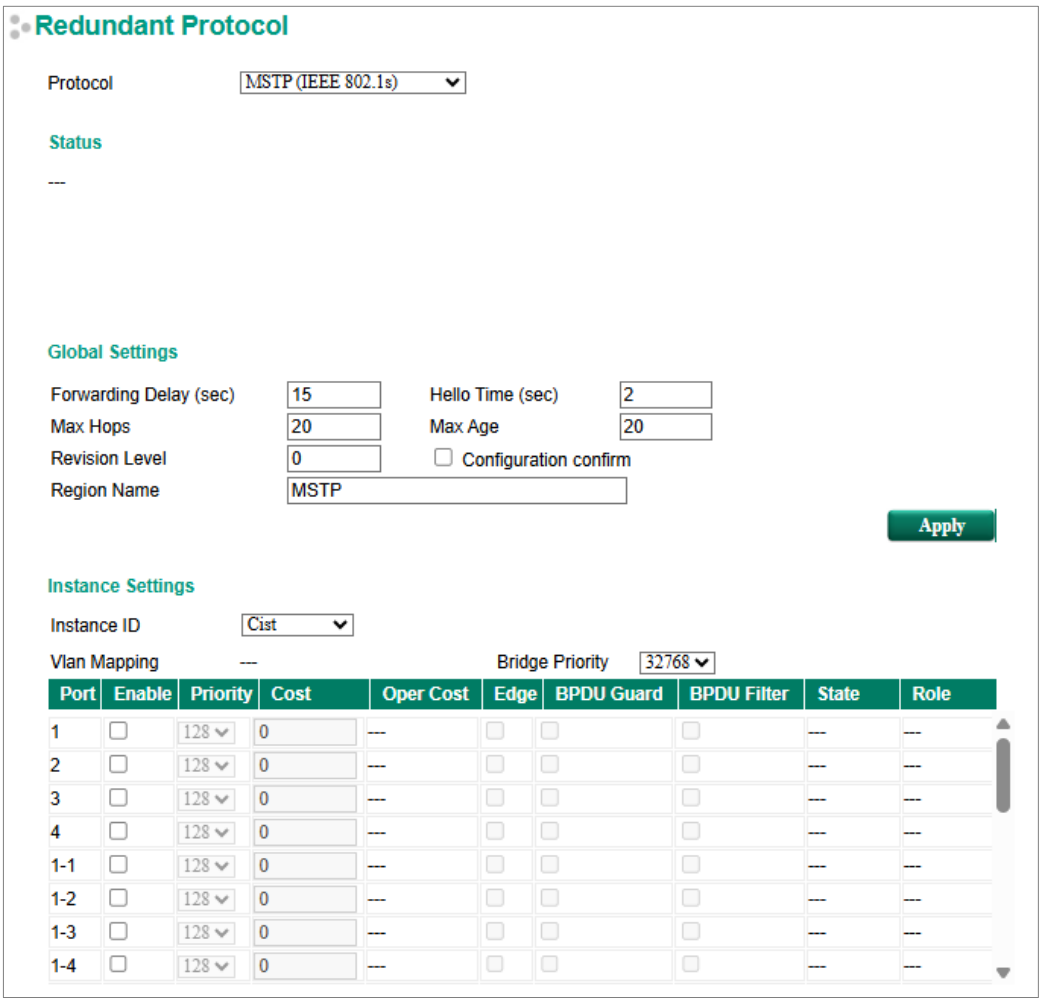
Configuring MSTP

Use the scrollbar at the top of the Redundancy Protocol page to select **Turbo Ring**, **Turbo Ring V2**, **Turbo Chain**, **RSTP**, or **MSTP**. Note that configuration pages for these five protocols are different.

Protocol

Setting	Description	Factory Default
Turbo Ring	Select this item to change to the Turbo Ring configuration page.	None
Turbo Ring V2	Select this item to change to the Turbo Ring V2 configuration page.	
Turbo Chain	Select this item to change to the Turbo Chain configuration page.	
RSTP (IEEE 802.1D-2004)	Select this item to change to the RSTP configuration page.	
MSTP (IEEE 802.1s)	Select this item to change to the MSTP configuration page.	

The following figure indicates which Multiple Spanning Tree Protocol parameters can be configured. A more detailed explanation of each parameter follows.



Explanation of "Status" Items

Status

Indicates the Root bridge of the Spanning Tree.

Explanation of "Global Settings" Items

Forwarding Delay (sec.)

Setting	Description	Factory Default
Numerical value input by user (4-30)	The amount of time this device waits before checking to see if it should change to a different state.	15

Hello time (sec.)

Setting	Description	Factory Default
Numerical value input by user (1-10)	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. The "hello time" is the amount of time the root waits between sending hello messages.	2

Max Hops

Setting	Description	Factory Default
Numerical value input by user (6-40)	The MSTP maximum hops value is the maximum number of hops in the region. Configure the maximum number of hops a BPDU can be forwarded in the MSTP region.	20

Max. Age (sec.)

Setting	Description	Factory Default
Numerical value input by user (6-40)	If this device is not the root, and it has not received a hello message from the root in an amount of time equal to "Max. Age," 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 to set up a new Spanning Tree topology.	20

Revision Level

Setting	Description	Factory Default
Numerical value input by user (0-65535)	The MSTP revision level is the revision number of the configuration. All switches in an MSTP region must be configured with the same revision level.	0

Region Name

Setting	Description	Factory Default
Character string	The region name helps define the logical boundary of the network. All switches in an MSTP region must be configured with the same name.	MSTP

Configuration confirm

Setting	Description	Factory Default
Enable/Disable	Clicking "Apply" button will only save the MSTP settings temporarily; you can select to enable this configuration to activate the MSTP settings during the operation.	Disabled

Explanation of "Instance Settings" Items

Instance ID

Setting	Description	Factory Default
Numerical value selected by user	Within each MST region, the MSTP maintains multiple spanning-tree instances. A common and internal spanning tree (CIST) is a collection of the following: ISTs in each MST region, and the common spanning tree (CST) that interconnects the MST regions, and a single spanning tree. All other MST instances are numbered from 1 to 16.	Cist

Vlan Mapping

Setting	Description	Factory Default
Numerical value input by user (1-4094)	Configure which VLAN ID is mapped to the multiple spanning-tree instances.	None

ridge priority

Setting	Description	Factory Default
Numerical value selected by user	Increase this device's bridge priority by selecting a lower number. A device with a higher bridge priority has a greater chance of being established as the root of the Spanning Tree topology.	32768

Enable

Setting	Description	Factory Default
Enable/Disable	Select to enable the port as a node on the Multiple Spanning Tree topology.	Disabled

Priority

Setting	Description	Factory Default
Numerical value selected by user	Increase this port's priority as a node on the Multiple Spanning Tree topology by entering a lower number.	128

Cost

Setting	Description	Factory Default
Numerical value input by user	Input a higher cost to indicate that this port is less suitable as a node for the Multiple Spanning Tree topology. Use the default value (0) to use port speed in the auto port cost.	0

Oper Cost

It indicates the cost of the path to the other bridge from this transmitting bridge at the specified port.

Edge

Setting	Description	Factory Default
Enable/Disable	Select to enable the port as the edge port for the Multiple Spanning Tree topology.	Disabled

PDU Guard

Setting	Description	Factory Default
BPDU Guard	Unchecked: Disable BPDU Guard	Unchecked
	Checked: Enable BPDU Guard	

BPDU Guard is a protection mechanism that prevents looping caused from misconnection or wrong setting of edge ports. Edge ports aren't supposed to connect to devices that are capable of sending BPDUs. 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. By default, this function is disabled.

PDU Filter

Setting	Description	Factory Default
BPDU Filter	Unchecked: Disable BPDU Filter	Unchecked
	Checked: Enable BPDU Filter	

BPDU filter prevents a port from sending and processing BPDUs. A BPDU filter enabled port cannot transmit any BPDUs and will drop all received BPDUs. If edge port is disabled, BPDU filter cannot be enabled on this port. By default, this function is disabled.

State

Indicates the current Multiple Spanning Tree status of this port. The "Blocking" status indicates the transmission is blocked; the "Learning" status indicates the MAC address of the device is being recorded in the MAC table, and the "Forwarding" status indicates normal transmission.

Role

Indicates the current port role status.

Setting	Port Role Status	Factory Default
Port Role	Backup Alternate port Root port Designated port Disable	None

Configuration Limits of STP/RSTP

The Spanning Tree Algorithm places limits on three of the configuration items described previously: [Eq. 1]: 1 sec ≤ Hello Time ≤ 10 sec

[Eq. 2]: 6 sec ≤ Max. Age ≤ 40 sec

[Eq. 3]: 4 sec ≤ Forwarding Delay ≤ 30 sec

These three variables are further restricted by the following two inequalities:

[Eq. 4]: 2 x (Hello Time + 1 sec) ≤ Max. Age ≤ 2 x (Forwarding Delay – 1 sec)

Moxa PT-G7728/G7828's firmware will alert you immediately if any of these restrictions are violated. For example, setting

Hello Time = 5 sec, Max. Age = 20 sec, and Forwarding Delay = 4 sec does not violate Eqs. 1 through 3, but does violate Eq. 4, since in this case,

2 x (Hello Time + 1 sec) = 12 sec, and 2 x (Forwarding Delay – 1 sec) = 6 sec.

You can remedy the situation in many ways. One solution is simply to increase the Forwarding Delay value to at least 11 sec.

HINT: Perform the following steps to avoid guessing:

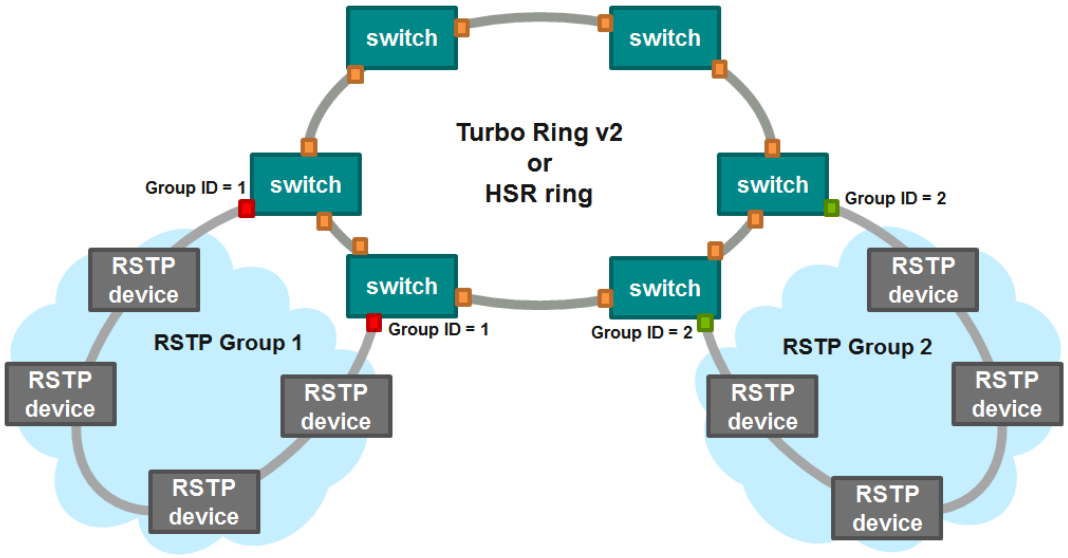
Step 1: Assign a value to **Hello Time** and then calculate the left most part of Eq. 4 to get the lower limit of **Max. Age**.

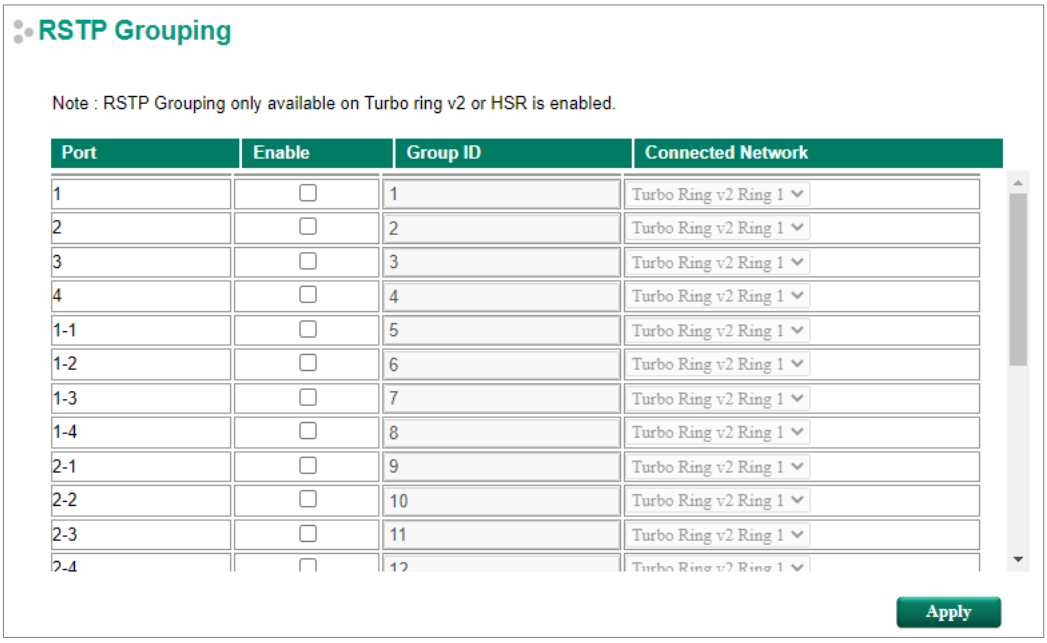
Step 2: Assign a value to **Forwarding Delay** and then calculate the right most part of Eq. 4 to get the upper limit for **Max. Age**.

Step 3: Assign a value to **Forwarding Delay** that satisfies the conditions.

RSTP Grouping

The purpose of RSTP grouping is to fulfil the legacy requirement of IEDs or PLCs that utilize RSTP to communicate with each other through the IEC 62439-3 HSR network or Moxa's proprietary architecture – Turbo Ring v2. As there is a max hops limitation when using RSTP, the quality of the devices that use RSTP is also limited. By grouping RSTP devices via assigning "RSTP Group ID", the total number of RSTP devices that are connected to Turbo Ring v2 or HSR can be extended.





Enable RSTP Grouping

Setting	Description	Factory Default
Enable/Disable RSTP Grouping of selected port	Enable or disable RSTP Grouping of selected port	Disable

Group ID

Setting	Description	Factory Default
1 to 4094	The RSTP Group ID	As port number

Connected Network

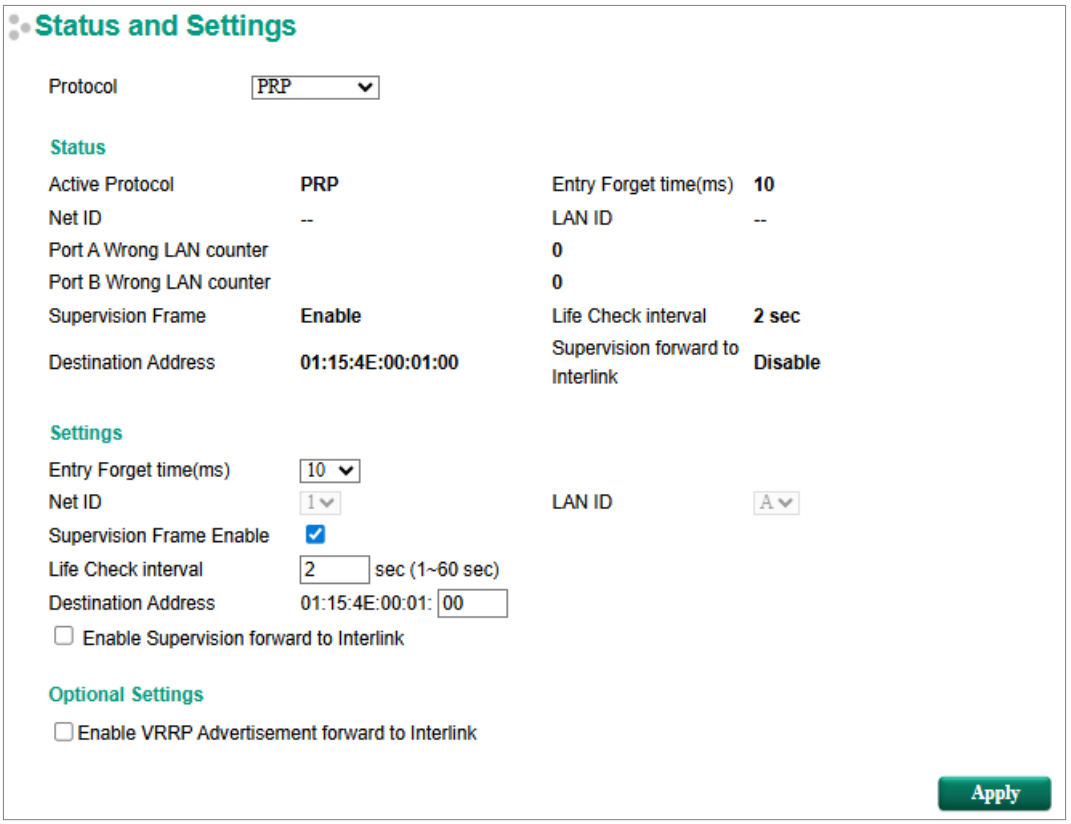
Setting	Description	Factory Default
Turbo Ring v2 Ring 1, Turbo Ring v2 Ring 2, HSR	Select the connected network of the RSTP Grouping.	Turbo Ring v2 Ring 1

IEC 62439-3 Protocol

The PT-G7728 Series supports three redundant protocols: PRP, HSR, and Coupling. Depending on the topology of your network, you can choose one of these redundancy protocols. All three protocols support a 0 ms recovery time.

- PRP: Copies of each packet are sent from the source to the destination via two LANs.
- HSR: Copies of each packet are sent from the source to the destination via an HSR ring.
- Coupling: Coupling is used to connect PRP and HSR.

Status and Settings



Protocol

Setting	Description	Factory Default
PRP/HSR/COUPLING	Select redundancy protocol	PRP

Status

Indicates the current IEC 62439-3 protocol status.

Settings

Entry Forget time (ms)

Setting	Description	Factory Default
10/100	Select 100 (ms) for 100M, and 10 (ms) for 1000M. This is the maximum time an entry may reside in the duplicate table.	10

NET ID

Setting	Description	Factory Default
1 to 7	Allows the user to set a Net ID, ranging from 1 to 7 (Coupling mode only).	1

LAN ID

Setting	Description	Factory Default
A/B	Allows the user to set a LAN ID (Coupling mode only).	A

Supervision Frame Enable

Setting	Description	Factory Default
Checked/Unchecked	Enable or disable the supervision Frame feature globally.	Checked

Life Check Interval

Setting	Description	Factory Default
1 to 60	Allows the user to set a Life Check Interval, ranging from 1 to 60 seconds. (Only available when the Supervision Frame feature is enabled). This is the typical interval between two successive supervision frames.	2

Destination Address

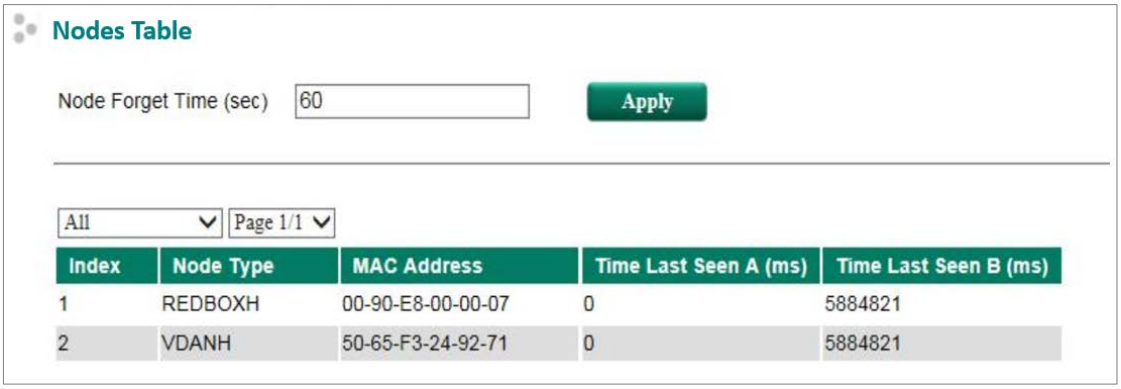
Setting	Description	Factory Default
00 to FF (Hex.)	Allows users to set the Bridge Multicast Address by the forwardable multicast address.	00

Enable Supervision forward to Interlink

Setting	Description	Factory Default
Checked/Unchecked	Forwards PRP_Supervision frames on the PRP network on behalf of the DANH devices in the HSR ring. (only when Coupling mode is enabled)	Unchecked
Checked/Unchecked	Forward VRRP advertisement to the interlink port	Unchecked

Nodes Table

The nodes table displays the current supervision frames that were received. On this page, users can view the supervision frame information by Node Type.



Node Forget Time (sec)

Setting	Description	Factory Default
60 to 120	Allows users to set a Node Forget Time, ranging from 60 to 120 seconds. The time after which a node entry is cleared from the Nodes Table after the frames from this node cease to be received.	60

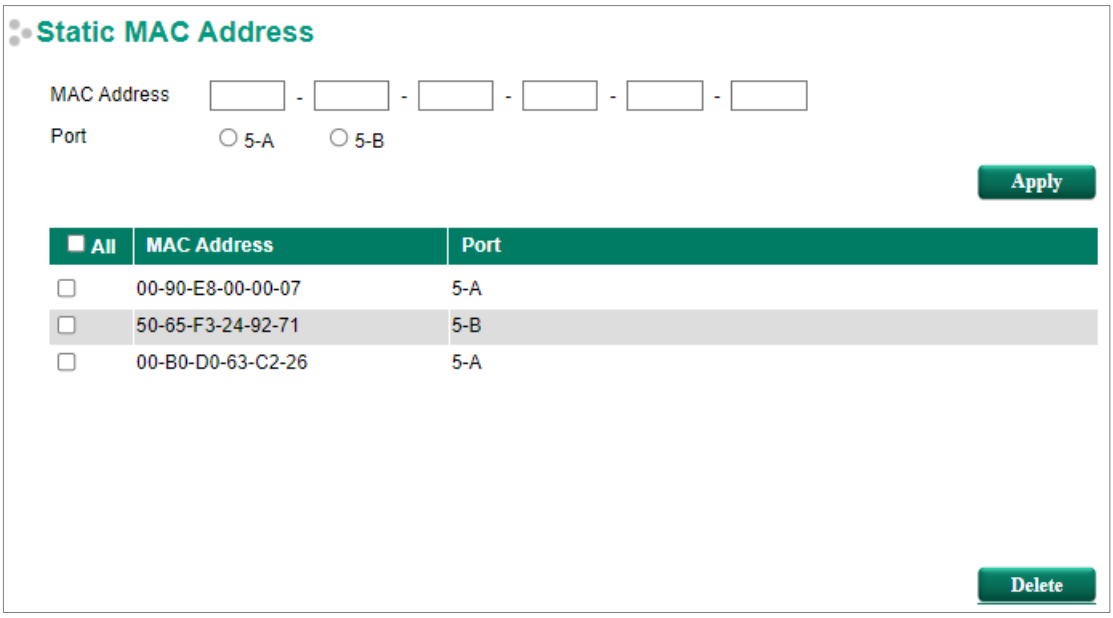
The information shown in the table includes:

- Index: The PT-G7728 Series supports a maximum of 1024 entries in the node table.
- Node Type: Display Node types DANP/RedboxP/VDANP/DANH/RedboxH/VDANH according to IEC 62439-3.
- MAC Address: Display the MAC address of the node.
- Time Last Seen A (ms): The time the packets were received from LAN A.
- Time Last Seen B (ms): The time the packets were received from LAN B.
  The time the packets were received from LAN A and LAN B should be the same or very close in a normally functioning network. The increasing difference may be due to packets being dropped in one of the LANs and may require further troubleshooting.

Static MAC

To avoid duplication of packets on SANs (Single Attached Nodes), the switch keeps track of the learned MAC addresses in the nodes table, identifies the device as attached to only one LAN, then sends the frame to only that LAN without the PRP trailer.

E.g., If one SAN pings another device on LAN A, all devices on LAN B receive the ICMP frames if PRP is implemented. This results in a "unicast flood" on LAN B. The **Static MAC** function provides users setting the unicast MAC address a way to specify which packet with the address should only be sent to LAN A or LAN B.



MAC Address

Setting	Description	Factory Default
Integer	Type the unicast MAC address in the MAC Address field to specify a static address. One static MAC Address supports up to a maximum of 16 unicast MAC addresses. NOTE: **Static MAC** is only supported in PRP mode.	None

Port

Setting	Description	Factory Default
Select/Deselect	Select the appropriate checkboxes to define the port for this unicast MAC address. 5-A: LAN A 5-B: LAN B	None

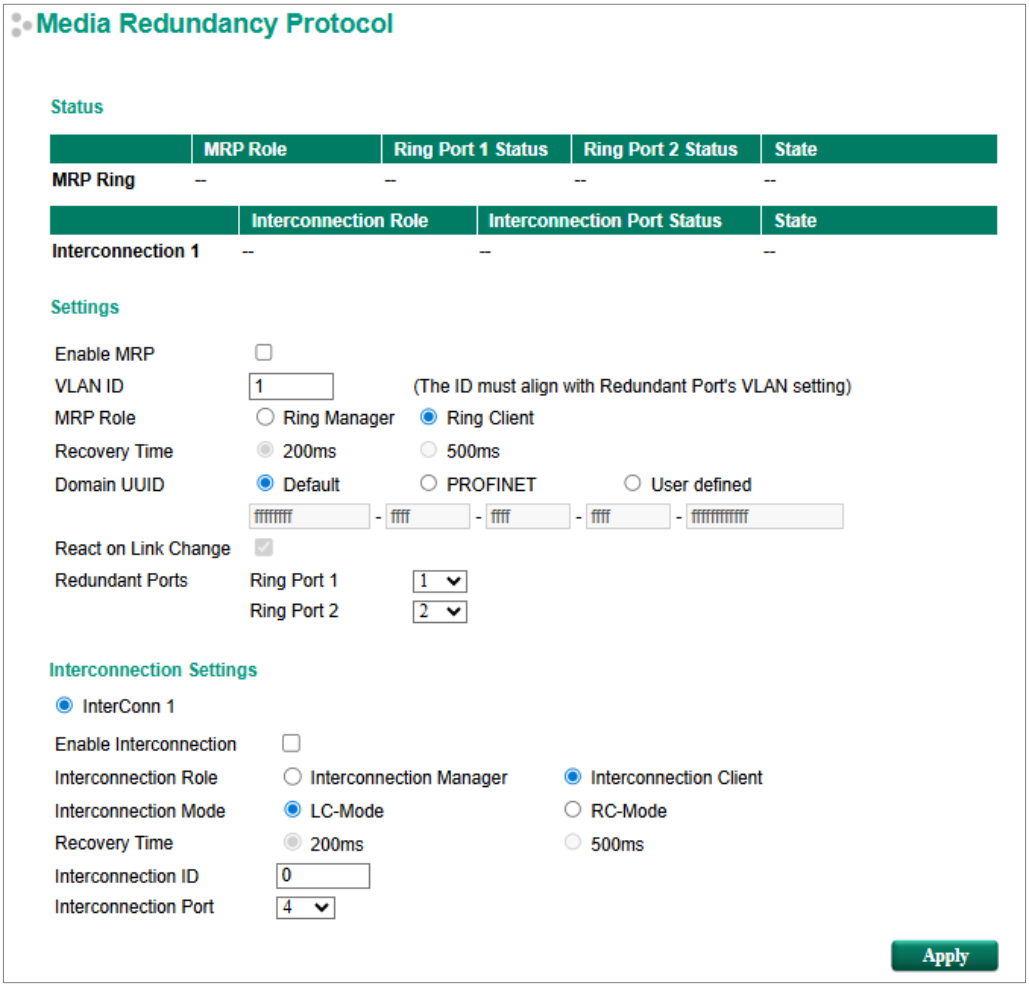
NOTE

The **Static MAC** function is compatible with the FPGA firmware version 2.0 and above. Additional information on the FPGA can be found by:

- Clicking the Home Page link to check the M-5 FPGA version information
- Downloading the latest FPGA firmware (*.rom) file from Moxa's website (www.moxa.com)
- Referring to the "FPGA Upgrade" section in this UM

Media Redundancy Protocol

The Media Redundancy Protocol (MRP) is a protocol that lets you set up high-availability, ring shaped network structures. An MRP ring with a Moxa switch is made up of up to 50 devices that support the MRP protocol according to IEC 62439-2.



Status

The table displays the current Media Redundancy Protocol (MRP) status.

Settings

Enable MRP

Setting	Description	Factory Default
Checked/Unchecked	Enable or disable the MRP feature globally	Unchecked

VLAN ID

Setting	Description	Factory Default
1 to 1049	This optional attribute may be used by the MRP object and specifies its VLAN identifier in the redundancy domain.	1

MRP Role

Setting	Description	Factory Default
Ring Manager Ring Client	Allow user defines MRP role. The Ring Manger represents Media Redundancy Manager (MRM). The Ring Client represents Media Redundancy Client (MRC).	Ring Client

Domain UUID

Setting	Description	Factory Default
Default ProfiNet (Siemens)	This key attribute defines the redundancy domain representing the ring the MRP object belongs to. It is set to default Domain ID or provided as a unique ID by the engineering team.	Default

React on Link Change

Setting	Description	Factory Default
Checked/Unchecked	This optional attribute specifies whether the MRM reacts immediately on MRP_LinkChange frames or not. (Ring Manager Only)	Checked

Redundant Ports 1st Port

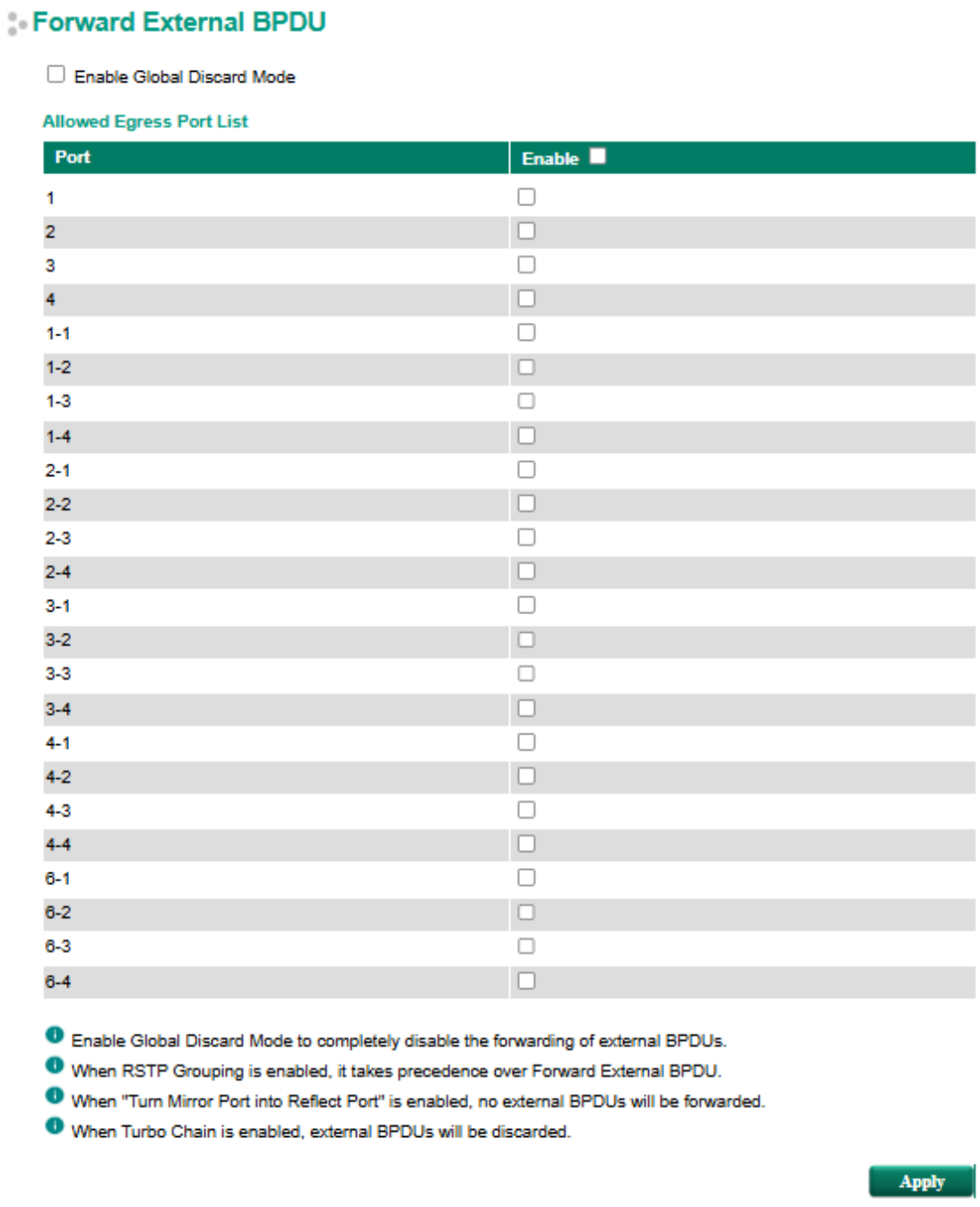
Setting	Description	Factory Default
1 to 28	This attribute specifies one port of a switch that is assigned as ring port 1 in the redundancy domain referenced by the value of the attribute Domain ID.	1

Redundant Ports 2nd Port

Setting	Description	Factory Default
1 to 28	This attribute specifies one port of a switch that is assigned as ring port 2 in the redundancy domain referenced by the value of the attribute Domain ID.	2

Forward External BPDU

The Forward External BPDU feature allows the switch to forward Bridge Protocol Data Units (BPDUs) received from external sources to specified egress ports. Users have the flexibility to configure which ports will forward external BPDUs.



Behavior of Forward External BPDU Enabled/Disabled

Active Redundancy Protocol	Ingress Port Protocol Status/ Role	Forward External BPDU			
		Enabled		Disabled	
		Untagged BPDU	Tagged BPDU	Untagged BPDU	Tagged BPDU
Factory Default	N/A	Forwarded	Forwarded w/ VLAN	Discarded	Discarded
MSTP	Enabled	Processed		Processed	
	Disabled	Discarded		Discarded	
RSTP	Enabled	Processed		Processed	
	Disabled	Discarded		Discarded	
MRP	N/A	Forwarded		Discarded	
	Ring Port/ Interconnection Port				
Turbo Ring V2	N/A	Forwarded		Discarded	
	Ring Port/ Dual Homing Port/ Coupling Port				
Turbo Chain	N/A	Discarded	Discarded	Discarded	
	Head/Member/Tail				

Multicast

Multicast filtering improves the performance of networks that carry multicast traffic. This section explains multicasts, multicast filtering, and how multicast filtering can be implemented on your Moxa switch.

The Concept of Multicast Filtering

What is an IP Multicast?

A multicast is a packet sent by one host to multiple hosts. Only those hosts that belong to a specific multicast group will receive the multicast. If the network is set up correctly, a multicast can only be sent to an end-station or a subset of end-stations on a LAN or VLAN that belong to the multicast group. Multicast group members can be distributed across multiple subnets, so that multicast transmissions can occur within a campus LAN or over a WAN. In addition, networks that support IP multicast send only one copy of the desired information across the network until the delivery path that reaches group members diverges. To make more efficient use of network bandwidth, it is only at these points that multicast packets are duplicated and forwarded. A multicast packet has a multicast group address in the destination address field of the packet's IP header.

Benefits of Multicast

The benefits of using IP multicast are:

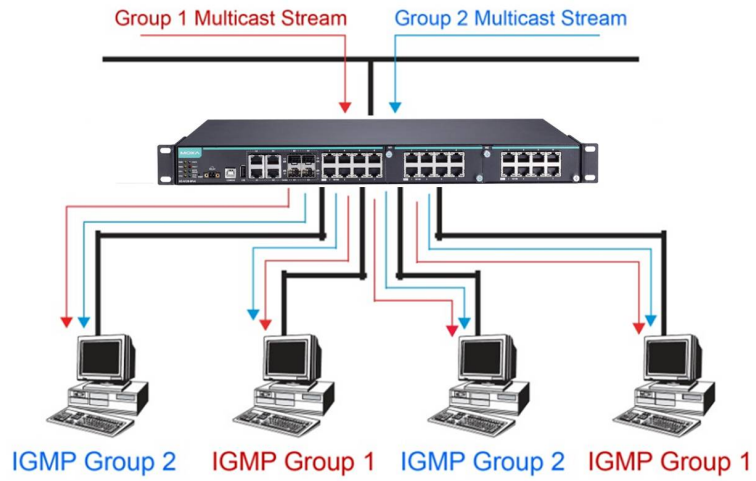
- It uses the most efficient, sensible method to deliver the same information to many receivers with only one transmission.
- It reduces the load on the source (for example, a server) since it will not need to produce several copies of the same data.
- It makes efficient use of network bandwidth and scales well as the number of multicast group members increases.
- Works with other IP protocols and services, such as Quality of Service (QoS).

Multicast transmission makes more sense and is more efficient than unicast transmission for some applications. For example, multicasts are often used for videoconferencing, since high volumes of traffic must be sent to several end-stations at the same time, but where broadcasting the traffic to all end-stations would cause a substantial reduction in network performance. Furthermore, several industrial automation protocols, such as Allen-Bradley, EtherNet/IP, Siemens Profibus, and Foundation Fieldbus HSE (High Speed Ethernet), use multicast. These industrial Ethernet protocols use publisher/subscriber communications models by multicasting packets that could flood a network with heavy traffic. IGMP Snooping is used to prune multicast traffic so that it travels only to those end destinations that require the traffic, reducing the amount of traffic on the Ethernet LAN.

Multicast Filtering

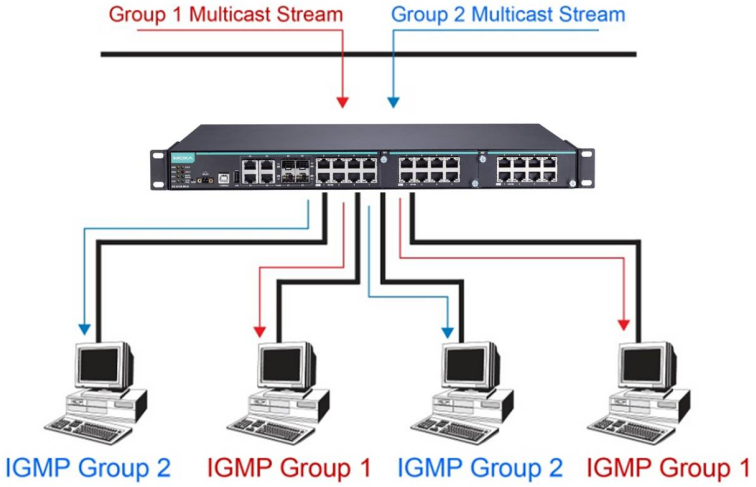
Multicast filtering ensures that only end-stations that have joined certain groups receive multicast traffic. With multicast filtering, network devices only forward multicast traffic to the ports that are connected to registered end-stations. The following two figures illustrate how a network behaves without multicast filtering, and with multicast filtering.

Network without multicast filtering



All hosts receive the multicast traffic, even if they don't need it.

Network with multicast filtering



Hosts only receive dedicated traffic from other hosts belonging to the same group.

Multicast Filtering and Moxa's Industrial Rackmount Switches

There are three ways to achieve multicast filtering with a Moxa switch: IGMP (Internet Group Management Protocol) Snooping, GMRP (GARP Multicast Registration Protocol), and adding a static multicast MAC manually to filter multicast traffic automatically.

Snooping Mode

Snooping Mode allows your switch to forward multicast packets only to the appropriate ports. The switch **snoops** on exchanges between hosts and an IGMP device, such as a router, to find those ports that want to join a multicast group, and then configures its filters accordingly.

Query Mode

Query mode allows the Moxa switch to work as the Querier if it has the lowest IP address on the subnetwork to which it belongs.

NOTE

IGMP Snooping Enhanced mode is only provided in Layer 2 switches.

IGMP querying is enabled by default on the Moxa switch to ensure that query election is activated. Enable query mode to run multicast sessions on a network that does not contain IGMP routers (or queriers). Query mode allows users to enable IGMP snooping by VLAN ID. Moxa switches support IGMP snooping version 1, version 2, and version 3. Version 2 is compatible with version 1.The default setting is IGMP V1/V2.

NOTE

Moxa Layer 3 switches are compatible with any device that conforms to the IGMP v2 and IGMP v3 device protocols. Layer 2 switches only support IGMP v1/v2.

IGMP Multicast Filtering

IGMP is used by IP-supporting network devices to register hosts with multicast groups. It can be used on all LANs and VLANs that contain a multicast capable IP router, and on other network devices that support multicast filtering. Moxa switches support IGMP version 1, 2 and 3. IGMP version 1 and 2 work as follows:

- The IP router (or querier) periodically sends query packets to all end-stations on the LANs or VLANs that are connected to it. For networks with more than one IP router, the router with the lowest IP address is the querier. A switch with IP address lower than the IP address of any other IGMP queriers connected to the LAN or VLAN can become the IGMP querier.
- When an IP host receives a query packet, it sends a report packet back that identifies the multicast group that the end-station would like to join.
- When the report packet arrives at a port on a switch with IGMP Snooping enabled, the switch knows that the port should forward traffic for the multicast group, and then proceeds to forward the packet to the router.
- When the router receives the report packet, it registers that the LAN or VLAN requires traffic for the multicast groups.
- When the router forwards traffic for the multicast group to the LAN or VLAN, the switches only forward the traffic to ports that received a report packet.

IGMP version 3 supports "source filtering," which allows the system to define how to treat packets from specified source addresses. The system can either white-list or black-list specified sources.

IGMP version comparison

IGMP Version	Main Features	Reference
V1	Periodic query	RFC-1112
V2	Compatible with V1 and adds: 1. Group-specific query 2. Leave group messages 3. Resends specific queries to verify leave message was the last one in the group 4. Querier election	RFC-2236
V3	Compatible with V1, V2, and adds: Source filtering • accept multicast traffic from specified source • accept multicast traffic from any source except the specified source	RFC-3376

GMRP (GARP Multicast Registration Protocol)

Moxa switches support IEEE 802.1D-1998 GMRP (GARP Multicast Registration Protocol), which is different from IGMP (Internet Group Management Protocol). GMRP is a MAC-based multicast management protocol, whereas IGMP is IP-based. GMRP provides a mechanism that allows bridges and end stations to register or de-register Group membership information dynamically. GMRP functions similarly to GVRP, except that GMRP registers multicast addresses on ports. When a port receives a ***GMRP-join*** message, it will register the multicast address to its database if the multicast address is not registered, and all the multicast packets with that multicast address are able to be forwarded from this port. When a port receives a ***GMRP-leave*** message, it will de-register the multicast address from its database, and all the multicast packets with this multicast address will not be able to be forwarded from this port.

Static Multicast MAC

Some devices may only support multicast packets, but not support either IGMP Snooping or GMRP. The Moxa switch supports adding multicast groups manually to enable multicast filtering.

Enabling Multicast Filtering

Use the serial console or web interface to enable or disable IGMP Snooping and IGMP querying. If IGMP Snooping is not enabled, then IP multicast traffic is always forwarded, flooding the network.

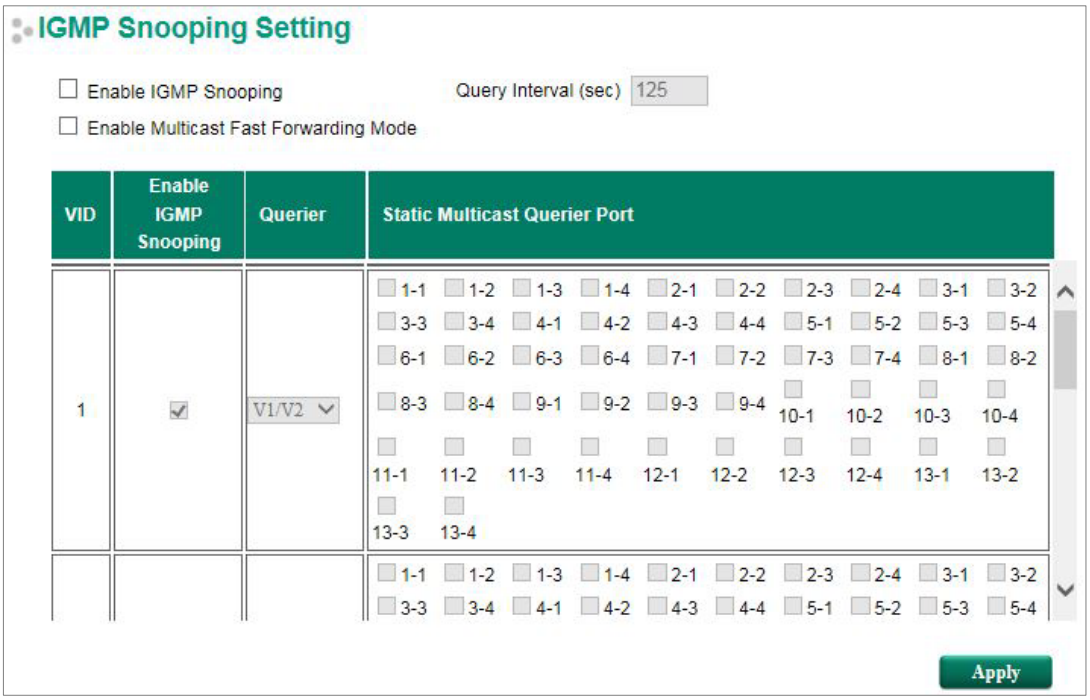
IGMP Snooping

IGMP Snooping provides the ability to prune multicast traffic so that it travels only to those end destinations that require that traffic, thereby reducing the amount of traffic on the Ethernet LAN.

NOTE

IGMP Snooping will be disabled when Port-based VLAN is enabled.

IGMP Snooping Setting



Enable IGMP Snooping (Global)

Setting	Description	Factory Default
Enable/Disable	Select the Enable IGMP Snooping checkbox near the top of the window to enable the IGMP Snooping function globally.	Disabled

Query Interval (sec)

Setting	Description	Factory Default
Numerical value, input by the user	Sets the query interval of the Querier function globally. Valid settings are from 20 to 600 seconds.	125 seconds

Enable Multicast Fast Forwarding Mode

Setting	Description	Factory Default
Enable/Disable	Select the Enable Multicast Fast Forwarding Mode checkbox to achieve fast multicast forwarding path re-learning while the ring redundant network is down. Note: Turbo Ring V2 or Turbo Chain must be enabled.	Disabled

Enable IGMP Snooping

Setting	Description	Factory Default
Enable/Disable	Enables or disables the IGMP Snooping function on that particular VLAN.	Enabled if IGMP Snooping is enabled globally

Querier

Setting	Description	Factory Default
Disable	Disables the Moxa switch's querier function.	V1/V2
V1/V2 and V3 checkbox	V1/V2: Enables the switch to send IGMP snooping version 1 and 2 queries V3: Enables the switch to send IGMP snooping version 3 queries	

Static Multicast Querier Port

Setting	Description	Factory Default
Select/Deselect	Select the ports that will connect to the multicast routers. These ports will receive all multicast packets from the source. This option is only active when IGMP Snooping is enabled.	Disabled

NOTE

If a router or layer 3 switch is connected to the network, it will act as the Querier, and consequently this Querier option will be disabled on all Moxa layer 2 switches.

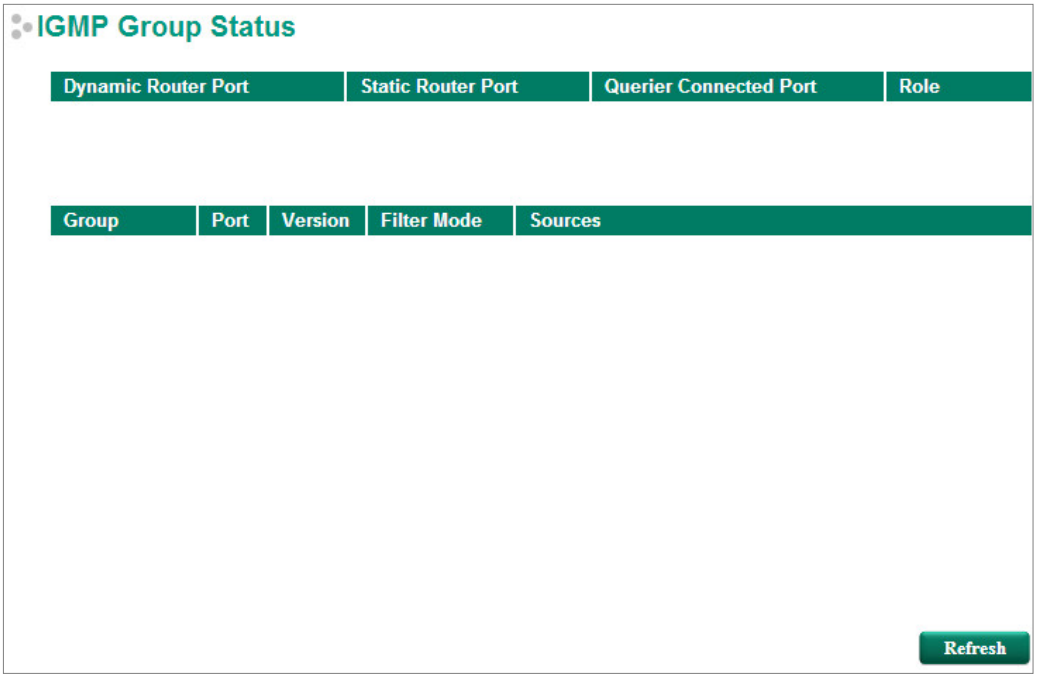
If all switches on the network are Moxa layer 2 switches, then only one layer 2 switch will act as Querier.

NOTE

Multicast Fast Forwarding Mode is one function of V-ON technology that should be enabled in layer 2 and layer 3 switches. For details, refer to *Moxa Managed Ethernet Switch Redundancy Protocol (UI 2.0) Users Manual*.

IGMP Group Status

The Moxa switch displays the current active IGMP groups that were detected. On this page, you can view IGMP group settings by VLAN ID.

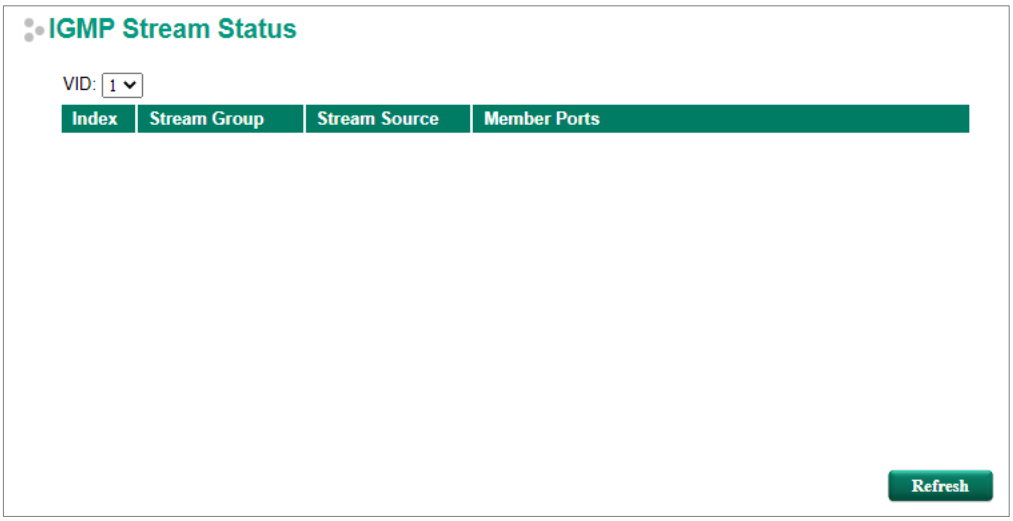


The information shown in the table includes:

- Dynamic Router Port: Indicates that a multicast router connects to or sends packets from these port(s).
- Static Router Port: Displays the static multicast querier port(s).
- Querier Connected Port: Displays the port that is connected to the querier.
- Role: Indicates if the switch is a querier. Displays Querier or Non-Querier.
- Group: Displays the multicast group addresses.
- Port: Displays the port that receives the multicast stream or the port the multicast stream is forwarded to.
- Version: Displays the IGMP Snooping version.
- Filter Mode: Indicates that the multicast source address is included or excluded. Displays Include or Exclude when IGMP v3 is enabled.
- Sources: Displays the multicast source address when IGMP v3 is enabled

Stream Table

This page displays the multicast stream forwarding status. Users can view the status by VLAN ID.



Stream Group: Multicast group IP address

Stream Source: Multicast source IP address

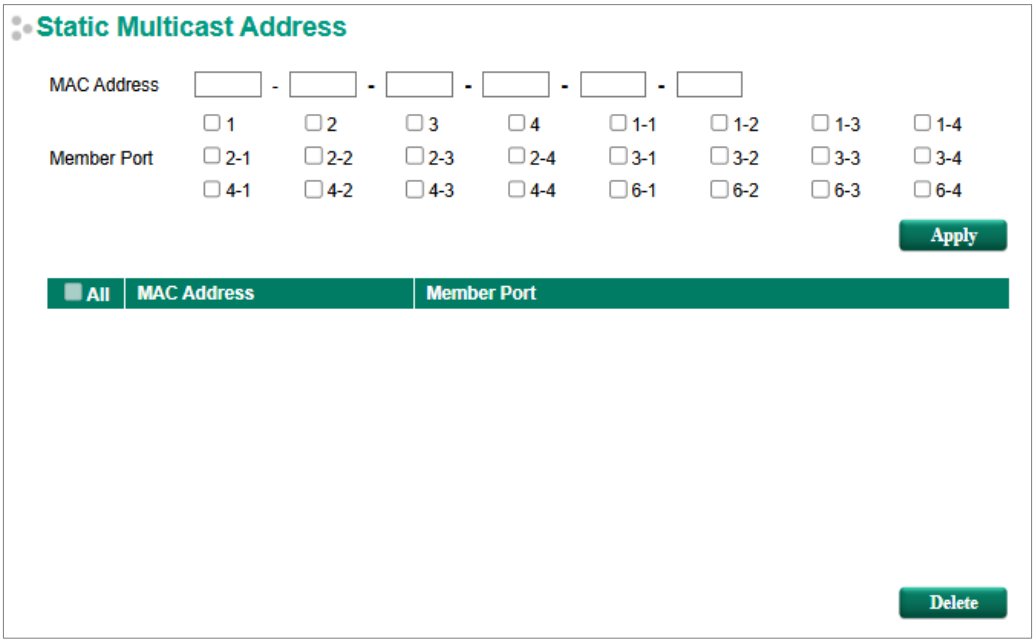
Port: The port that receives the multicast stream

Member Ports: Ports to which the multicast stream is forwarded

NOTE

IGMP Stream Status is only supported by Moxa's Layer 3 switches.

Static Multicast Address



NOTE

The MAC address (01:00:5E:XX:XX:XX) will appear on the Static Multicast Address page. Activate IGMP Snooping to implement automatic classification.

MAC Address

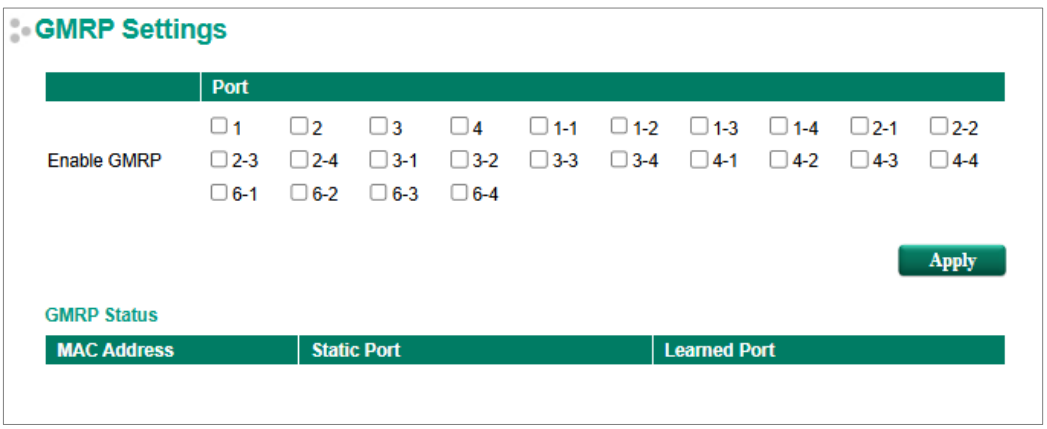
Setting	Description	Factory Default
Integer	Type the MAC address in the MAC Address field to specify a static multicast address.	None

Member Port

Setting	Description	Factory Default
Select/Deselect	Select the appropriate checkboxes to define the join ports for this multicast group.	None

GMRP

GMRP is a MAC-based multicast management protocol, whereas IGMP is IP-based. GMRP provides a mechanism that allows bridges and end stations to register or un-register Group membership information dynamically.



Enable GMRP

Setting	Description	Factory Default
Select/Deselect	Select the appropriate checkboxes to define which ports are to be GMRP enabled.	None

GMRP Status

The Moxa switch displays the current active GMRP groups that were detected.

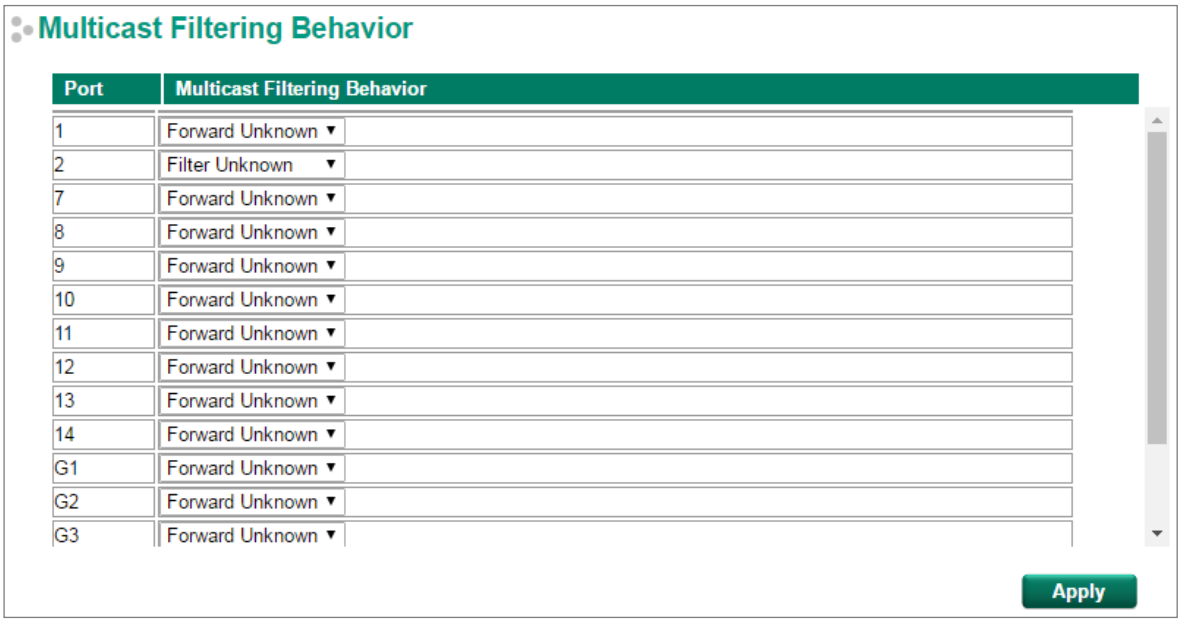
MAC Address: The Multicast MAC address

Static Port: This multicast address is defined by static multicast

Learned Port: This multicast address is learned by GMRP

Multicast Filtering Behavior

Multicast Filtering Behavior supports two options: **Forward Unknown** and **Filter Unknown**.



Behavior

Setting	Description	Factory Default
Forward Unknown	Allows the switch to forward all unknown Multicast streams	Forward Unknown
Filter Unknown	Allows the switch to drop all unknown Multicast steams	

QoS

The Moxa switch's traffic prioritization capability provides Quality of Service (QoS) to your network by making data delivery more reliable. You can prioritize traffic on your network to ensure that high priority data is transmitted with minimum delay. Traffic can be controlled by a set of rules to obtain the required Quality of Service for your network. The rules define different types of traffic and specify how each type should be treated as it passes through the switch. The Moxa switch can inspect both IEEE 802.1p/1Q layer 2 CoS tags, and even layer 3 TOS information to provide consistent classification of the entire network. The Moxa switch's QoS capability improves the performance and determinism of industrial networks for mission-critical applications.

The Traffic Prioritization Concept

Traffic prioritization allows you to prioritize data so that time-sensitive and system-critical data can be transferred smoothly and with minimal delay over a network. The benefits of using traffic prioritization are:

- Improve network performance by controlling a wide variety of traffic and by managing congestion.
- Assign priorities to different categories of traffic. For example, set higher priorities for time-critical or business-critical applications.
- Provide predictable throughput for multimedia applications, such as video conferencing or voice over IP, and minimize traffic delay and jitter.
- Improve network performance as the amount of traffic grows. Doing so will reduce costs since it will not be necessary to keep adding bandwidth to the network.

Traffic prioritization uses the four traffic queues that are present in your Moxa switch to ensure that high priority traffic is forwarded on a different queue from lower priority traffic. Traffic prioritization provides Quality of Service (QoS) to your network.

Moxa switch traffic prioritization depends on two industry-standard methods:

- **IEEE 802.1D**—a layer 2 marking scheme.
- **Differentiated Services (DiffServ)**—a layer 3 marking scheme.

IEEE 802.1D Traffic Marking

The IEEE Std 802.1D, 1998 Edition marking scheme, which is an enhancement to IEEE Std 802.1D, enables Quality of Service on the 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. The 4-byte tag immediately follows the destination MAC address and Source MAC address.

The IEEE Std 802.1D, 1998 Edition priority marking scheme assigns an IEEE 802.1p priority level between 0 and 7 to each frame. The priority marking scheme determines the level of service that this type of traffic should receive. Refer to the following table for an example of how different traffic types can be mapped to the eight IEEE 802.1p priority levels.

IEEE 802.1p Priority Level	IEEE 802.1D Traffic Type
0	Best Effort (default)
1	Background
2	Standard (spare)
3	Excellent Effort (business critical)
4	Controlled Load (streaming multimedia)
5	Video (interactive media); less than 100 milliseconds of latency and jitter
6	Voice (interactive voice); less than 10 milliseconds of latency and jitter
7	Network Control Reserved traffic

Even though the IEEE 802.1D 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 on a LAN and not across routed WAN links, since the IEEE 802.1Q tags are removed when the packets pass through a router.

Differentiated Services (DiffServ) Traffic Marking

DiffServ is a Layer 3 marking scheme that uses the DiffServ Code Point (DSCP) field in the IP header to store the packet priority information. DSCP is an advanced intelligent method of traffic marking that allows you to choose how your network prioritizes different types of traffic. DSCP uses 64 values that map to user-defined service levels, allowing you to establish more control over network traffic.

The advantages of DiffServ over IEEE 802.1D are:

- You can configure how you want your switch to treat selected applications and types of traffic by assigning various grades of network service to them.
- No extra tags are required in the packet.
- DSCP uses the IP header of a packet to preserve priority across the Internet.
- DSCP is backwards compatible with IPV4 TOS, which allows operation with existing devices that use a layer 3 TOS enabled prioritization scheme.

Traffic Prioritization

Moxa switches classify traffic based on layer 2 of the OSI 7-layer model, and the switch prioritizes received traffic according to the priority information defined in the received packet. Incoming traffic is classified based upon the IEEE 802.1D frame and is assigned to the appropriate priority queue based on the IEEE 802.1p service level value defined in that packet. Service level markings (values) are defined in the IEEE 802.1Q 4-byte tag, and consequently traffic will only contain 802.1p priority markings if the network is configured with VLANs and VLAN tagging. The traffic flow through the switch is as follows:

- A packet received by the Moxa switch may or may not have an 802.1p tag associated with it. If it does not, then it is given a default 802.1p tag (which is usually 0). Alternatively, the packet may be marked with a new 802.1p value, which will result in all knowledge of the old 802.1p tag being lost.
- Because the 802.1p priority levels are fixed to the traffic queues, the packet will be placed in the appropriate priority queue, ready for transmission through the appropriate egress port. When the packet reaches the head of its queue and is about to be transmitted, the device determines whether or not the egress port is tagged for that VLAN. If it is, then the new 802.1p tag is used in the extended 802.1D header.
- The Moxa switch will check a packet received at the ingress port for IEEE 802.1D traffic classification, and then prioritize it based on the IEEE 802.1p value (service levels) in that tag. It is this 802.1p value that determines which traffic queue the packet is mapped to.

Traffic Queues

The hardware of Moxa switches has multiple traffic queues that allow packet prioritization to occur. Higher priority traffic can pass through the Moxa switch without being delayed by lower priority traffic. As each packet arrives in the Moxa switch, it passes through any ingress processing (which includes classification, marking/re-marking), and is then sorted into the appropriate queue. The switch then forwards packets from each queue.

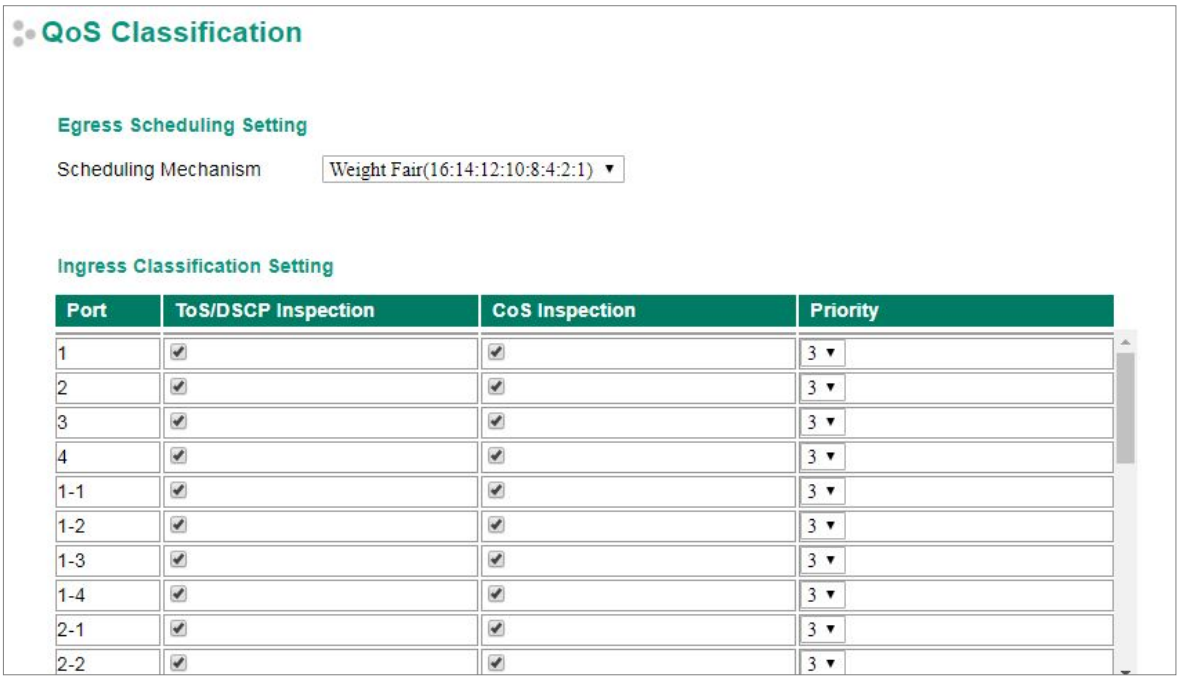
Moxa switches support three different queuing mechanisms:

- **Weight Fair:** This method services all the traffic queues, giving priority to the higher priority queues. Under most circumstances, the Weight Fair method gives high priority precedence over low priority, but in the event that high priority traffic does not reach the link capacity, lower priority traffic is not blocked.
- **Strict:** This method services high traffic queues first; low priority queues are delayed until no more high priority data needs to be sent. The Strict method always gives precedence to high priority over low priority.
- **Weighted Round Robin:** This method allows users to give priority to specific packets in the higher weighted queue to ensure those packets will be sent first. Queued packets will be forwarded based on their associated weight.

Configuring Traffic Prioritization

Quality of Service (QoS) provides a traffic prioritization capability to ensure that important data is delivered consistently and predictably. The Moxa switch can inspect IEEE 802.1p/1Q layer 2 CoS tags, and even layer 3 TOS information, to provide a consistent classification of the entire network. The Moxa switch's QoS capability improves your industrial network's performance and determinism for mission critical applications.

CoS Classification



Scheduling Mechanism

Setting	Description	Factory Default
Weight Fair	The Moxa switch has 8 priority queues. In the weight fair scheme, a 16, 14, 12, 10, 8, 4, 2, 1 weighting is applied to the four priorities. This approach prevents the lower priority frames from being starved of opportunity for transmission with only a slight delay to the higher priority frames.	Weight Fair
Strict	In the Strict-priority scheme, all top-priority frames egress a port until that priority's frames egress. This approach can cause the lower priorities to be starved of opportunity for transmitting frames but ensures that all high priority frames will egress the switch as soon as possible.	
1 Strict, 7 Weighted Fair	• Strict Priority: The highest priority queue (queue 1) is always serviced first. This ensures that critical or time-sensitive traffic is transmitted will egress the switch as soon as possible. • Weighted Fair Queuing: The remaining seven queues (queues 2 to 8) are serviced based on their assigned weights. Each queue receives a proportion of the available bandwidth according to its weight, ensuring fair distribution of resources among different traffic classes.	

Setting	Description	Factory Default
2 Strict, 6 Weighted Fair	• Strict Priority: The highest priority queues (queue 1 and 2) are always serviced first. This ensures that critical or time-sensitive traffic is transmitted will egress the switch as soon as possible. • Weighted Fair Queuing: The remaining seven queues (queues 3 to 8) are serviced based on their assigned weights. Each queue receives a proportion of the available bandwidth according to its weight, ensuring fair distribution of resources among different traffic classes.	
3 Strict, 5 Weighted Fair	• Strict Priority: The highest priority queues (queue 1, 2 and 3) are always serviced first. This ensures that critical or time-sensitive traffic is transmitted will egress the switch as soon as possible. • Weighted Fair Queuing: The remaining seven queues (queues 4 to 8) are serviced based on their assigned weights. Each queue receives a proportion of the available bandwidth according to its weight, ensuring fair distribution of resources among different traffic classes.	

TOS/DSCP Inspection

Setting	Description	Factory Default
Enable/Disable	Enables or disables the Moxa switch for inspecting Type of Server (TOS) bits in the IPV4 frame to determine the priority of each frame.	Enable

COS Inspection

Setting	Description	Factory Default
Enable/Disable	Enables or disables the Moxa switch for inspecting 802.1p COS tags in the MAC frame to determine the priority of each frame.	Enable

Priority

Setting	Description	Factory Default
0 to 7	The port priority has 8 priority queues: from 0 (lowest) to 7 (highest)	3

NOTE

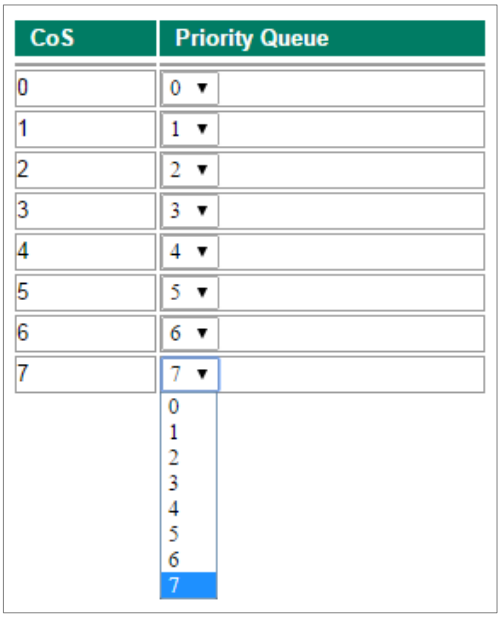
The priority of an ingress frame is determined in the following order:

1. ToS/DSCP Inspection
2. CoS Inspection
3. Priority

NOTE

The designer can enable these classifications individually or in combination. For instance, if a "hot" higher priority port is required for a network design, **TOS/DSCP Inspection** and **Cos Inspection** can be disabled. This setting leaves only port default priority active, which results in all ingress frames being assigned the same priority on that port.

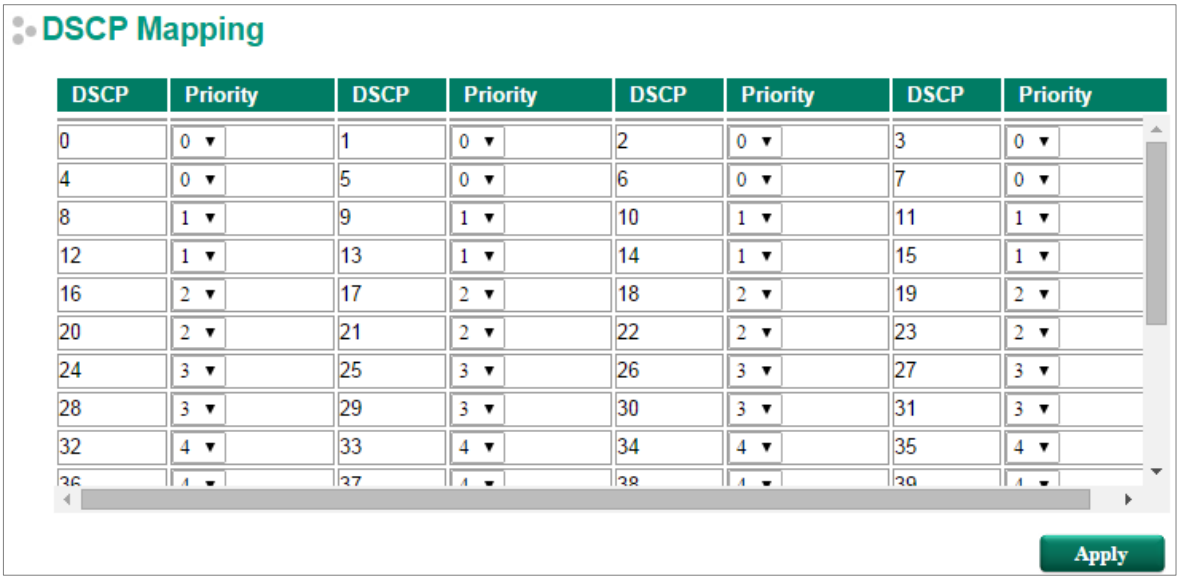
Priority Mapping



CoS Value and Priority Queues

Setting	Description	Factory Default
0 to 7	Maps different CoS values to 8 different egress queues.	CoS 0: 0 CoS 1: 1 CoS 2: 2 CoS 3: 3 CoS 4: 4 CoS 5: 5 CoS 6: 6 CoS 7: 7

DSCP Mapping



DSCP Value and Priority

Setting	Description	Factory Default
0 to 7	Different DSCP values map to one of 8 different priorities.	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

Rate Limiting

In general, one host should not be allowed to occupy unlimited bandwidth, particularly when the device malfunctions. For example, so-called "broadcast storms" could be caused by an incorrectly configured topology, or a malfunctioning device. Moxa industrial Ethernet switches not only prevent broadcast storms but can also be configured to a different ingress rate for all packets, giving administrators full control of their limited bandwidth to prevent undesirable effects caused by unpredictable faults.

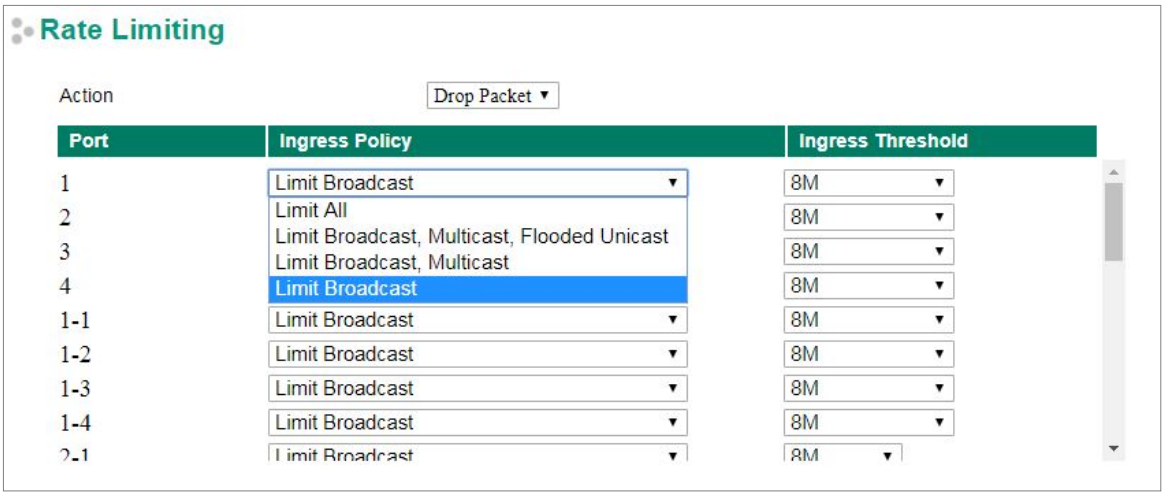
The **Control Mode** setting on the **Rate Limiting** page can be set to **Normal** or **Port Disable**.

Control Mode

Setting	Description	Factory Default
Normal	Set the max. ingress rate limit for different packet types	30 seconds
Port Disable	When the ingress multicast and broadcast packets exceed the ingress rate limit, the port will be disabled for a certain period. During this period, all packets from this port will be discarded.	Unlimited

Rate Limiting: Normal

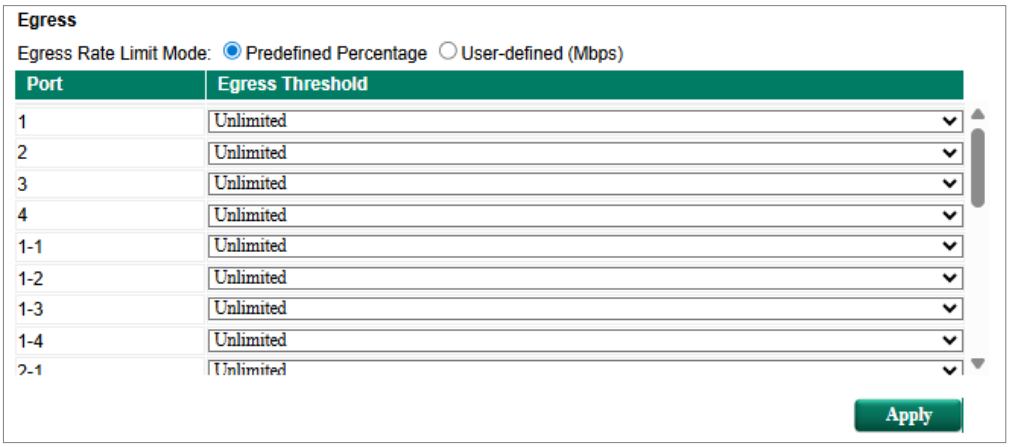
Ingress Rate Limit



Policy	Description	Factory Default
Limit All	Select the ingress rate limit for different packet types from the following options: Unlimited, 128K, 256K, 512K, 1M, 2M, 4M, 8M, 10%(100Mbps), 15%(150Mbps), 25%(250Mbps), 35%(350Mbps), 50%(500Mbps), 65%(650Mbps), 85%(850Mbps)	Limit Broadcast 8M
Limit Broadcast, Multicast, Flooded Unicast		
Limit Broadcast, Multicast		
Limit Broadcast		

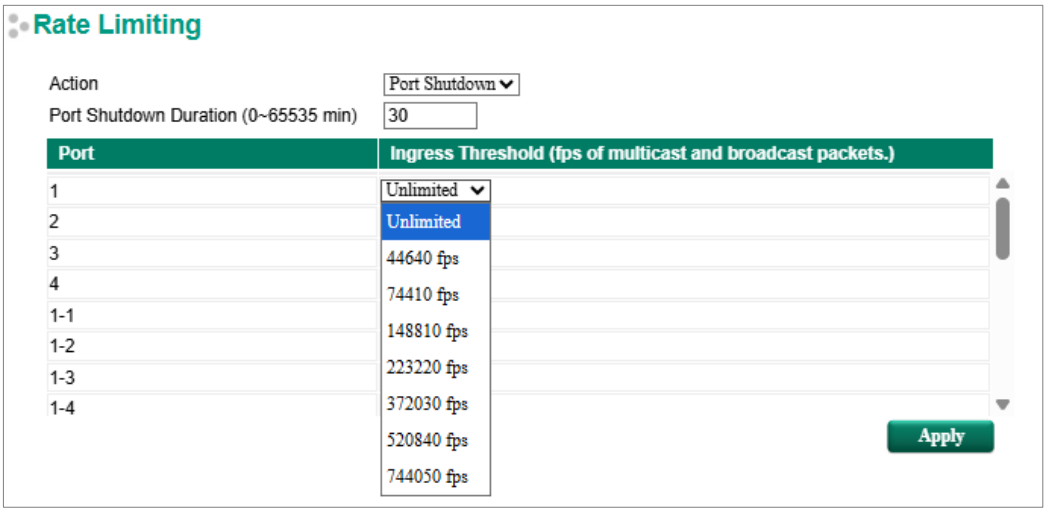
Egress Rate Limit

User can set the egress rate limit using predefined percentages or by specifying custom values in Mbps.



Egress Rate Limit Mode	Setting	Description
Predefined Percentage	Egress Rate	Select the egress rate limit (% of max. throughput) for all packets from the following options: Not Limited, 3%, 5%, 10%, 15%, 25%, 35%, 50%, 65%, 85%.
User-defined (Mbps)	Egress Rate	Input custom values in Mbps, providing flexibility in setting the rate limits. Decimal points are not accepted; only whole numbers are allowed.

Rate Limiting: Port Shutdown

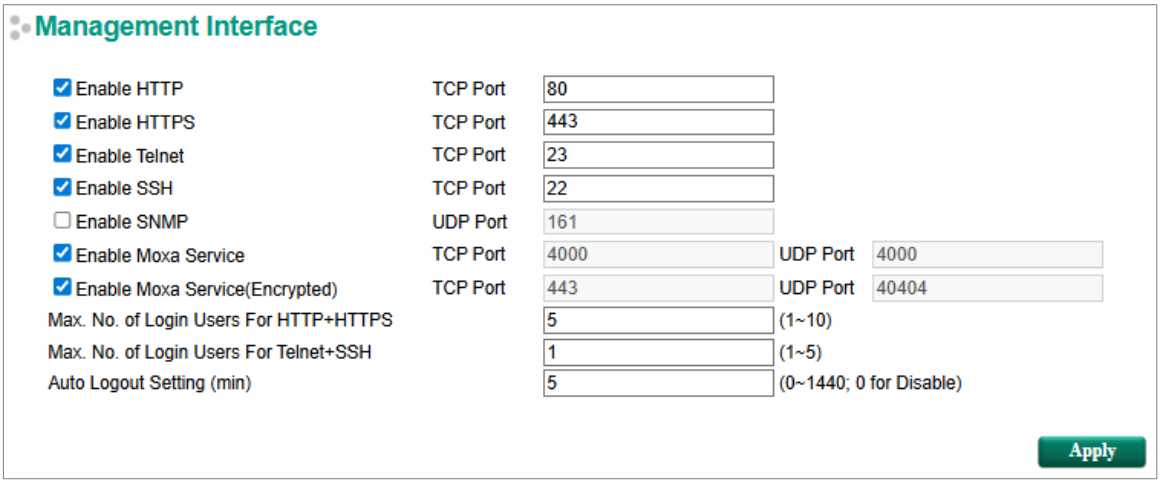


Setting	Description	Factory Default
Port Shutdown Duration (0~65535 seconds)	When the ingress packets exceed the ingress rate limit, the port will be disabled for a certain period.	30 seconds
Ingress Threshold (frames per second)	Select the ingress rate (fps) limit for all packets from the following options: Not Limited, 44640, 74410, 148810, 223220, 372030, 520840, 744050.	Unlimited

Security

Security can be categorized into two levels: the username/password level, and the port access level. Moxa switches provide many kinds of security functions, including Management Interface, Trusted Access, SSL/SSH Authentication certificate, Login Authentication, IEEE 802.1X, MAC Authentication Bypass, Port Security, Broadcast Storm Protection, Loop Protection, and Access Control List.

Management Interface



Enable HTTP

Setting	Description	Factory Default
Select/Deselect	Select the appropriate checkboxes to enable HTTP.	Enabled TCP Port: 80

Enable HTTPS

Setting	Description	Factory Default
Select/Deselect	Select the appropriate checkboxes to enable HTTPS.	Enabled TCP Port: 443

Enable Telnet

Setting	Description	Factory Default
Select/Deselect	Select the appropriate checkboxes to enable Telnet.	Enabled TCP Port: 23

Enable SSH

Setting	Description	Factory Default
Select/Deselect	Select the appropriate checkboxes to enable SSH.	Enabled TCP Port: 22

Enable SNMP

Setting	Description	Factory Default
Select/Deselect	Select the appropriate checkboxes to enable SNMP.	Disabled UDP Port: 161

Enable Moxa Service

Setting	Description	Factory Default
Select/Deselect	Select the appropriate checkboxes to enable Moxa Service. NOTE: Moxa Service is only for Moxa network management software suite.	Enabled TCP Port: 4000 UDP Port: 4000

Enable Moxa Service (Encrypted)

Setting	Description	Factory Default
Select/Deselect	Select the appropriate checkboxes to enable Moxa Service (Encrypted). NOTE: Moxa Service (Encrypted) is only for Moxa network management software suite.	Enabled TCP Port: 443 UDP Port: 40404

Maximum Login Users for HTTP+HTTPS

Setting	Description	Factory Default
Integer (1 to 10)	Sets the maximum number of login users for HTTP and HTTPS	5

Maximum Login Users for Telnet+SSH

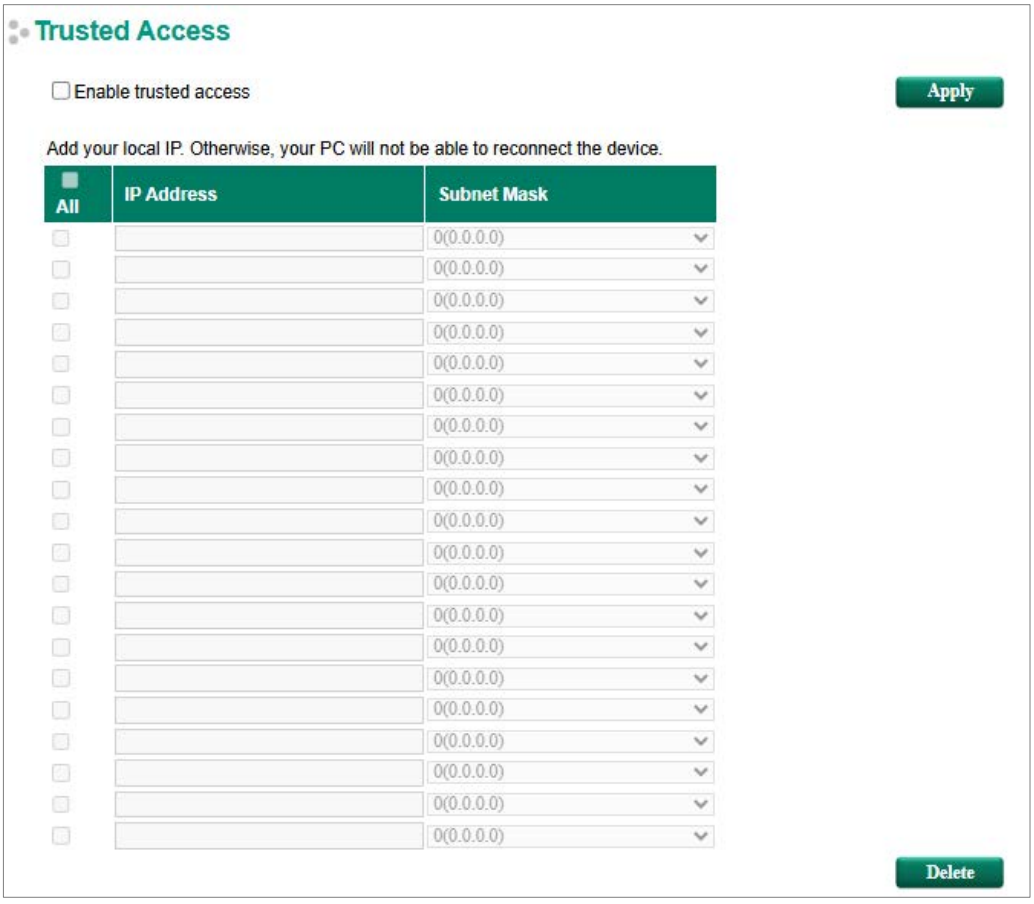
Setting	Description	Factory Default
Integer (1 to 5)	Sets the maximum number of login users for Telnet and SSH	1

Auto Logout Setting (min)

Setting	Description	Factory Default
Integer (0 to 1440)	Sets the web auto logout period. (Enter 0 to disable this function.)	5

Trusted Access

The Moxa switch uses an IP address-based filtering method to control access.



You may add or remove IP addresses to limit access to the Moxa switch. When the Trusted Access list is enabled, only addresses on the list will be allowed access to the Moxa switch. Each IP address and netmask entry can be tailored for different situations:

- **Grant access to one host with a specific IP address**

  For example, enter IP address 192.168.1.1 with netmask 255.255.255.255 to allow access to 192.168.1.1 only.

- **Grant access to any host on a specific subnetwork**

  For example, enter IP address 192.168.1.0 with netmask 255.255.255.0 to allow access to all IPs on the subnet defined by this IP address/subnet mask combination.

- **Grant access to all hosts**

  Make sure the Trusted Access list is not enabled by removing the checkmark from Enable trusted access.

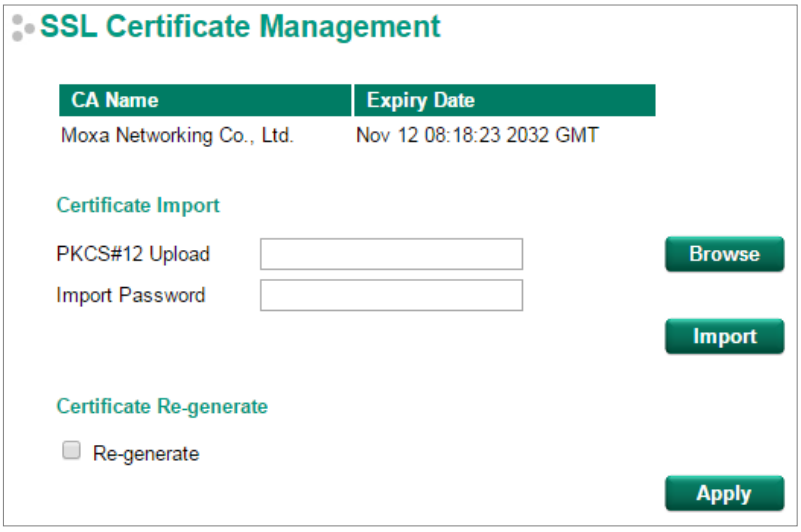
NOTE

Max. 20 set of IP address can be added into the list.

The following table shows additional configuration examples:

Hosts That Need Access	Input Format
Any host	Disable
192.168.1.120	192.168.1.120 / 255.255.255.255
192.168.1.1 to 192.168.1.254	192.168.1.0 / 255.255.255.0
192.168.0.1 to 192.168.255.254	192.168.0.0 / 255.255.0.0
192.168.1.1 to 192.168.1.126	192.168.1.0 / 255.255.255.128
192.168.1.129 to 192.168.1.254	192.168.1.128 / 255.255.255.128

SSL Certificate Management



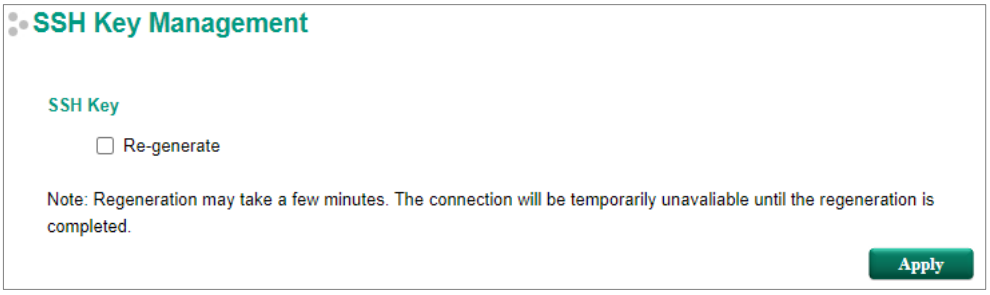
Certificate Import

1. Click **Browse** and select Public-Key Cryptography Standard (PKCS) #12 certificate file.
2. Enter the **Import Password** and click **Import.**
3. The SSL certificate is updated.

Regenerate SSL Certificate

Setting	Description	Factory Default
Select/Deselect	Enable the SSL Certificate Regeneration	Deselect

SSH Key Management



SSH Key Re-generate

Setting	Description	Factory Default
Select/Deselect	Enable SSH Key Re-generate	Deselect

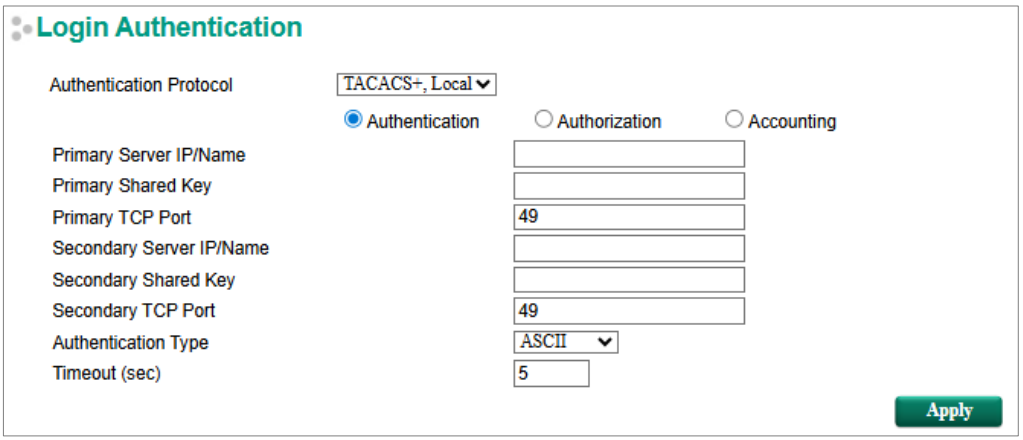
Authentication

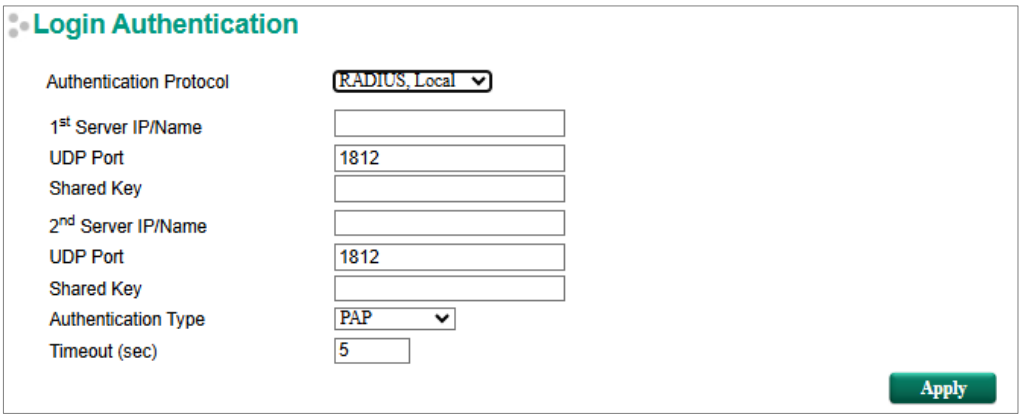
Login Authentication

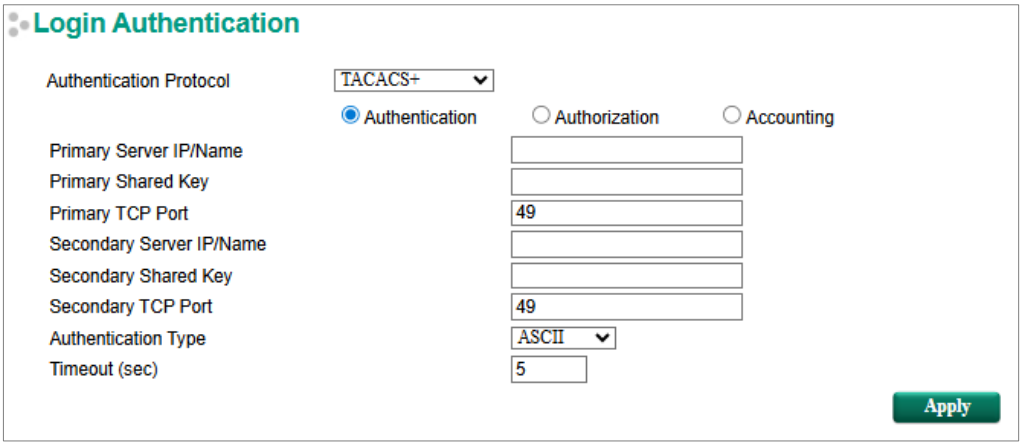
Moxa switches provide three different user login authentications: TACACS+ (Terminal Access Controller Access-Control System Plus), RADIUS (Remote Authentication Dial In User Service), and Local. The TACACS+ and RADIUS mechanisms are centralized "AAA" (Authentication, Authorization and Accounting) systems for connecting to network services. The fundamental purpose of both TACACS+ and RADIUS is to provide an efficient and secure mechanism for user account management.

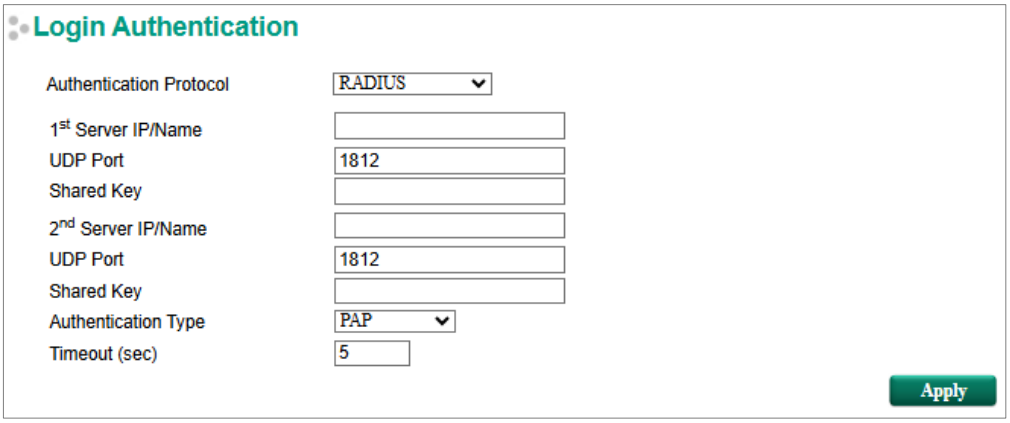
There are five combinations for users:

1. **TACACS+, Local:** Check TACACS+ database first. If checking the TACACS+ database fails, then check the Local database
2. **RADIUS, Local:** Check RADIUS database first. If checking the RADIUS database fails, then check the Local database
3. **TACACS+:** Only check TACACS+ database
4. **RADIUS:** Only check the RADIUS database
5. **Local:** Only check the Local database




Login Authentication
Authentication Protocol
RADIUS, Local
1st Server IP/Name
UDP Port
1812
Shared Key
2nd Server IP/Name
UDP Port
1812
Shared Key
Authentication Type
PAP
Timeout (sec)
5
Apply


Login Authentication
Authentication Protocol
TACACS+
Authentication
Authorization
Accounting
Primary Server IP/Name
Primary Shared Key
Primary TCP Port
49
Secondary Server IP/Name
Secondary Shared Key
Secondary TCP Port
49
Authentication Type
ASCII
Timeout (sec)
5
Apply


Login Authentication
Authentication Protocol
RADIUS
1st Server IP/Name
UDP Port
1812
Shared Key
2nd Server IP/Name
UDP Port
1812
Shared Key
Authentication Type
PAP
Timeout (sec)
5
Apply


Login Authentication
Authentication Protocol
Local
Apply

Setting	Description	Factory Default
Authentication Protocol	Authentication protocol selection.	Local
Authentication/ Authorization/ Accounting	Select the AAA service you want to configure if **TACACS+** or **TACSCS+**, **Local** is selected as the Authentication Protocol.	Authentication
Server IP/Name	Sets the IP address of an external TACACS+/RADIUS server as the authentication database.	None
TCP/UDP Port	Sets the communication port of an external TACACS+/RADIUS server as the authentication database.	TACACS+: 49 RADIUS: 1812
Shared Key	Sets specific characters for server authentication verification.	None
Authentication Type	Authentication mechanism selection. ASCII, PAP, CHAP, and MSCHAP are for TACACS+; PAP, CHAP and MSCHAPv2 are for RADIUS.	ASCII for TACACS+ PAP for RADIUS
Timeout (sec)	The timeout period for waiting for a server response.	5

NOTE

The account privilege level is authorized under service type settings in RADIUS, and the privilege level is under TACACS+.

RADIUS Server

- RADIUS Service type = 6 = read/write = administrator
- RADIUS Service type = 1 = read only = user

TACACS+ Server

- TACACS+ privilege level= 15 = read/write = administrator
- TACACS+ privilege level= 1 to 14 = read only = user

IEEE 802.1X Settings

The IEEE 802.1X standard defines a protocol for client/server-based access control and authentication. The protocol restricts unauthorized clients from connecting to a LAN through ports that are open to the Internet, and which otherwise would be readily accessible. The purpose of the authentication server is to check each client that requests access to the port. The client is only allowed access to the port if the client's permission is authenticated.

Three components are used to create an authentication mechanism based on 802.1X standards: Client/Supplicant, Authentication Server, and Authenticator.

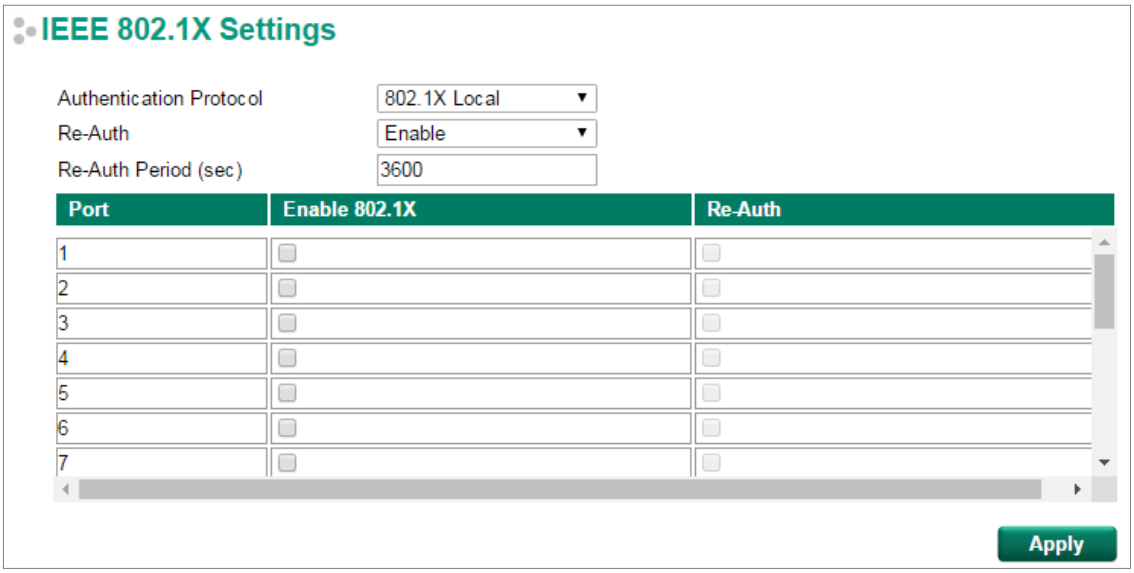
Client/Supplicant: The end station that requests access to the LAN and switch services and responds to the requests from the switch.

Authentication Server: The server that performs the actual authentication of the supplicant.

Authenticator: Edge switch or wireless access point that acts as a proxy between the supplicant and the authentication server, requesting identity information from the supplicant, verifying the information with the authentication server, and relaying a response to the supplicant.

The Moxa switch acts as an authenticator in the 802.1X environment. 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 we use an external RADIUS server as the authentication server, the authenticator and the authentication server exchange EAP frames.

Authentication can be initiated either by the supplicant or the authenticator. When the supplicant initiates the authentication process, it sends an **EAPOL-Start** frame to the authenticator. When the authenticator initiates the authentication process or when it receives an **EAPOL Start** frame, it sends an **EAP Request/Identity** frame to ask for the username of the supplicant.



Authentication Protocol

Setting	Description	Factory Default
802.1X Local (Max. of 32 users)	Select this option when setting the 802.1X Local User Database as the authentication database.	802.1X Local
RADIUS	Select this option to set an external RADIUS server as the authentication database. The authentication mechanism is EAP-MD5.	
RADIUS, 802.1X Local	Select this option to make using an external RADIUS server as the authentication database the first priority. The authentication mechanism is EAP-MD5. The second priority is to set the 802.1X Local User Database as the authentication database.	

Re-Auth (Global)

Setting	Description	Factory Default
Enable/Disable	Select enable to require re-authentication of the client after a preset time period of no activity has elapsed.	Enable

Re-Auth Period (sec)

Setting	Description	Factory Default
60 to 65535	Sets the Re-Auth period	3600

Enable 802.1X

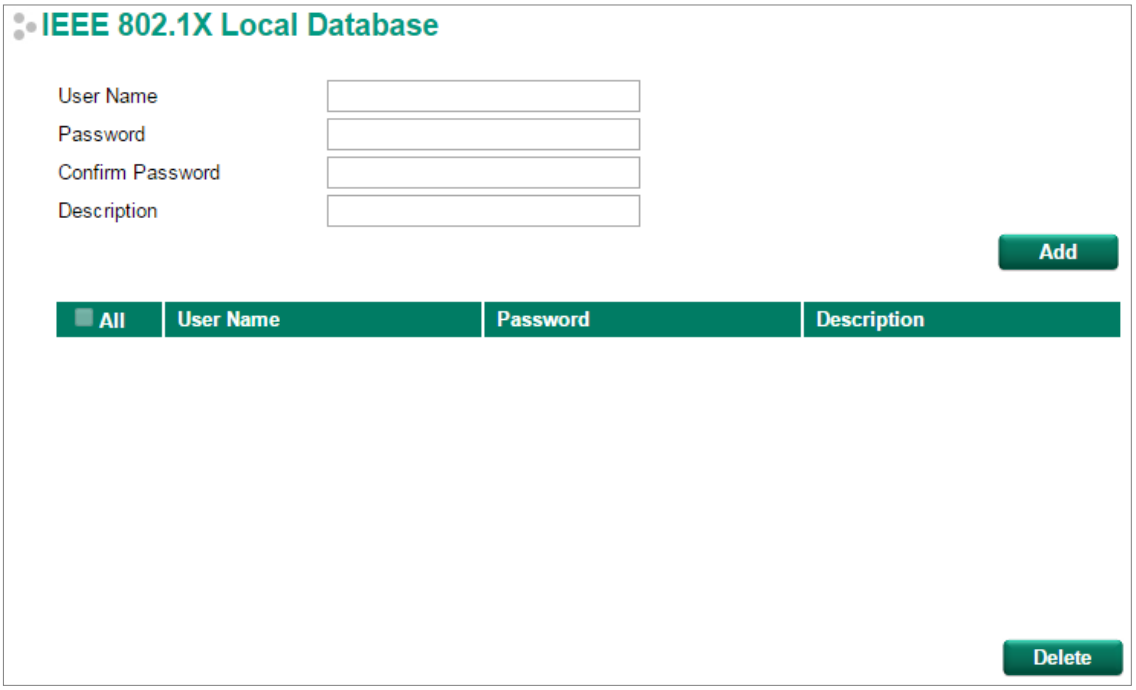
Setting	Description	Factory Default
Select/Deselect	Select the checkbox under the 802.1X column to enable IEEE 802.1X for one or more ports. All end stations must enter usernames and passwords before access to these ports is allowed.	Deselect

Re-Auth

Setting	Description	Factory Default
Select/Deselect	Select enable to require re-authentication of the client by port	Deselect

IEEE 802.1X Local Database

When selecting the 802.1X Local as the authentication protocol, set the IEEE 802.1X Local Database first.



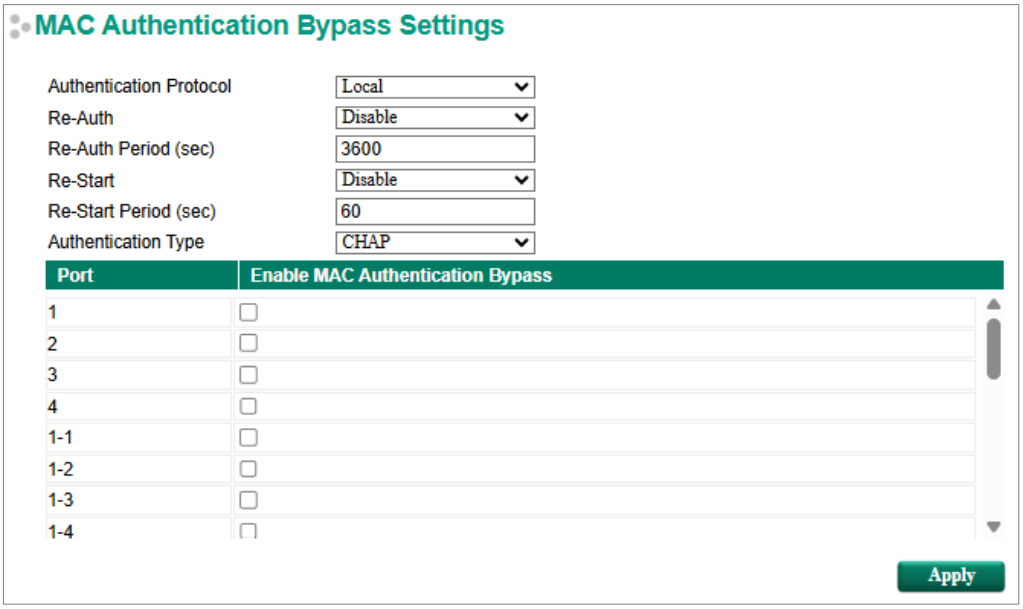
IEEE 802.1X Local Database Setup

Setting	Description	Factory Default
User Name (Max. of 30 characters)	Username for the Local User Database	None
Password (Max. of 16 characters)	Password for the Local User Database	None
Confirm Password (Max. of 16 characters)	Confirm Password for the Local User Database	None
Description (Max. of 30 characters)	Description for the Local User Database	None

NOTE

The username for the IEEE 802.1X Local Database is case-insensitive.

MAC Authentication Bypass Settings



Authentication Protocol

Setting	Description	Factory Default
Local	Devices on your network are authenticated using local database.	Local
RADIUS	RADIUS is the only authentication protocol of the MAC Authentication Bypass.	

Re-Auth

Setting	Description	Factory Default
Enable/Disable	Select enable to require re-authentication of the client after a preset time period of no activity has elapsed	Disable

Re-Auth Period (sec)

Setting	Description	Factory Default
60 to 65535	Sets the Re-Auth period	3600

Re-Start

Setting	Description	Factory Default
Enable/Disable	Select enable to require a present time period to re-start authentication after failure of authentication	Disable

Re-Start Period (sec)

Setting	Description	Factory Default
5 to 300	Sets the Re-Start period	60

Authentication Type

Setting	Description	Factory Default
PAP	Password Authentication Protocol	CHAP
CHAP	Challenge Handshake Authentication Protocol	
MS-CHAPv2	Microsoft Challenge Handshake Authentication Protocol version 2	

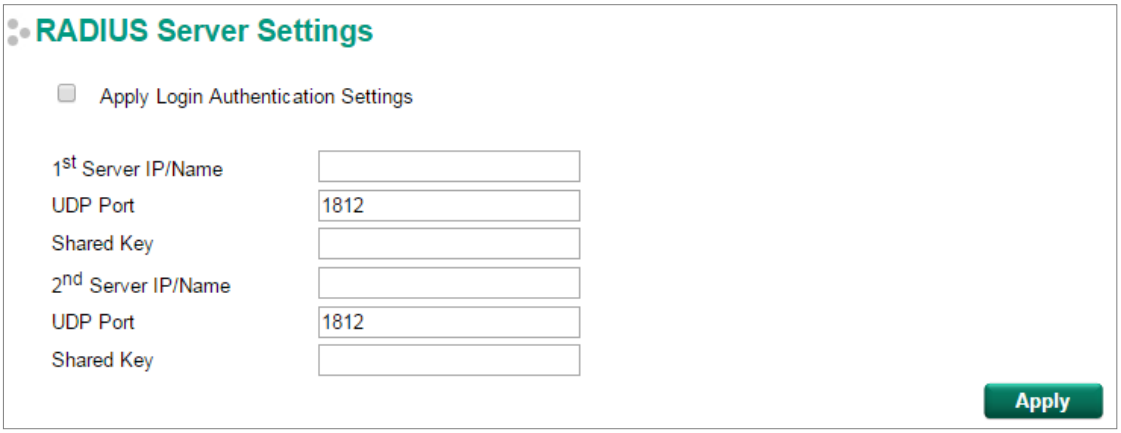
Bypass

Setting	Description	Factory Default
Select/Deselect	Check the checkbox under the MAC Authentication Bypass column to enable MAC Authentication Bypass for one or more ports	Deselect

NOTE

If RADIUS Server is case sensitive, use lower-case characters for the username and password.

RADIUS Server Settings



Apply Login Authentication Setting

Setting	Description	Factory Default
Select/Deselect	Enables using the same setting as Auth Server.	Deselect

Server Setting

Setting	Description	Factory Default
Server IP/Name	Specifies the IP/name of the server	None
Server Port	Specifies the port of the server	1812
Server Shared Key	Specifies the shared key of the server	None

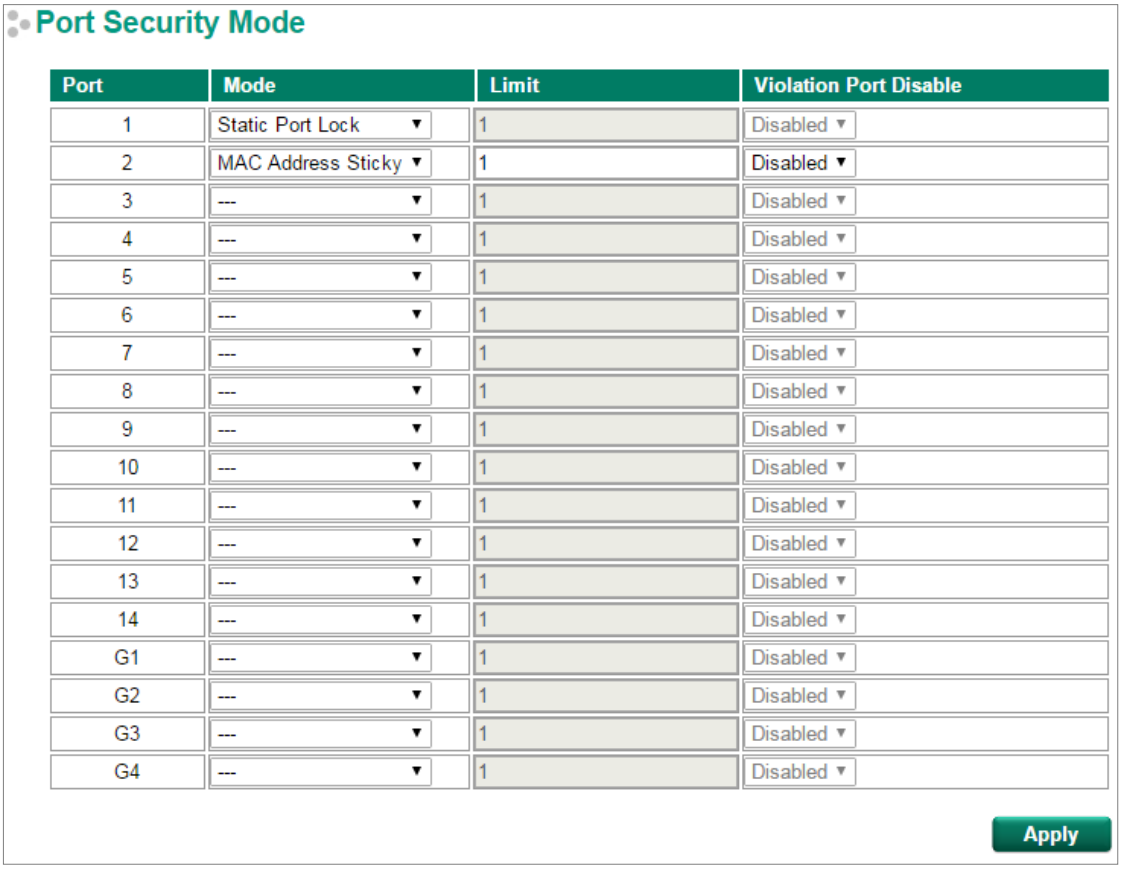
Port Security

Moxa switches provide a Port Security function that lets packets with allowed MAC Addresses access the switch's ports. Two Port Security modes are supported: **Static Port Lock** and **MAC Address Sticky**.

Static Port Lock: Allows users to configure specific MAC addresses that are allowed to access the port.

MAC Address Sticky: Allows users to configure the maximum number of MAC addresses (the Limit) that a port can "learn." Users can configure what action should be taken (under Violation Port Disable) when a new MAC address tries to access a port after the maximum number of MAC addresses have already been learned. The total number of allowed MAC addresses cannot exceed 1024.

Port Security Mode



Mode

Setting	Description	Factory Default
Static Port Lock	The switch will block unauthorized MAC addresses and allow access to packets with a MAC address defined in the Static Unicast MAC Address Table.	None
MAC Address Sticky	If Limit is set to n, the switch will learn the first n MAC addresses that access the port, and automatically store them in the MAC Address Control Table.	

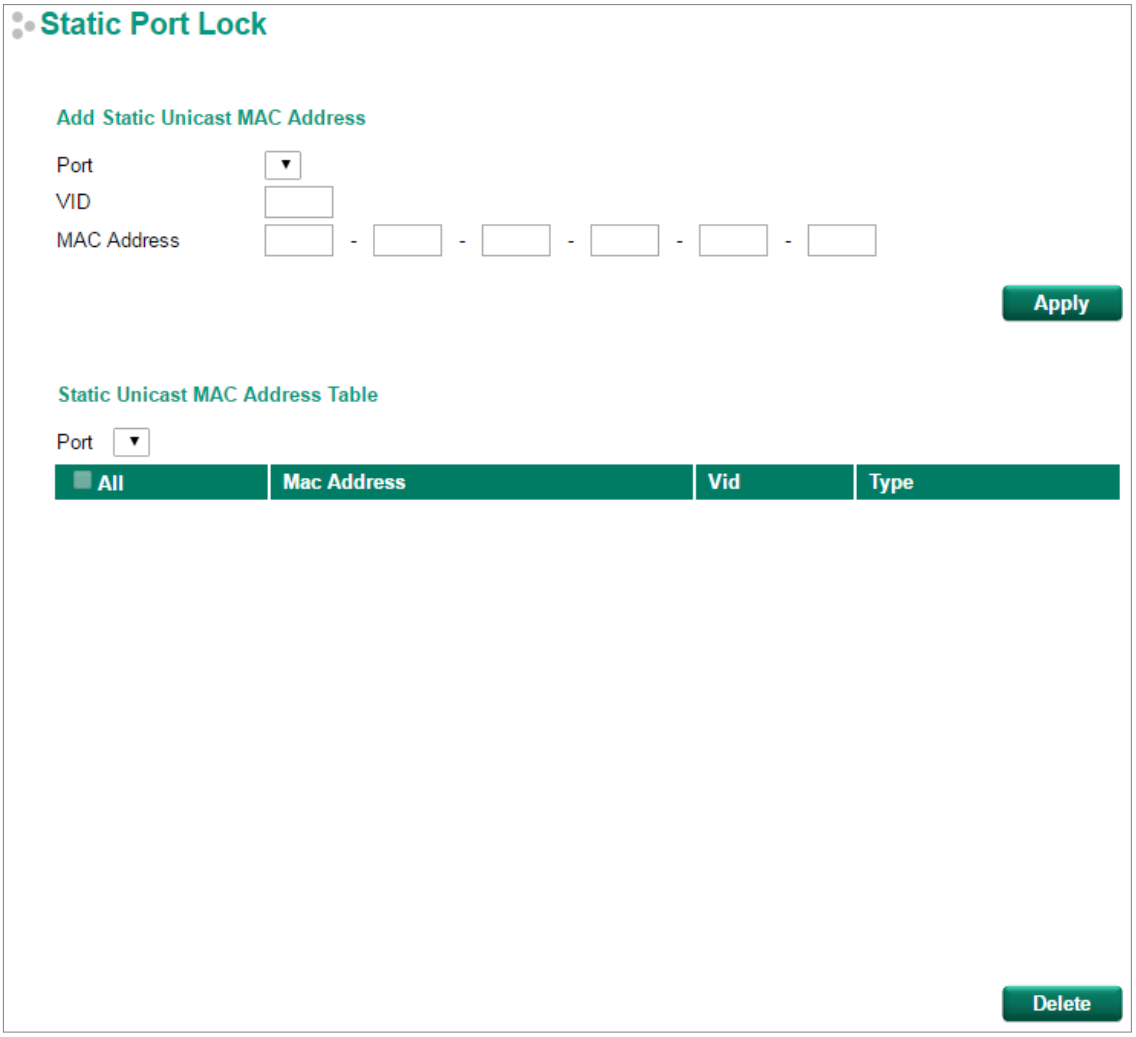
Limit (only active for MAC Address Sticky)

Setting	Description	Factory Default
1 to 1024	The maximum number of learned MAC addresses allowed for that port.	1

Violation Port Disable (only active for MAC Address Sticky)

Setting	Description	Factory Default
Disable	When the port receives a packet with an unlearned MAC address, the packet will be discarded.	Disable
Enable	When the port receives a packet with an unlearned MAC address, the port will be disabled.	

Static Port Lock



Port Number

Setting	Description	Factory Default
Port Number	Associates the static address to a dedicated port	None

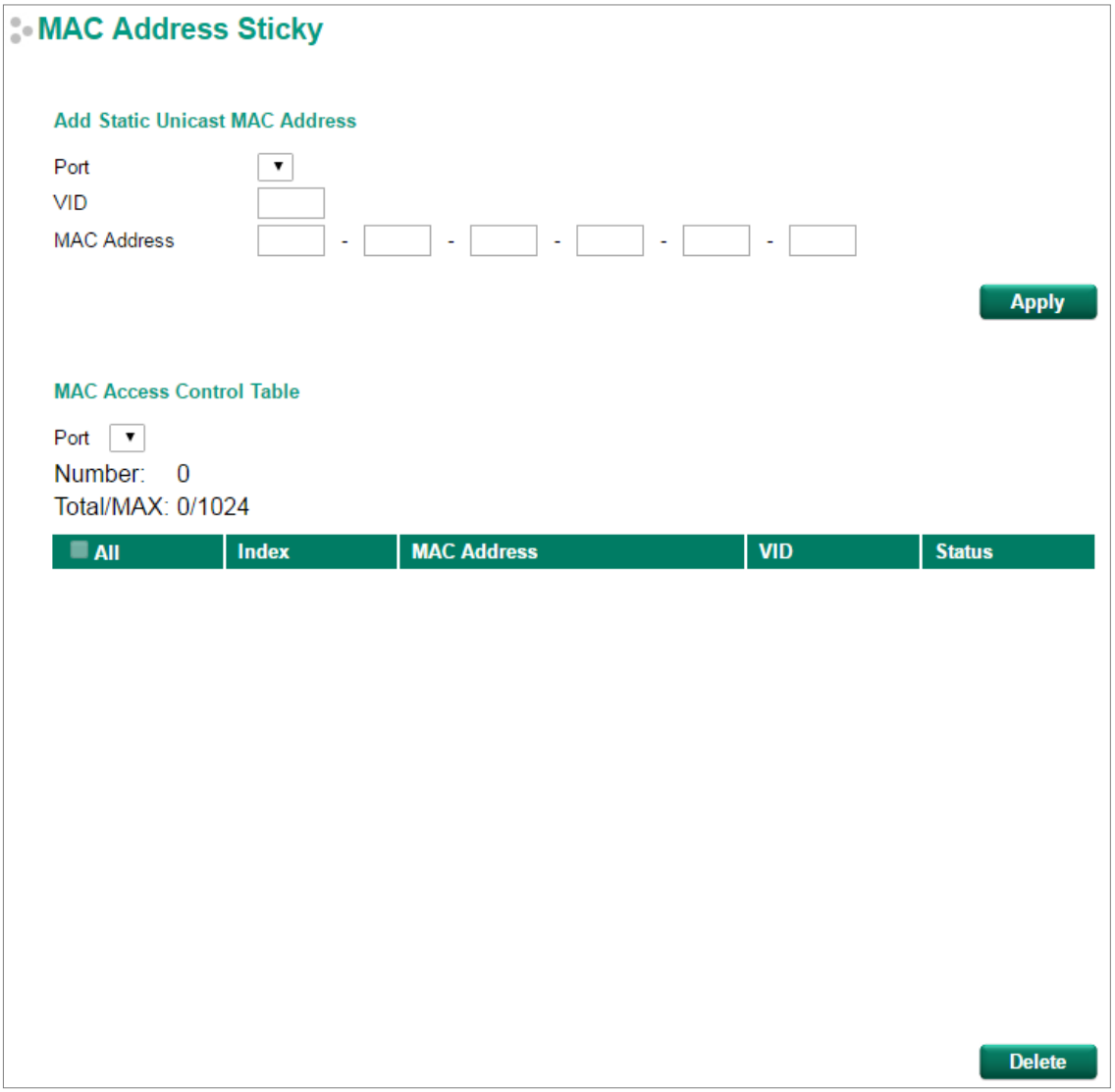
VID

Setting	Description	Factory Default
VLAN ID	Associates the static address to a dedicated VLAN on the port	None

MAC Address

Setting	Description	Factory Default
MAC Address	Adds the static unicast MAC address into the address table	None

MAC Address Sticky



Port Number

Setting	Description	Factory Default
Port Number	Associates the static address to a dedicated port	None

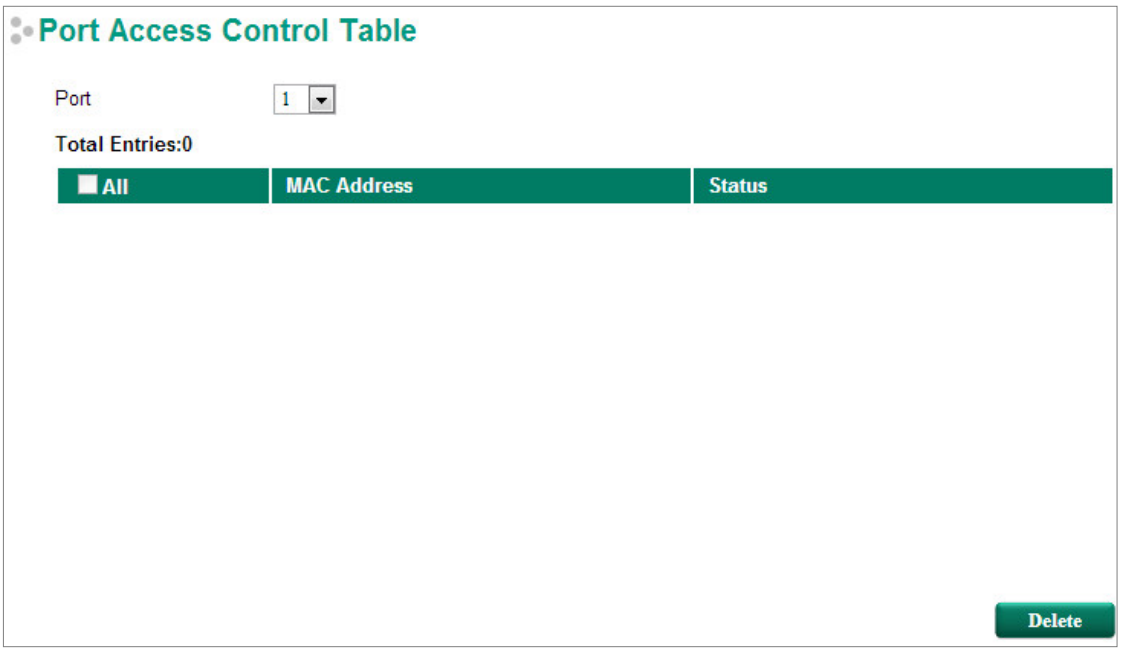
VID

Setting	Description	Factory Default
VLAN ID	Associates the static address to a dedicated VLAN on the port	None

MAC Address

Setting	Description	Factory Default
MAC Address	Adds the static unicast MAC address into the address table	None

Port Access Control Table



The port status will be indicated as **authorized** or **unauthorized**.

Loop Protection

Enable Loop Protection

Setting	Description	Factory Default
Enable	Select the Enable checkbox to enable the loop protection function.	Disable
Disable	Deselect the Enable checkbox to disable the loop protection function.	

Access Control List

NOTE

PT-G7728 switches only support Ingress ACL.

Access control lists (ACLs) increase the flexibility and security of networking management. ACLs provide traffic filtering capabilities for ingress and egress packets. Moxa ACLs can manage filter criteria for a diverse range of protocols and allow users to configure customized filter criteria. For example, users can deny access to specific source or destination IP/MAC addresses. The Moxa ACL configuration interface is easy to use. Users can quickly establish filtering rules, manage rule priorities, and view overall settings on the display page.

The ACL Concept

What is ACL?

An access control list is a basic traffic filter for ingress and egress packets. The ACL can examine each Ethernet packet's information and take the necessary action. Moxa Layer 3 switches provide complete filtering capabilities. Access list criteria could include the source or destination IP address of the packets, the source or destination MAC address of the packets, IP protocols, or other information. The ACL can check these criteria to decide whether to permit or deny access to a packet.

Benefits of ACL

ACLs support per interface, per packet direction, and per protocol filtering capability. These features can provide basic protection by filtering specific packets. The main benefits of an ACL are:

- **Manage authority of hosts:** An ACL can restrict specific devices through MAC address filtering. The user can deny all packets or only permit packets that come from specific devices.
- **Subnet authority management:** Configure filtering rules for specific subnet IP addresses. An ACL can restrict packets from or to specific subnets.
- **Network security:** The demand for networking security is growing. An ACL can provide basic protection that works in a similar manner to an Ethernet firewall device.
- **Control traffic flow by filtering specific protocols:** An ACL can filter specific IP protocols such as TCP or UDP packets.

How an ACL Works

The ACL working structure is based on access lists. Each access list is a filter. When a packet enters into or exits from a switch, the 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. In other words, Access Control Lists have "Priority Index" as an attribute to define the priority in the web configuration console.

There are two types of settings for an ACL: list settings and rule settings. In order to be created, an Access Control List needs the following list settings: Name, Priority Index, Filter Type, and Ports to Apply. Once created, each Access Control List has its own set of rule settings. The Priority Index represents the priority of the names in the access list. Names at Priority Index 1 have first priority in packet filtering. The Priority Index is adjustable whenever users need to change the priority. Two types of packet filtering can be used:

- IP based
- MAC Based

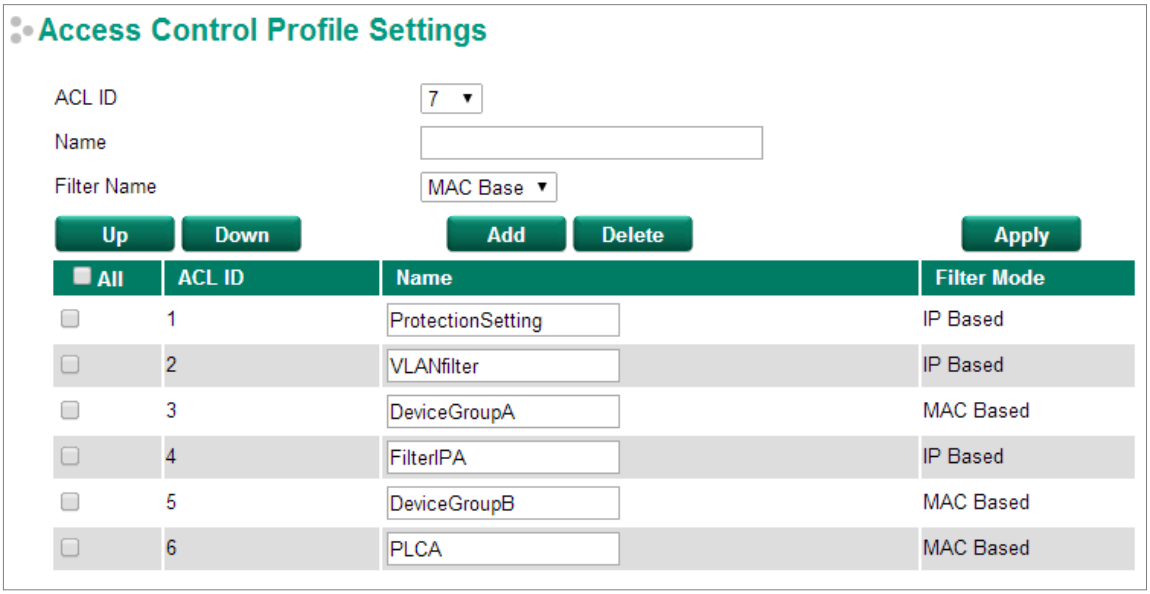
The filter type defines whether the access list will examine packets based on IP or MAC address. The type affects what detailed rules can be edited. You can then assign the ports you would like to apply the list to. You can also define Ingress and Egress per port.

After adding a new access control list, you can also create new rules for the access control list. Each ACL group accepts 10 rules. Rules can filter packets by source and destination IP/MAC address, IP protocol, TCP/UDP Port, Ethernet Type, and VLAN ID.

After all rules are set, the ACL starts to filter the packets by the rule with the highest Priority Index (smaller number, higher priority). Once a rule denies or accepts its access, the packet will be dropped or passed.

Access Control List Configuration and Setup

Access Control Profile Settings



On this page, you can configure two settings: (1) Add/Modify Access Control list, and (2) Adjust ACL ID.

Add/Modify Access Control List

This function lets you add a new access control profile or modify an existing access control profile. The operation depends on the ACL ID you select. If the selected ACL ID is still empty, you can start by creating a new access control profile. Parameters for editing are as follows:

- **ACL ID:** The ACL checking sequence is based on these IDs. Smaller ID numbers have a higher priority for packet filtering. If a packet is filtered by an access control profile with a higher priority, those access control profiles with a lower priority will not be executed.

  Note that the ACL ID is not unique with respect to the profile name. The ID changes when swapping the priority of different access control profiles.

  The maximum Priority Index number is 16.
- **Name:** You can name the access control profile in this field.
- **Filter Name:** Select filtering by either IP or MAC address. Detailed settings can be configured in the Access Control Rule Settings page.

If a selected ACL ID is already in the access control list, then you can modify the parameters listed above. After the configuration is complete, click **Apply** to confirm the settings. A new list will appear in the Access Control List Table.

Adjust ACL ID

Changing an established access control profile's priority is easy. Moxa provides a simple interface to let you easily adjust the priority. Follow the three steps below to adjust the priority:

Step 1: Select the profile.

Step 2: Click the **Up/Down** button to adjust the sequence. The ACL ID will change with the profile's position.

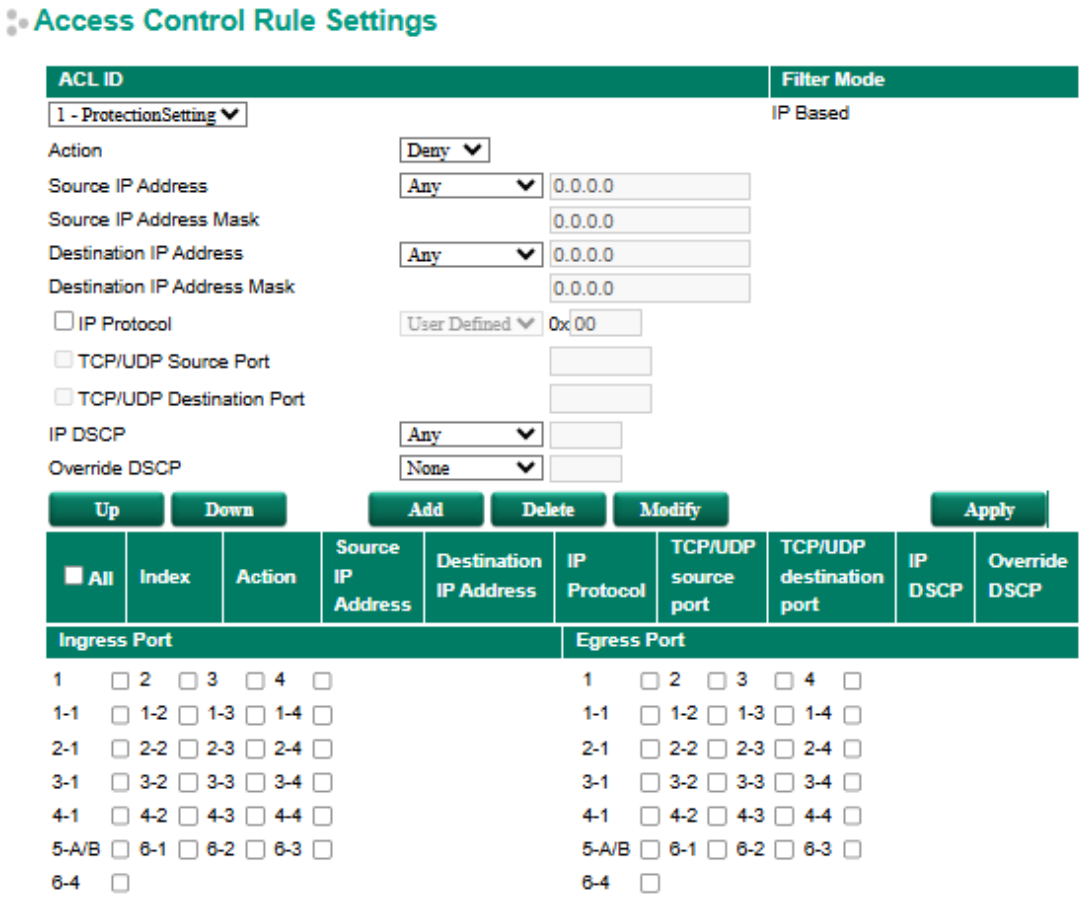
Step 3: Click the **Apply** button to confirm the settings.

Access Control Rule Settings

You can edit access control rules on this page. Each ACL includes up to 10 rules. First, select the access control profile you would like to edit based on the ACL ID, and then set up the rule content and ingress/egress ports. After configuring, click the **Add** button to add the rule to the list. Finally, click **Apply** to activate the settings.

An access control rule displays setting options based on the filtering type used:

Based (Layer 3 Device)

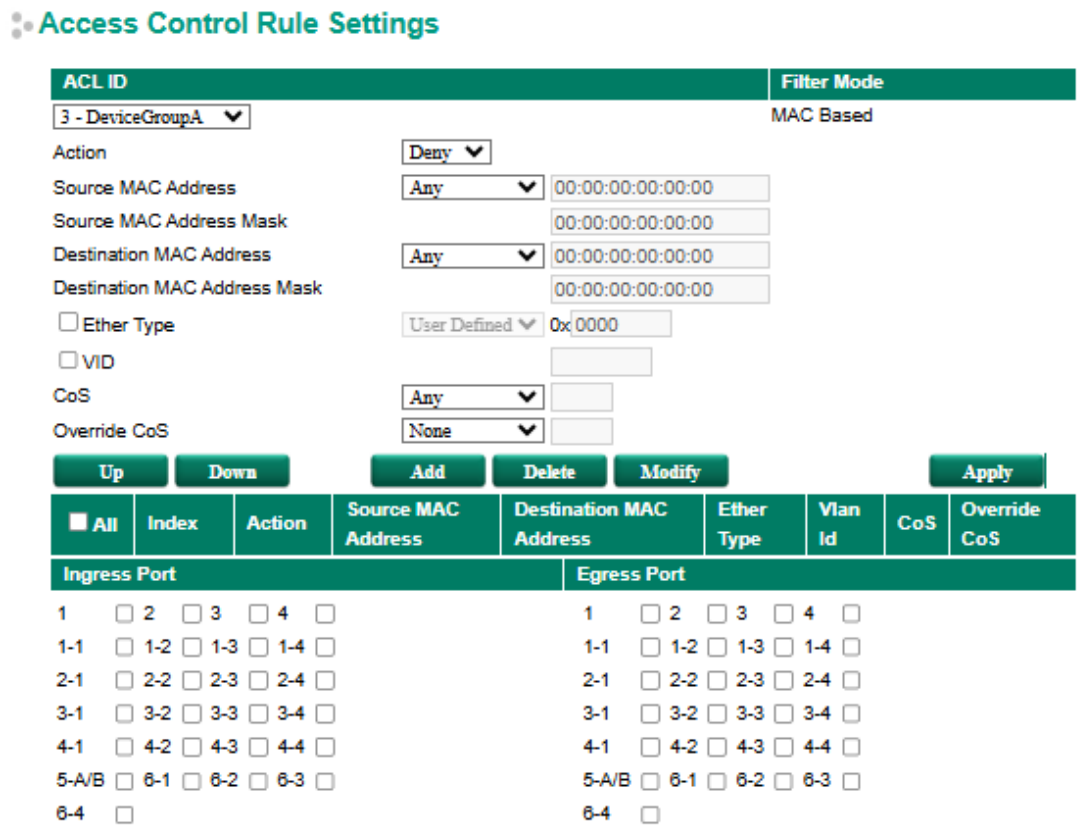


NOTE

The DSCP override rule will only be executed when permitted by the rules in the ACL.

- **Action:** Whether to deny or permit access if the rule criterion is met.
- **Source (Destination) IP Address / IP Address Mask:** Defines the IP address rule. By using the mask, you can assign specific subnet ranges to filter. It allows checking the source or destination of the packet. Choose **Any** if you do not need to use this criteria.
- **IP Protocol:** Select the type of protocols to be filtered. Moxa provides ICMP, IGMP, IP over IP, TCP, and UDP as options in this field.
- **TCP/UDP Source (Destination) Port:** If TCP or UDP are selected as the filtering protocol, these fields will allow you to enter port numbers for filtering.
- **IP DSCP / Override DSCP:** Defines the rules of IP DSCP and Override DSCP.

Based (Layer 2 Device)

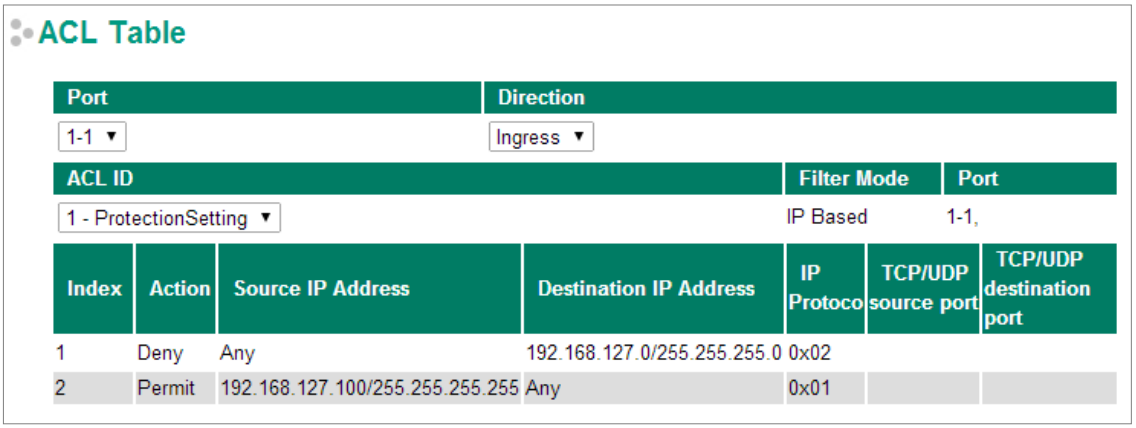


- **Action:** Whether to deny or permit access if the rule criterion is met.
- **Source (Destination) MAC Address / MAC Address Mask:** Defines the MAC address rule. By using the mask, you can assign specific MAC address ranges to filter. It allows checking the source or destination of the packet. Choose **Any** if you do not need to use this criterion.
- **Ethernet Type:** Select the type of Ethernet protocol to filter. Options are IPv4, ARP, RARP, IPv6, IEE802.3, PROFIENT, LLDP, and IEEE1588.
- **VLAN ID:** Enter a VLAN ID you would like to filter by. Defines the rules of CoS and Override CoS to override the CoS value within the VLAN Tag, if required.

Once ready, click the **Add** button to add the rule to the list and set up the ingress/egress ports, and then click **Apply** to activate the settings.

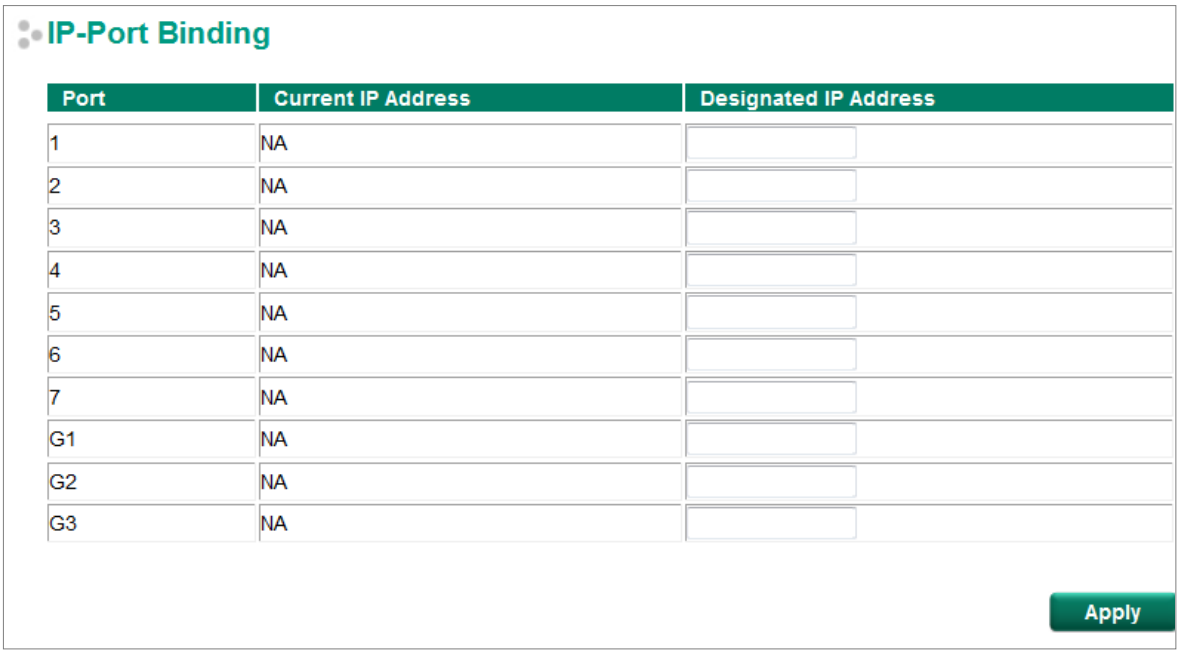
Access Control List Table

The Access Control List Table page provides a complete view of all ACL settings. On this page, you can view the rules by Ingress port, Egress port, or ACL ID. Click the drop-down menu to select Port or ACL ID, and all the rules will be displayed in the table.



DHCP

IP-Port Binding



Designated IP Address

Setting	Description	Factory Default
IP Address	Set the desired IP of connected devices.	None

DHCP Relay Agent

The DHCP Relay Agent makes it possible for DHCP broadcast messages to be sent over routers. The DHCP Relay Agent enables DHCP clients to obtain IP addresses from a DHCP server on a remote subnet, or those that are not located on the local subnet.

DHCP Relay Agent (Option 82)

Option 82 is used by the relay agent to insert additional information into the client's DHCP request. The Relay Agent Information option is inserted by the DHCP relay agent when forwarding client-originated DHCP packets to a DHCP server. Servers can recognize the Relay Agent Information option and use the information to implement IP addresses to Clients.

When Option 82 is enabled on the switch, a subscriber device is identified by the switch port through which it connects to the network (in addition to its MAC address). Multiple hosts on the subscriber LAN can be connected to the same port on the access switch and are uniquely identified.

The Option 82 information contains 2 sub-options, Circuit ID and Remote ID, which define the relationship between the end device IP and the DHCP Option 82 server. The Circuit ID is a 4-byte number generated by the Ethernet switch—a combination of physical port number and VLAN ID. The format of the Circuit ID is shown below:

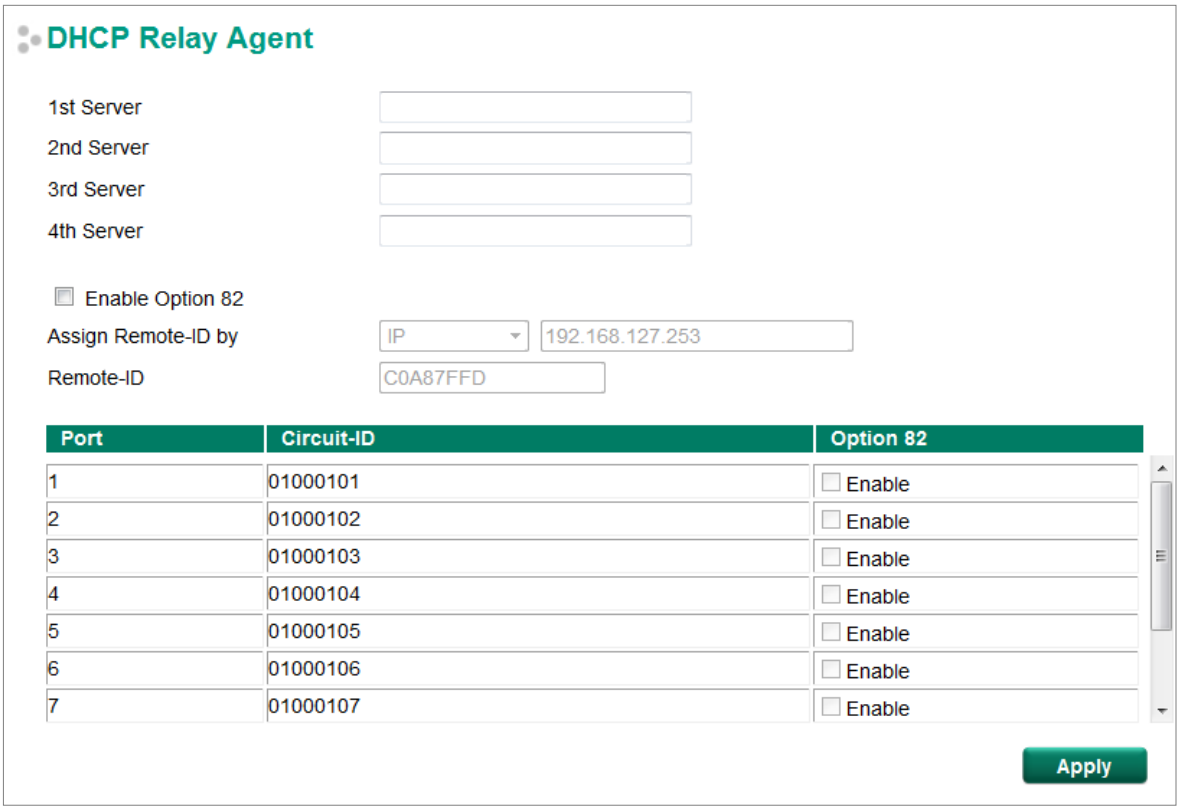
FF–VV–VV–PP

This is where the first byte "FF" is fixed to "01", the second and the third byte "VV-VV" is formed by the port VLAN ID in hex, and the last byte "PP" is formed by the port number in hex. For example:

01–00–0F–03 is the "Circuit ID" of port number 3 with port VLAN ID 15.

The "Remote ID" identifies the relay agent itself and can be one of the following:

1. The IP address of the relay agent.
2. The MAC address of the relay agent.
3. A combination of IP address and MAC address of the relay agent.
4. A user-defined string.



Server IP Address

1st Server

Setting	Description	Factory Default
IP address for the 1st DHCP server	Assigns the IP address of the 1st DHCP server that the switch tries to access.	None

2nd Server

Setting	Description	Factory Default
IP address for the 2nd DHCP server	Assigns the IP address of the 2nd DHCP server that the switch tries to access.	None

3rd Server

Setting	Description	Factory Default
IP address for the 3rd DHCP server	Assigns the IP address of the 3rd DHCP server that the switch tries to access.	None

4th Server

Setting	Description	Factory Default
IP address for the 4th DHCP server	Assigns the IP address of the 4th DHCP server that the switch tries to access.	None

DHCP Option 82

Enable Option 82

Setting	Description	Factory Default
Enable or Disable	Enable or disable the DHCP Option 82 function.	Disable

Assign Remote-ID by

Setting	Description	Factory Default
IP	Uses the switch's IP address as the remote ID sub.	IP
MAC	Uses the switch's MAC address as the remote ID sub.	IP
Client-ID	Uses a combination of the switch's MAC address and IP address as the remote ID sub.	IP
Other	Uses the user-designated ID sub.	IP

Value

Setting	Description	Factory Default
Max. of 12 characters	Displays the value that was set. Complete this field if type is set to Other.	Switch IP address

Remote-ID

Setting	Description	Factory Default
read-only	The actual hexadecimal value configured in the DHCP server for the Remote-ID. This value is automatically generated according to the Value field. Users cannot modify it.	C0A87FFD

DHCP Function Table

Enable

Setting	Description	Factory Default
Enable or Disable	Enable or disable the DHCP Option 82 function for this port.	Disable

SNMP

The Moxa switch supports SNMP V1, V2c, and V3. SNMP V1 and SNMP V2c use a community string match for authentication, which means that SNMP servers access all objects with read-only or read/write permissions using the community strings public and private by default. SNMP V3 requires that you select an authentication level of MD5 or SHA and is the most secure protocol. You can also enable data encryption to enhance data security.

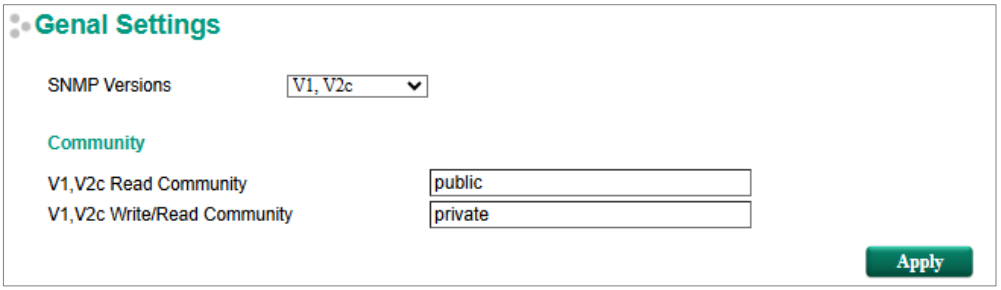
Supported SNMP security modes and levels are shown in the following table. Select the security mode and level that will be used to communicate between the SNMP agent and manager.

Protocol Version	UI Setting	Authentication	Encryption	Method
SNMP V1, V2c	V1, V2c Read Community	Community string	No	Uses a community string match for authentication.
	V1, V2c Write/Read Community	Community string	No	Uses a community string match for authentication.

NOTE

- Users can create dedicated accounts using an independent SNMPv3 Account Database.
- The SNMPv3 accounts **admin-snmp** and **user-snmp** can only access SNMP information and cannot log into other network management interfaces.
- The **admin-sys** and **user-sys** accounts are imported from User Account into the SNMPv3 Account Database to . The accounts can access all network management interfaces. The settings and management of these accounts are handled in the User Account and cannot be changed in the SNMPv3 account database.
- Accounts with admin privilege have read/write access to all configuration parameters. Accounts with user authority only have read access to configuration parameters.
- A maximum of 10 SNMPv3 accounts can be setup.

These parameters are configured on the SNMP page. A more detailed explanation of each parameter is given below the figure.



SNMP Read/Write Settings

SNMP Versions

Setting	Description	Factory Default
V1, V2c, V3, or V1, V2c, or V3 only	Specifies the SNMP protocol version used to manage the switch.	V1, V2c

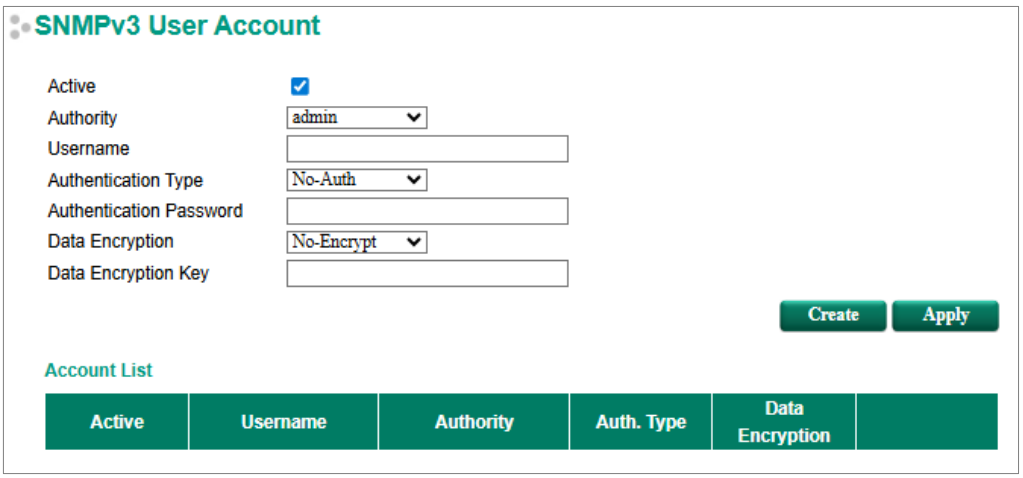
V1, V2c Read Community

Setting	Description	Factory Default
Max. 30 characters	Specifies the community string to authenticate the SNMP agent for read-only access. The SNMP agent will access all objects with read-only permissions using this community string.	Public

V1, V2c Write/Read Community

Setting	Description	Factory Default
Max. 30 characters	Specifies the community string to authenticate the SNMP agent for read/write access. The SNMP server will access all objects with read/write permissions using this community string.	Private

For SNMP V3, two levels of privilege are available for accessing the Moxa switch. **Admin** privilege provides access and authorization to read and write the MIB file. **User** privilege only allows reading the MIB file.



Admin Auth. Type

Setting	Description	Auth. Password Valid Range	Factory Default
No-Auth	Allows the admin account to access objects without authentication.	N/A	No-Auth
MD5	Authentication will be based on the HMAC-MD5 algorithms.	8-32 characters	
SHA	Authentication will be based on the HMAC-SHA algorithms.	8-32 characters.	
SHA 256	Authentication will be based on the HMAC-SHA256 algorithms.	8-32 characters.	
SHA 512	Authentication will be based on the HMAC-SHA512 algorithms.	8-32 characters.	

Enable Admin Data Encryption Key (for SNMP V1, V2c, V3, and V3 only)

Setting	Description	Factory Default
Enable	Enables data encryption using the specified data encryption key: DES or AES (between 8 and 32 characters).	No
Disable	Specifies that data will not be encrypted.	No

User Auth. Type

Setting	Description	Auth. Password Valid Range	Factory Default
No-Auth	Allows the admin account to access objects without authentication.	N/A	No-Auth
MD5	Authentication will be based on the HMAC-MD5 algorithms.	8-32 characters	
SHA	Authentication will be based on the HMAC-SHA algorithms.	8-32 characters.	
SHA 256	Authentication will be based on the HMAC-SHA256 algorithms.	8-32 characters.	
SHA 512	Authentication will be based on the HMAC-SHA512 algorithms.	8-32 characters.	

Enable User Data Encryption Key (for SNMP V1, V2c, V3 and V3 only)

Setting	Description	Factory Default
Enable	Enables data encryption using the specified data encryption key: DES or AES (between 8 and 32 characters).	No
Disable	No data encryption	No

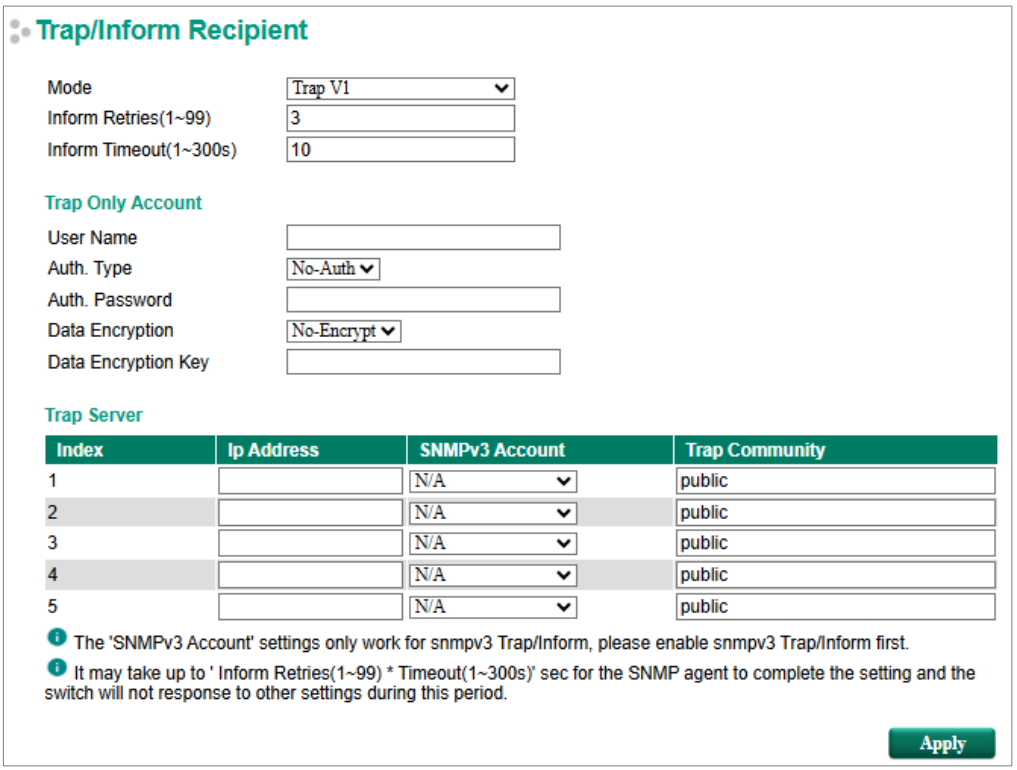
Trap/Inform Settings

SNMP traps allow an SNMP agent to notify the NMS of a significant event. The switch supports two SNMP modes: Trap mode and Inform mode.

SNMP Trap Mode—Trap

SNMP traps allow an SNMP agent to notify the NMS of a significant event. The switch supports two SNMP modes: Trap mode and Inform mode.

SNMP Trap V1, Trap V2c



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.

Setting	Description	Factory Default
Trap V1	Use Trap V1 for SNMP notifications	Trap V1
Trap V2c	Use Trap V2c for SNMP notifications	
Inform V2c	Use Inform V2c for SNMP notifications	
Trap V3	Use Trap V3 for SNMP notifications	
Inform V3	Use Inform V3 for SNMP notifications	

The 'SNMPv3 Account' settings only work for snmpv3 Trap/Inform, you should first enable snmpv3 Trap/Inform.

Auth. Type

Setting	Description	Auth. Password Valid Range	Factory Default
No-Auth	Allows the admin account to access objects without authentication.	N/A	No-Auth
MD5	Authentication will be based on the HMAC-MD5 algorithms.	8-32 characters	
SHA	Authentication will be based on the HMAC-SHA algorithms.	8-32 characters.	
SHA 256	Authentication will be based on the HMAC-SHA256 algorithms.	8-32 characters.	
SHA 512	Authentication will be based on the HMAC-SHA512 algorithms.	8-32 characters.	

Data Encryption

Setting	Description	Auth. Password Valid Range	Factory Default
No-Encrypt	No data encryption	N/A	No-Encrypt
DES	A symmetric-key algorithm	8-32 characters	
AES	A symmetric-key algorithm	16-32 characters	

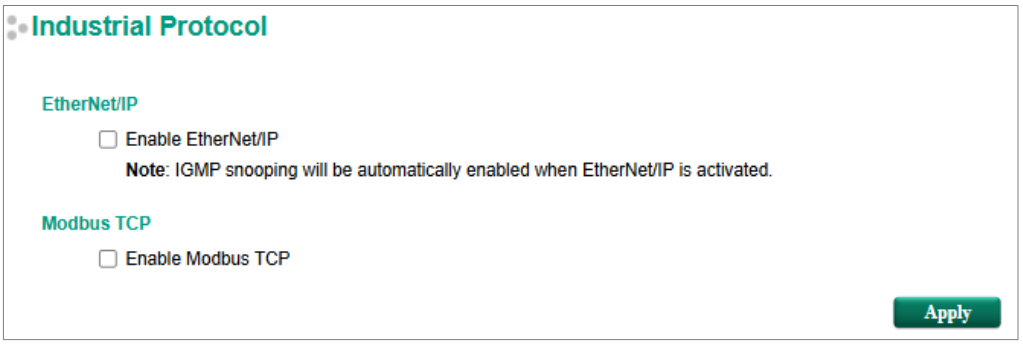
SNMP Trap/Inform Summary

The table below shows the SNMP protocol version applicable to PT-G7728/PT-G7828 SNMP trap/inform services and the associated authentication and authorization settings that can be configured via web console. Note that the SNMP protocol version set in the agent (switch) is only downward compatible with the protocol version set in the trap/inform services. Therefore, SNMP protocol version v1, v2c does not allow Trap/Inform v3.

SNMP Protocol Version	Available Trap Mode	Authentication for Trap/Inform	Authorization for Trap/Inform	Message
SNMP v1, v2c, v3	Trap v1	No	No	Plain text
	Trap v2c	No	No	Plain text
	Inform v2c	No	No	Plain text
Or	Trap v3	MD5 or SHA authentication in Trap/Inform recipient section	Data encryption key in Trap/Inform recipient section	Encrypted
SNMP v3	Inform v3	MD5 or SHA authentication in Trap/Inform recipient section	Data encryption key in Trap/Inform recipient section	Encrypted
SNMP v1, v2c	Trap v1	No	No	Plain text
	Trap v2c	No	No	Plain text
	Inform v2c	No	No	Plain text

Industrial Protocols

The Moxa switch supports two industrial protocols, EtherNet/IP and Modbus TCP. Both protocols can be enabled or disabled by checking the appropriate checkbox. Modbus TCP is enabled by default and the other option is disabled.



NOTE

1. IGMP Snooping and IGMP Query functions will be enabled automatically to be properly integrated in Rockwell systems for multicast Implicit (I/O) Messaging for efficient EtherNet/IP communication.
2. EtherNet/IP cannot be enabled while IGMP snooping is disabled due to the VLAN settings.

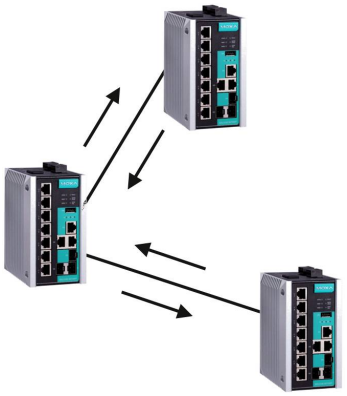
Diagnostics

The Moxa switch provides three important tools for administrators to diagnose network systems: LLDP, Ping, and Port Mirror.

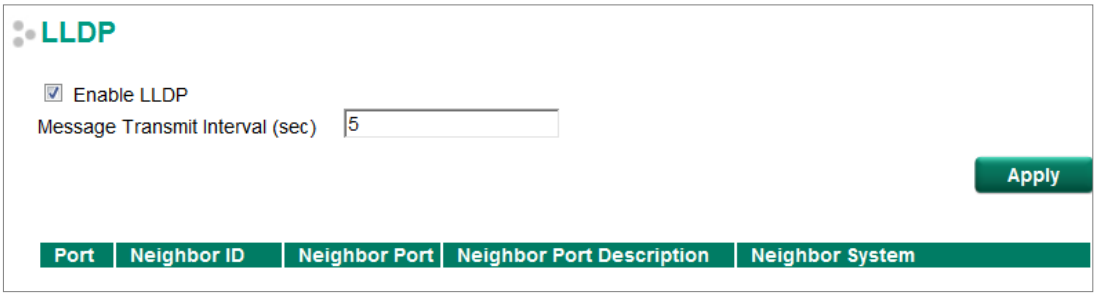
LLDP

Overview

LLDP is an OSI Layer 2 protocol defined by IEEE 802.11AB. LLDP standardizes the self-identification advertisement method, and allows each networking device, such as a Moxa managed switch, 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 configuration, and with SNMP, this information can be transferred to Moxa's MXview for auto-topology and network visualization.
From the switch'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 to automatically display the network's topology and system setup details, such as VLAN and Trunking, for the entire network.



Configuring LLDP Settings



General Settings

LLDP

Setting	Description	Factory Default
Enable or Disable	Enables or disables the LLDP function.	Enable

Message Transmit Interval

Setting	Description	Factory Default
5 to 32768 sec.	Sets the transmit interval of LLDP messages, in seconds.	5 (seconds)

LLDP Table

The LLDP Table displays the following information:

Port	The port number that connects to the neighbor device.
Neighbor ID	A unique entity (typically the MAC address) that identifies a neighbor device.
Neighbor Port	The port number of the neighbor device.
Neighbor Port Description	A textual description of the neighbor device's interface.

Neighbor System	Hostname of the neighbor device.

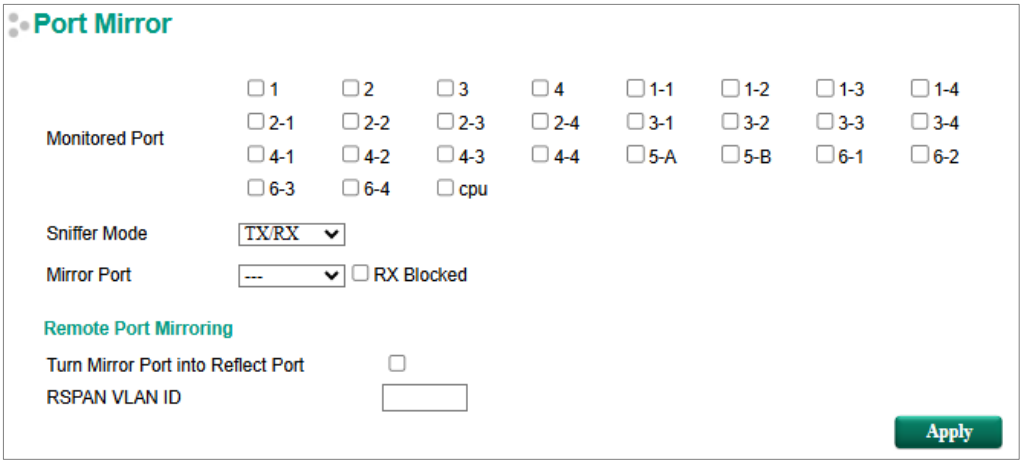
Ping

The **Ping** function uses the ping command to give users a simple but powerful tool for troubleshooting network problems. The function's most unique feature is that even though the ping command is entered from the user's PC keyboard, the actual ping command originates from the Moxa switch itself. In this way, the user can essentially sit on top of the Moxa switch and send ping commands out through its ports.

To use the Ping function, type in the desired IP address, and then press **Enter** from the Console utility, or click **Ping** when using the Web Browser interface.

Port Mirroring

The **Port Mirroring** function can be used to monitor data being transmitted through a specific port. This is done by setting up another port (the mirror port) to receive the same data being transmitted from, or both to and from, the port under observation. Using a mirror port allows the network administrator to **sniff** the observed port to keep tabs on network activity.



Port Mirroring Settings

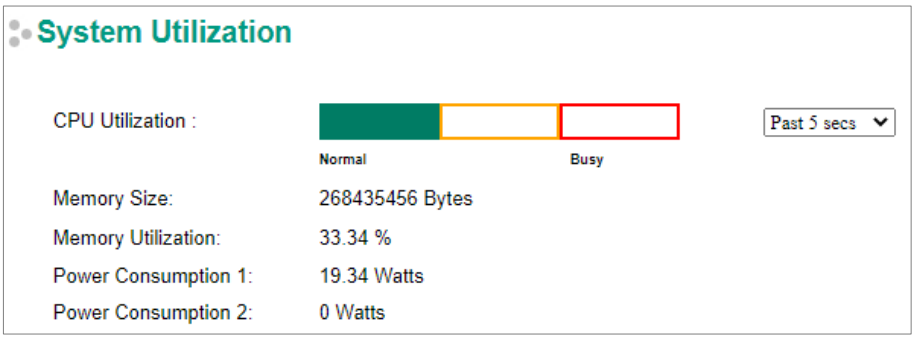
Setting	Description
Monitored Port	Select which ports will be monitored.
Sniffer Mode	Select one of the following three watch direction options: • **RX:** Select this option to monitor only those data packets coming into the Moxa switch's port. • **TX:** Select this option to monitor only those data packets being sent out through the Moxa switch's port. • **TX/RX:** Select this option to monitor data packets both coming into, and being sent out through, the Moxa switch's port.
Mirror Port	Select the number of the port that will be used to monitor the activity of the monitored port.
RX Blocked	When enabled, Mirror Port will receive monitored port packets only.
Turn Mirror Port into Reflect Port	Check to turn the specified mirror port into reflect port.
RSPAN VLAN ID	Specify the VLAN ID to use as the RSPAN VLAN ID. Only existing VLAN IDs can be selected.

Monitoring

You can monitor statistics in real time from the Moxa switch's web console and serial console.

System Utilization

The System Utilization page displays the status of system resources. Monitor this information to easily understand the status of the switch.



CPU Utilization

Setting	Description	Factory Default
Read-only	The CPU usage volume in the past 5 seconds, 30 seconds, and 5 minutes.	Past 5 secs

Memory Size

Setting	Description	Factory Default
Read-only	The switch's current free memory.	None

Memory Utilization

Setting	Description	Factory Default
Read-only	The switch's current memory utilization.	None

Power Consumption 1

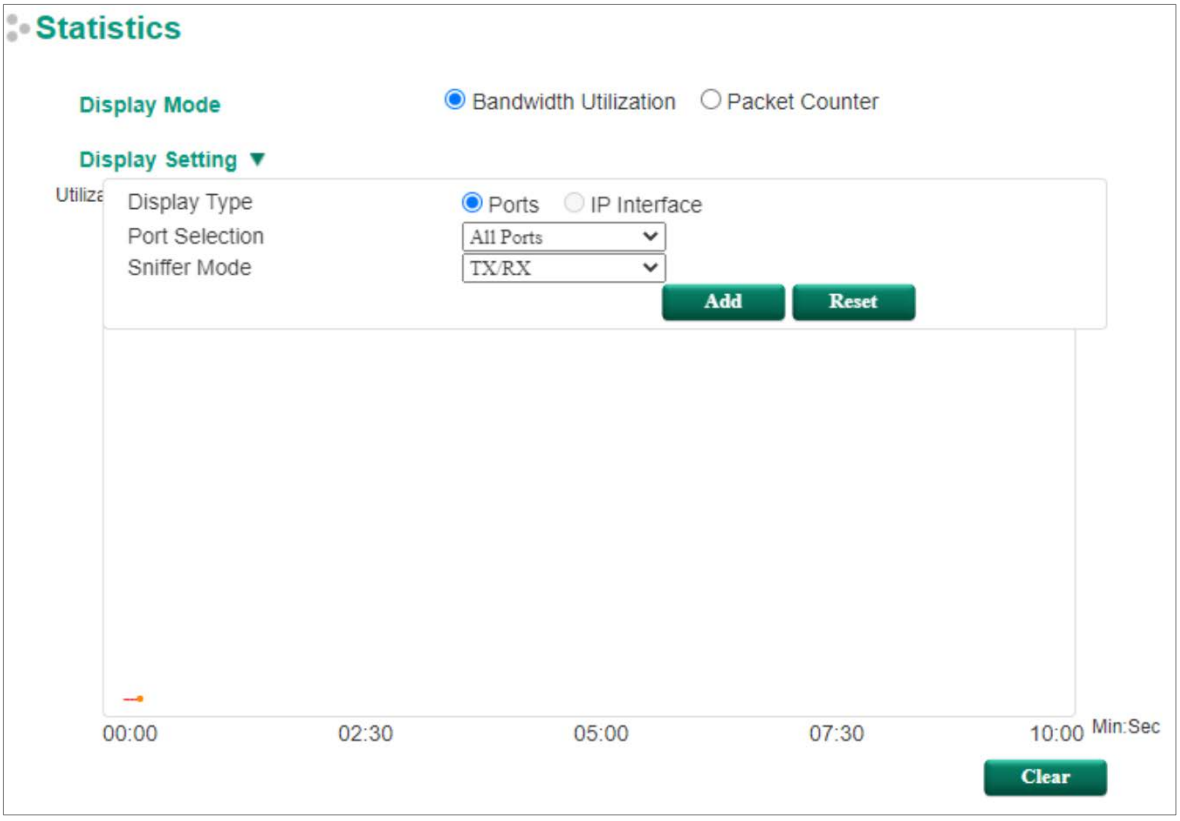
Setting	Description	Factory Default
Read-only	The current PWR1 power consumption information. The measurement tolerance is 7% (Unit: watts.).	None

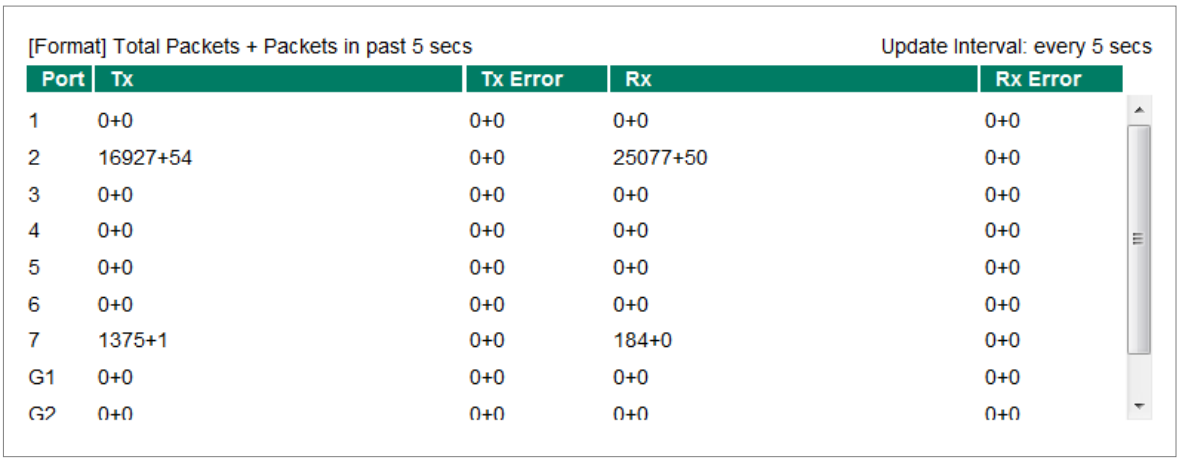
Power Consumption 2

Setting	Description	Factory Default
Read-only	The current PWR2 power consumption information. The measurement tolerance is 7% (Unit: watts.).	None

Statistics

Access the Monitor by selecting **Monitoring** from the left selection bar. Monitor by System allows the user to view a graph that shows the combined data transmission activity of all of the Moxa switch's 18 ports. Click one of the four options—**Total Packets, TX Packets, RX Packets,** or **Error Packets**—to view transmission activity of specific types of packets. Recall that TX Packets are packets sent out from the Moxa switch, RX Packets are packets received from connected devices, and Error Packets are packets that did not pass TCP/IP's error checking algorithm. The Total Packets option displays a graph that combines TX, RX, and TX Error, RX Error Packet activity. The graph displays data transmission activity by showing **Packets/s** (i.e., packets per second, or pps) versus sec. (seconds). In fact, three curves are displayed on the same graph: **Uni-cast** packets (in red color), **Multi-cast** packets (in green color), and **Broad-cast** packets (in blue color). The graph is updated every few seconds, allowing the user to analyze data transmission activity in real-time.



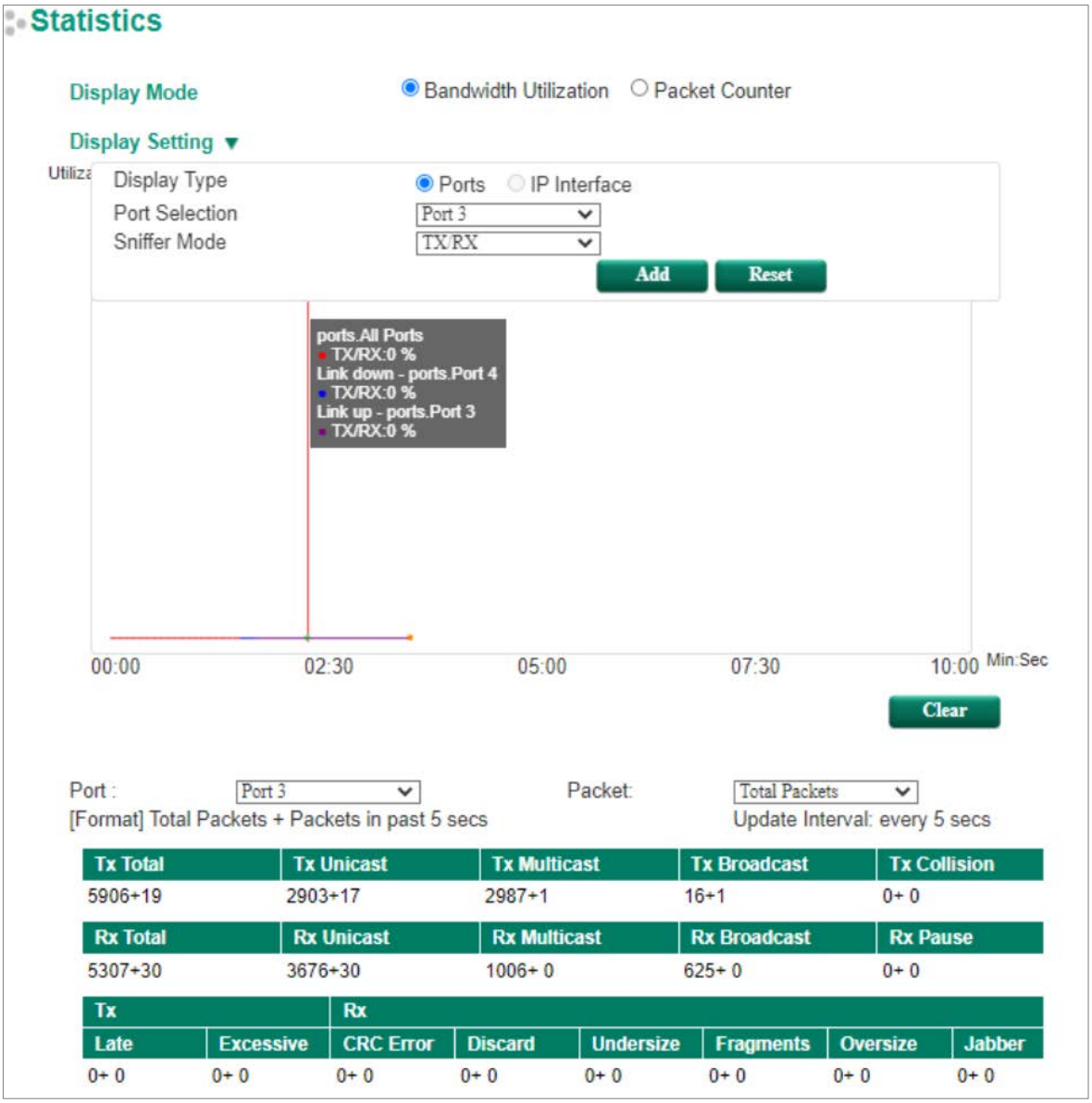


[Format] Total Packets + Packets in past 5 secs — Update Interval: every 5 secs

Port	Tx	Tx Error	Rx	Rx Error
1	0+0	0+0	0+0	0+0
2	16927+54	0+0	25077+50	0+0
3	0+0	0+0	0+0	0+0
4	0+0	0+0	0+0	0+0
5	0+0	0+0	0+0	0+0
6	0+0	0+0	0+0	0+0
7	1375+1	0+0	184+0	0+0
G1	0+0	0+0	0+0	0+0
G2	0+0	0+0	0+0	0+0

Monitor by Port

Access the Monitor by Port function by selecting **FE or GE Ports** or **Port *i***, in which **i = 1, 2, ..., G2**, from the left pull-down list. The **Port *i*** options are identical to the Monitor by System function discussed above, in that users can view graphs that show All Packets, TX Packets, RX Packets, or Error Packets activity, but in this case, only for an individual port. The **All Ports** option is essentially a graphical display of the individual port activity that can be viewed with the Console Monitor function discussed above. The All Ports option shows three vertical bars for each port. The height of the bar represents **Packets/s** for the type of packet, at the instant the bar is being viewed. That is, as time progresses, the height of the bar moves up or down so that the user can view the change in the rate of packet transmission. The blue colored bar shows **Uni-cast** packets, the red colored bar shows **Multi-cast** packets, and the orange colored bar shows **Broad-cast** packets. The graph is updated every few seconds, allowing the user to analyze data transmission activity in real-time.

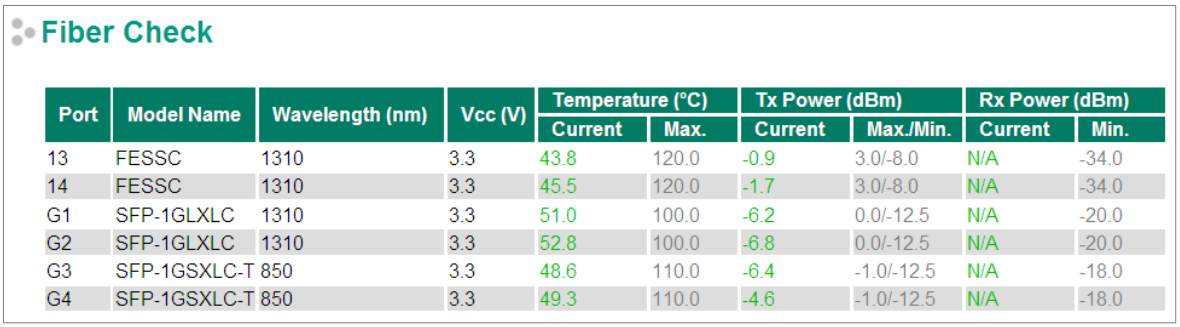


Fiber Digital Diagnostics Monitoring (Fiber Check)

Optical fiber is commonly used for long distance data transmission. However, when link issues occur, it is very costly to troubleshoot fiber cables and fiber transceivers at remote sites. To solve this problem, Moxa industrial Ethernet switches provide digital diagnostics and monitoring (DDM) functions on Moxa SFP's and/or fixed type (multi-mode SC/ST and single-mode SC connectors) optical fiber links and allow users to measure optical parameters and its performance from a central site. This function can greatly facilitate the troubleshooting process for optical fiber links and reduce costs for onsite debugging.

Fiber Check

Fiber Check is used to diagnose the link status of fiber connectors, including SFP and fixed type (Multi-mode SC/ST & Single-mode SC) connectors. Monitor the temperature, TX/RX power, and other parameters on fiber ports to determine if the ports are working properly. Enable the trap, email warning, and/or relay warning functions on the System Event Settings page to receive an alarm or relay if one of the fiber ports exceeds the threshold for that port.



Parameter	Description
Port	Switch port number with a fiber connection.
Model Name	Moxa SFP/fixed type fiber model name.
Wavelength (nm)	Wavelength of the fiber connection.
Vcc (V)	Voltage supply to the fiber connection.
Temperature (°C) – Current	Fiber connection current temperature.
Temperature (°C) – Max.	Fiber connection Max. temperature threshold.
Tx power (dBm) – Current	The current amount of light being transmitted into the fiber optic cable.
Tx power (dBm) – Max.	The Max. threshold of light being transmitted into the fiber optic cable.
Tx power (dBm) - Min.	The Min. threshold of light being transmitted into the fiber optic cable.
Rx power (dBm) – Current	The current amount of light being received from the fiber optic cable.
Rx power (dBm) – Max.	The Max. threshold of light being received from the fiber optic cable.

Fiber Check Threshold Values

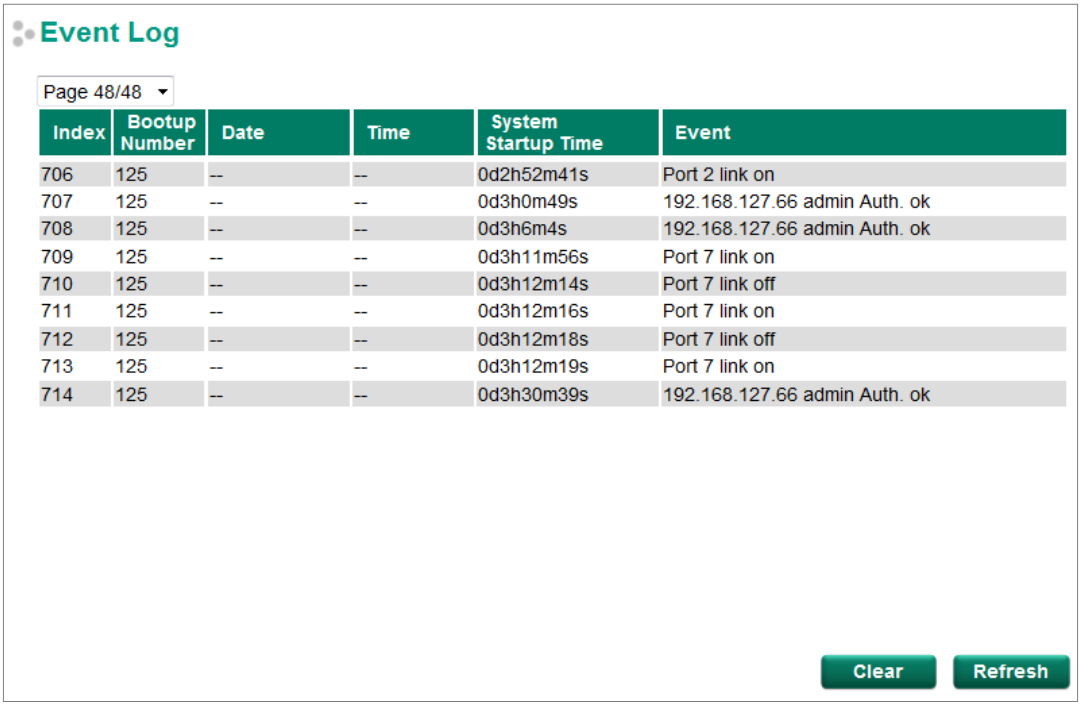
Model Name	Temperature Threshold (°C)	Tx Power (Max./Min.) (dBm)	Rx Power (Min.) (dBm)
FEMST	120	-14.0/-20.0	-35.0
FEMSC	120	-14.0/-20.0	-35.0
FESSC	120	0.0/-5.0	-37.0
SFP-1FEMLC-T	120	-8.0/-18.0	-35.0
SFP-1FESLC-T	120	0.0/-5.0	-37.0
SFP-1FELLC-T	120	0.0/-5.0	-37.0
SFP-1GSXLC-T	110	-4.0/-9.5	-21.0
SFP-1GLSXLC-T	120	-1.0/-9.0	-22.0
SFP-1GLXLC-T	120	-3.0/-9.0	-24.0
SFP-1GLHLC-T	120	-3.0/-8.0	-26.0
SFP-1GLHXLC-T	120	3.0/-4.0	-27.0
SFP-1GZXLC-T	120	5.0/0.0	-27.0
SFP-1G10ALC-T	120	-3.0/-9.0	-24.0
SFP-1G10BLC-T	120	-3.0/-9.0	-24.0

Model Name	Temperature Threshold (°C)	Tx Power (Max./Min.) (dBm)	Rx Power (Min.) (dBm)
SFP-1G20ALC-T	120	-2.0/-8.0	-26.0
SFP-1G20BLC-T	120	-2.0/-8.0	-26.0
SFP-1G40ALC-T	120	2.0/-3.0	-26.0
SFP-1G40BLC-T	120	2.0/-3.0	-26.0
SFP-1GSXLC	100	-4.0/-9.5	-21.0
SFP-1GLSXLC	100	-1.0/-9.0	-22.0
SFP-1GLXLC	100	-3.0/-9.0	-24.0
SFP-1GLHLC	100	-3.0/-8.0	-26.0
SFP-1GLHXLC	100	3.0/-4.0	-27.0
SFP-1GZXLC	100	5.0/0.0	-27.0
SFP-1GEZXLC	100	5.0/0.0	-33.0
SFP-1GEZXLC-120	100	-3.0/-2.0	-36.0
SFP-1G10ALC	100	-3.0/-9.0	-24.0
SFP-1G10BLC	100	-3.0/-9.0	-24.0
SFP-1G20ALC	100	-2.0/-8.0	-26.0
SFP-1G20BLC	100	-2.0/-8.0	-26.0
SFP-1G40ALC	100	2.0/-3.0	-26.0
SFP-1G40BLC	100	2.0/-3.0	-26.0

NOTE

Certain tolerances exist between real data and measured data.

Event Log



The Event Log Table displays the following information:

Index	Event index assigned to identify the event sequence.
Bootup Number	This field shows how many times the Moxa switch has been rebooted or cold started.
Date	The date is updated based on how the current date is set in the Basic Setting page.
Time	The time is updated based on how the current time is set in the Basic Setting page.
System Startup Time	The system startup time related to this event.
Event	Events that have occurred.

NOTE

The following events will be recorded into the Moxa switch's Event Log Table:

- Cold start
- Warm start
- Configuration change activated
- Power 1/2 transition (Off (On), Power 1/2 transition (On (Off))
- Authentication fail
- Topology changed
- Master setting is mismatched
- Port traffic overload
- dot1x Auth Fail
- Port link off/on
- The Grandmaster Clock has changed
- The PTP synchronization status has changed
- The external power supply for PoE transition: Off to On or On to Off

Tracking Function

This function is only available on the PT-G7828.

The tracking function allows users to monitor the destined interface or the port availability. The tracking function is a mechanism that is designed to complement defective current protocols, which provides better redundancy for the overall system.

The device will continuously monitor the status of the tracked interface or port and transfer these status changes into the action. e.g., enable the port, decrease the priority of the VRRP interface and activate the routing interface.

Moxa's devices provide 3 types of tracking functions: Interface Tracking, Ping Tracking, and Logic Tracking. A maximum of 64 tracking entries can be supported.

Interface Tracking

Track the status of each port or layer 3 interfaces.

Ping Tracking

Track the status of certain remote devices by IP address.

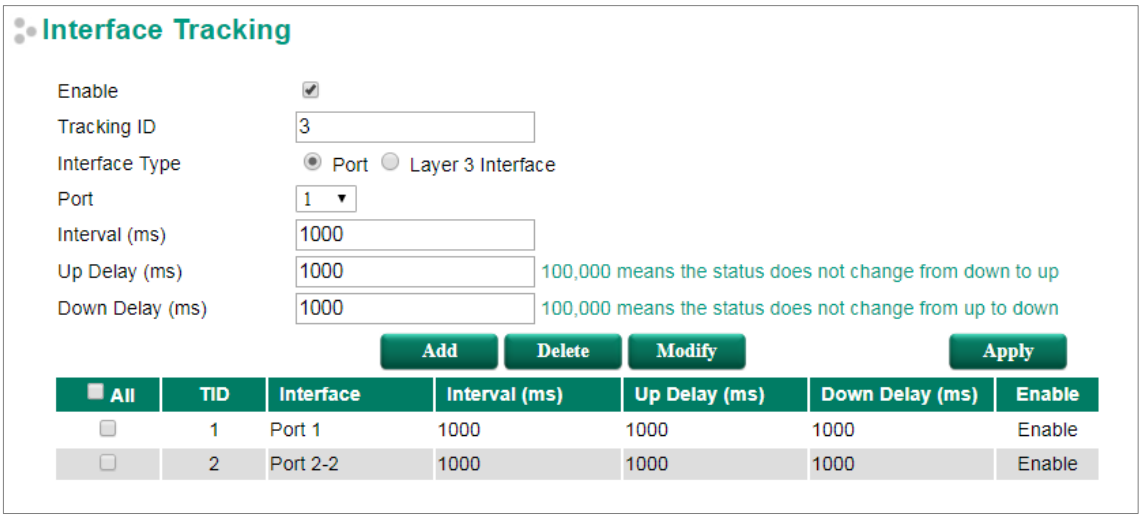
Logic Tracking

This function is a logic flow that can combine interface tracking, ping tracking, and the logic tracking item with AND or OR logic.

Tracking Function

Setting	Description	Factory default
Enable/Disable	Enable or disable the tracking feature	Disabled

Interface Tracking



Enable

Setting	Description	Factory default
Enable/Disable	Enable or disable the interface tracking entry	Enabled

Tracking ID

The tracking ID is the ID of the interface tracking entry. The tracking ID is unique in interface tracking, ping tracking, and logical tracking.

Interface Type

Setting	Description
Port	Track the port of the device
Layer 3 Interface	Track the interface of the device

Port/VLAN

Choose the Port or VLAN that will be monitored.

Interval

Setting	Description	Factory default
Range: 100 to 100,000 ms	The frequency to check the status of the monitored port or interface.	1000

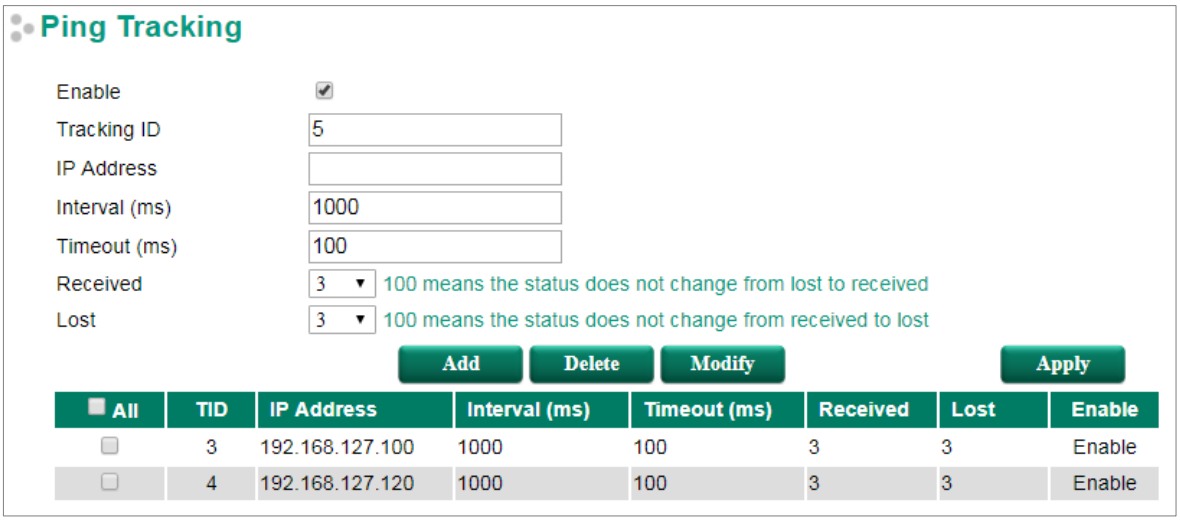
Up delay

Setting	Description	Factory default
Range: 0 to 100,000 ms	The status will change from down to up once the status of the monitored port or interface exceeds the delay time. If 100,000 ms is entered, the status will not change to up even if the monitored port/interface is up.	1000

Down delay

Setting	Description	Factory default
Range: 0 to 100,000 ms	The status will change from up to down once the status of the monitored port or interface is less than the delay time. If 100,000 ms is entered, the status will not change to down even if the monitored port/interface is down.	1000

Ping Tracking



Enable

Setting	Description	Factory default
Enable/Disable	Enable or disable the interface tracking feature.	Enabled

Tracking ID

This is the ID of the ping tracking entry. The tracking ID is unique in interface tracking, ping tracking, and logical tracking.

IP address

The IP address that the user wants to monitor.

Interval

Setting	Description	Factory default
Range: 100 to 100,000 ms	The frequency to check the status of the monitored IP address.	1000

Timeout

Setting	Description	Factory default
Range: 1 to 100,000 ms	Specific period of time to determine that the ping request has no response.	100

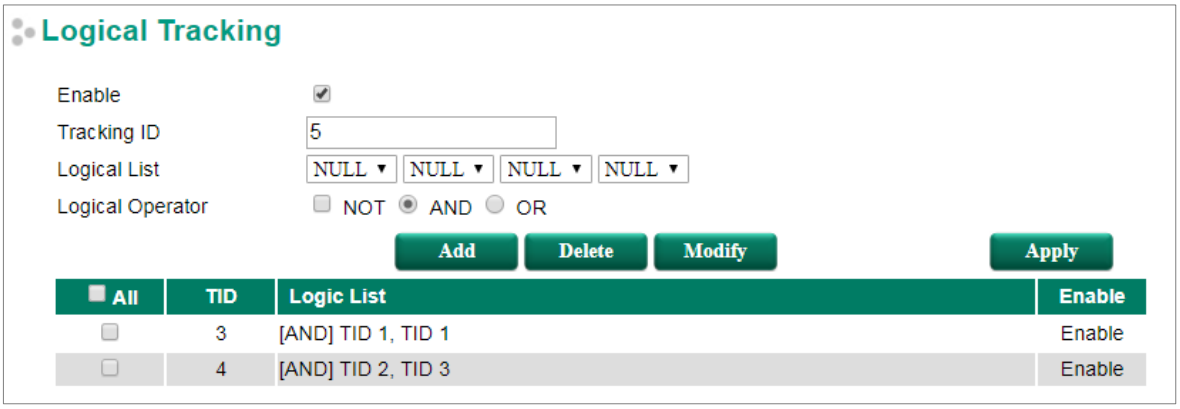
Received

Setting	Description	Factory default
Range: 1 to 100 times	The status will change from down to up once the ping replies are greater or equal to the count. If 100 times is entered, the status will not change to up even if the condition is reached.	3

Lost

Setting	Description	Factory default
Range: 1 to 100 times	The status will change from up to down once lost the ping replies are greater or equal to the count. If 100 times is entered, the status will not change to down even if the condition is reached.	3

Logical Tracking



Enable

Setting	Description	Factory default
Enable/Disable	Enable or disable the interface tracking feature.	Disabled

Tracking ID

This is the ID of the logical tracking entry. The tracking ID is unique in interface tracking, ping tracking, and logical tracking.

Logic List

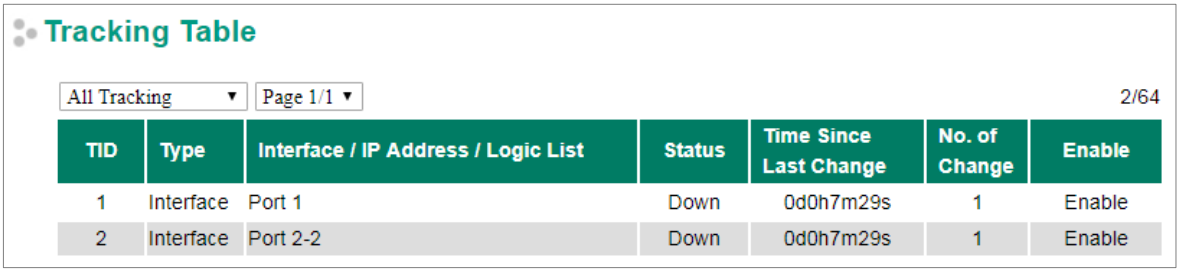
Choose the Tracking ID that the user wants to put in the logic list; up to 4 tracking IDs are allowed.

Logic Operator

NOT is used to reverse the status of the logic tracking entry. If AND is chosen, then the status of the logical tracking entry will be up when all the status of the tracking entries are up. If OR is chosen, then any status of tracking id entries is up, the status of the logical tracking entry will be up.

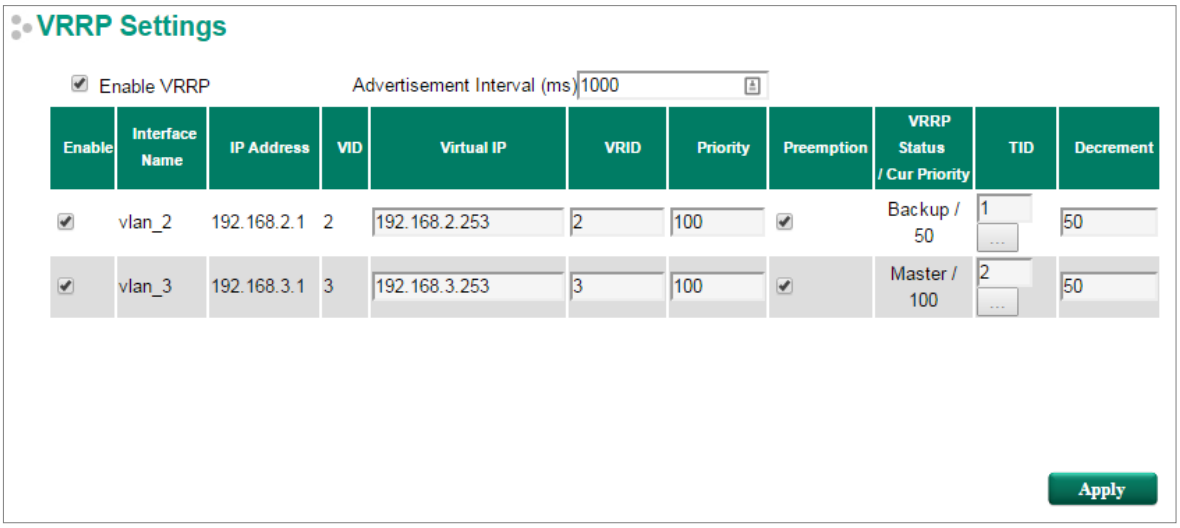
Tracking Table

This table shows all of the information of the tracking entries.



VRRP and Static Routing can be modified by the triggered tracking entry.

VRRP Settings



For detailed VRRP settings, refer to the VRRP section in the *Layer 3 Routing User Manual*.

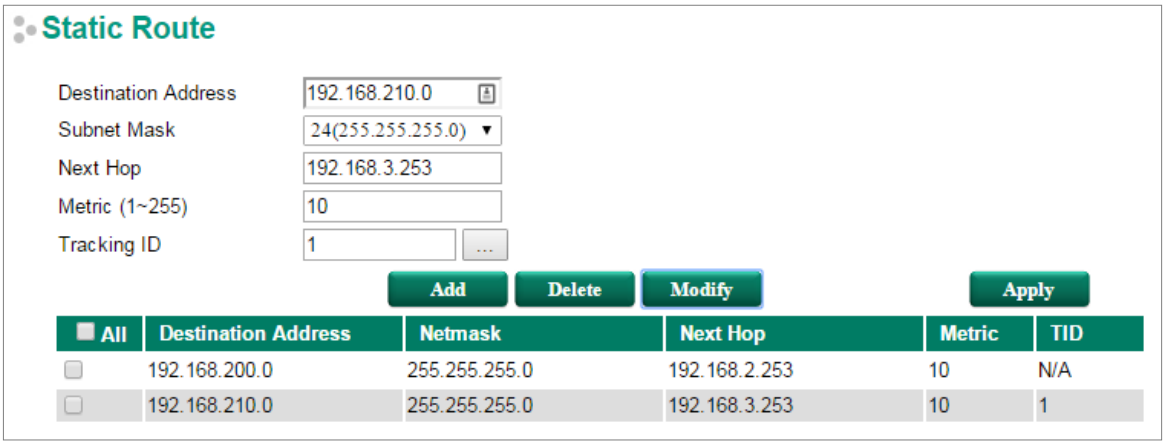
If the VRRP entry does not bind any tracking entry or the status of the bound tracking entry is "up", the running VRRP priority would be equal to the VRRP priority configuration. If the VRRP entry binds a tracking entry and the status of the bound tracking entry is "down", then the running VRRP priority would be (VRRP priority configuration minus decrement).

TID: The tracking entry ID can affect the VRRP entry.

Decrement

Settings	Description	Factory Default
Decrement (Range: 0 to 255)	This is the amount that will be reduced from the priority of the VRRP entry once the status of TID entry is down	0 (The value cannot be greater than the VRRP priority)

Static Route Settings

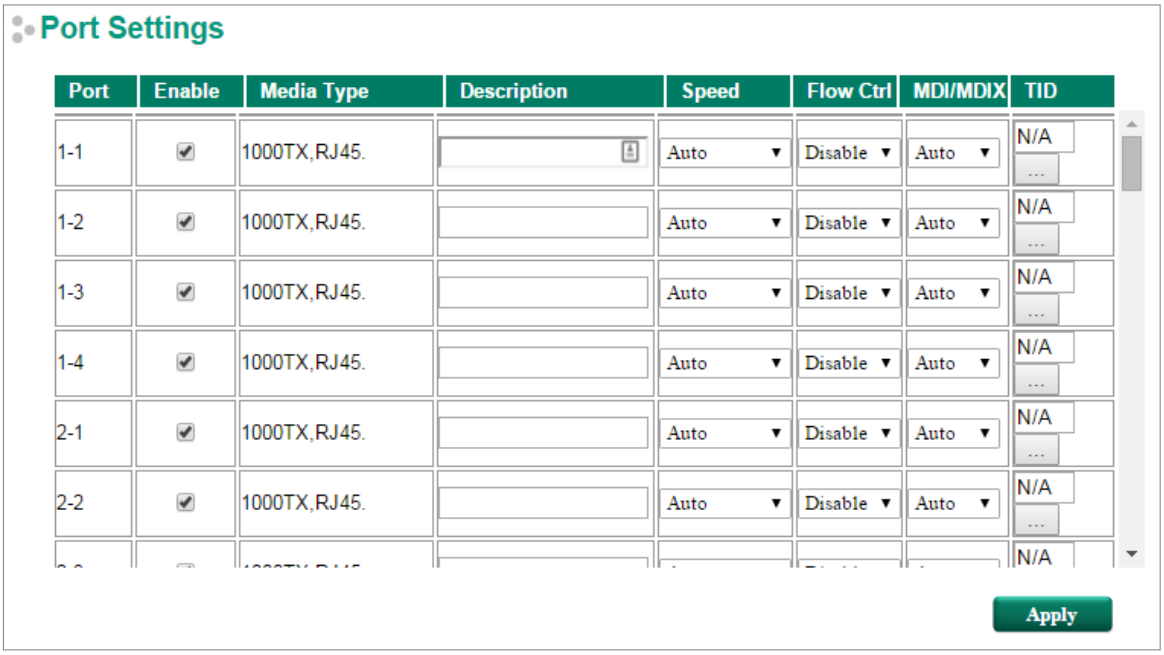


For detailed Static Route settings, refer to the *Static Routing* section in the *Layer 3 Routing User Manual*.

If the status of related TID entry is up, the routing address will remain at the routing table. If the status of TID entry is down, the routing address will be erased from the routing table.

TID: The tracking entry ID can affect the Static Route.

Port Settings



For detailed information, refer to Port Settings.

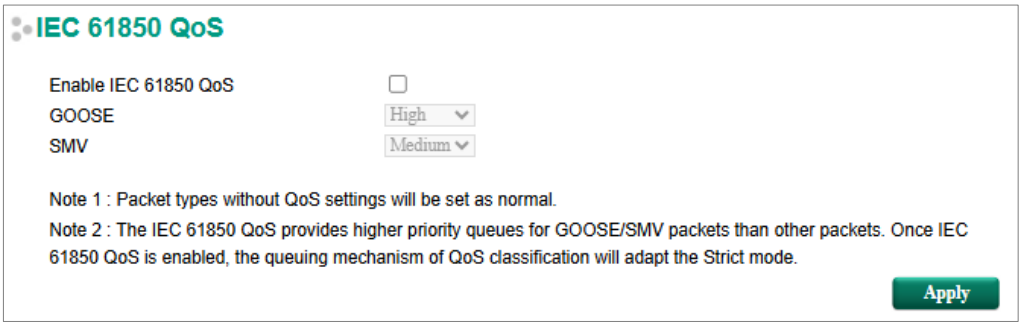
If the status of related TID entry is up, the port will be enabled. If the status of TID entry is down, the port will be disabled. This can be observed in the page port status.

TID: The tracking entry ID can affect the port settings.

Substation

IEC 61850 QoS

GOOSE (Generic Object Oriented Substation Events) and SMV (Sampled Measured Values) play a key role in IEC 61850 substations. Once IEC 61850 QoS (Quality of Service) has been enabled, users can assign queuing priority for GOOSE and SMV packets to ensure they are always processed with a higher priority.



Enable IEC 61850 QoS

Setting	Description	Factory Default
Enable/Disable IEC 61850 QoS	Enable or disable IEC 61850 QoS	Disable

GOOSE

Setting	Description	Factory Default
High, Medium, Normal, Low	The priority of the GOOSE message	High

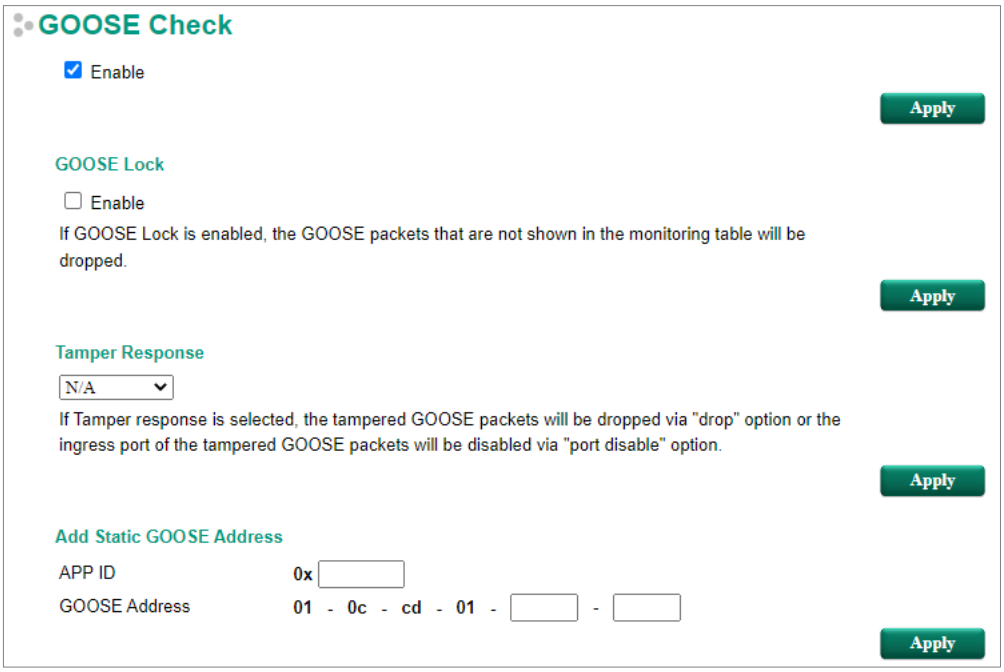
SMV

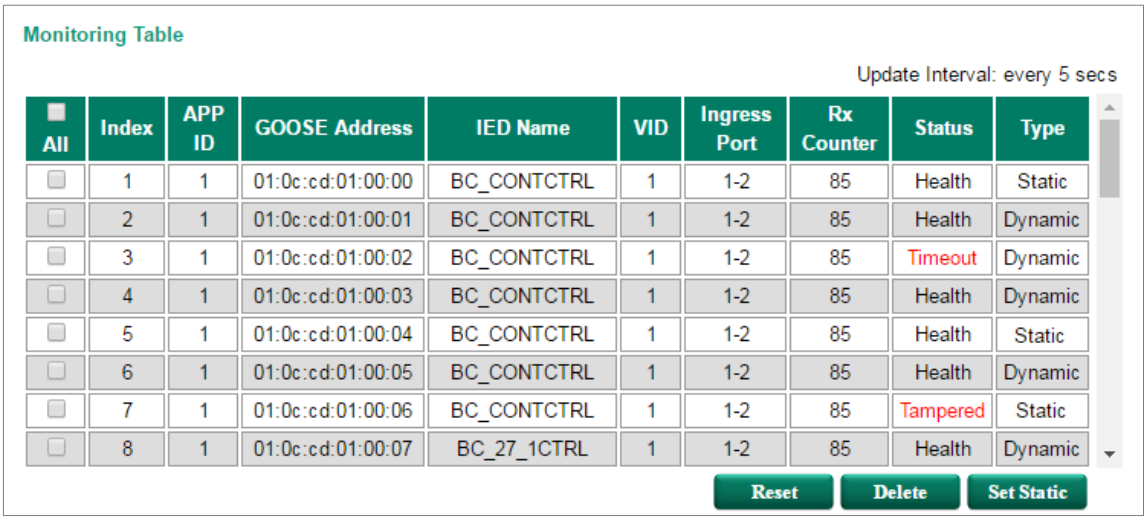
Setting	Description	Factory Default
High, Medium, Normal, Low	The priority of the GOOSE message	Medium

GOOSE Check

The switch can snoop the GOOSE messages passing through the switch and show the communication status of GOOSE messages on this page. The basic function will allow users to monitor if the GOOSE packets recorded in the monitoring list are consistent with the registered and valid GOOSE stream transmitted over the network. The user can manually change the GOOSE message entry type to static in order to keep a record of it in the monitoring list, even if the device reboots or reaches the maximum number of messages that can be stored in the GOOSE Check page. The advanced function "GOOSE Lock", which is similar to GOOSE ACL (Access control list), will lock down the white-listing GOOSE packets shown in the monitoring table, and protect the network from unregistered or invalid GOOSE packets caused by incorrect operation. The advanced function also offers responses to GOOSE intrusion actions. If tampered GOOSE packets are detected, further responses such as dropping the tampered GOOSE packets can be selected to keep the GOOSE communications intact.

GOOSE Check supports up to a maximum of 100 GOOSE packets.





Enable GOOSE Check

Setting	Description	Factory Default
Enable/Disable GOOSE Check	Enable or disable GOOSE Check	Enable

Advanced function

Enable GOOSE lock

Setting	Description	Factory default
Enable/Disable GOOSE Lock	When GOOSE Lock is enabled, the switch will not learn and forward any other new GOOSE packets except the GOOSE stream shown in the monitoring table. The function assists the GOOSE configuration integrity. NOTE: Ensure the monitoring table has recorded all desirable GOOSE streams subscribed in the IEDs before the function is enabled.	Disable

Tamper response

Setting	Description	Factory default
Drop	If a tampering event is detected, the switch will drop the tampered packets	Disable
Port disable	If a tampering event is detected, the switch will disable the tampered Ethernet port. Note: Disabling the tampered port may affect the network communication of other protocols. Verify the network topology before disabling a port.	Disable

Add Static GOOSE Address

APP ID

Setting	Description
0000 to ffff (Hex.)	GOOSE application identifier

GOOSE Address

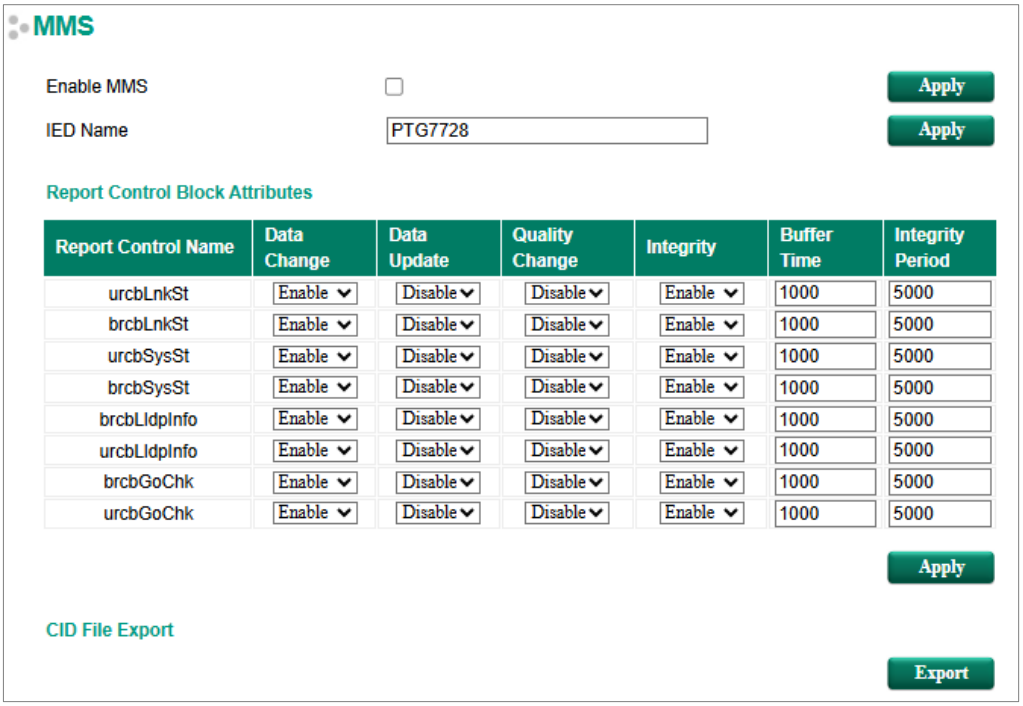
Setting	Description
01-0C-CD-01-00-00 to 01-0C-CD-01-01-ff	Destination MAC address of ingress GOOSE message

Monitoring Table

Item	Description
APP ID	GOOSE application identifier of ingress GOOSE message
GOOSE Address	Destination MAC address of ingress GOOSE message
IED Name	IED name of ingress GOOSE message
VID	VLAN ID of ingress GOOSE message
Ingress Port	The ingress port of GOOSE message
Rx Counter	Packet counter of ingress GOOSE message
Status	The status of GOOSE message communication. Health: The communication status of the GOOSE message is normal. Timeout: The communication status of the GOOSE message is abnormal. This GOOSE message does not pass through the switch at the correct time. Tampered: The GOOSE message has been sent from an abnormal port. Also be aware that the packet may have been tampered with.
Type	The type of GOOSE communication status entry Static: The GOOSE message is selected to be on the GOOSE message communication monitoring list. The static type of GOOSE packet will not be erased once the port link is down, and the device is turned off. Dynamic: The GOOSE message is discovered by the switch automatically. The dynamic type of GOOSE packet will be erased once the port link is down, and the device is turned off.
Reset	Reset the Rx counter and the status of the selected GOOSE messages
Delete	Delete selected GOOSE message
Set Static	Set the communication status of the GOOSE message to static entry

MMS Server

As Moxa's PT-G7728/G7828 Series switches support the MMS protocol, MMS client (e.g., SCADA) is able to receive the data objects sent from the switch (MMS server), just as the SCADA does for IEDs. A built-in MMS (Manufacturing Message Specification) server allows Ethernet switches to be controlled, monitored, and managed via a Power SCADA system without the need for any additional network management software.



Enable MMS

Setting	Description	Factory Default
Enable/Disable MMS	Enable or disable the MMS server	Enable

IED Name

Setting	Description	Factory Default
Max. 20 characters	This option is used to change the device name for MMS client. The IED Name can only include these characters, a-z/A-Z/0-9/_/	PT-G7728

Block Attributes

Reporting allows a server to send data based on events and without explicit requests from the client. What data is sent and the events that cause reports are configured through report control blocks (RCB). The standard distinguishes between two types of reporting: buffered reporting and unbuffered reporting. With buffered reporting, the reports are buffered by the server in case a connection to the client is interrupted. This way reports can be sent after the client has connected again. Buffered reporting is configured through buffered report control blocks (BRCB). Unbuffered reporting is configured through unbuffered report control blocks (URCB).

PT-G7728/G7828 Series provides the Report Control Name listed below for MMS client:

- 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
- brcbLldpInfo: Buffered Report Control Block Link Layer Discovery Protocol Information
- urcbLldpInfo: Unbuffered Report Control Block Link Layer Discovery Protocol Information
- brcbGoChk: Buffered Report Control Block GOOSE Check
- urcbGoChk: Unbuffered Report Control Block GOOSE Check

Modify the attributes details, and then click **Apply** to save the changes.

Data Change

Setting	Description	Factory Default
Enable/Disable	Enable or disable Data Change (dchg). Data-change relates to a change in a value of a Data Attribute representing the process-related value of the data object.	Enable

Data Update

Setting	Description	Factory Default
Enable/Disable	Enable or disable Data Update (dupd). Data-update relates to a freeze event in a value of a Data Attribute representing a freeze value of the data object or to an event triggered by updating the value of a Data Attribute.	Disabled

Quality Change

Setting	Description	Factory Default
Enable/Disable	Enable or disable Quality Change (qchg). Quality-change relates to a change in the quality value of a Data Attribute.	Disabled

Integrity

Setting	Description	Factory Default
Enable/Disable	Enable or disable integrity report generation. When integrity reports are enabled, the BRCB shall be notified each time the value of the time as specified in the IntgPd has expired. The BRCB shall then build a report with the values of all members of the referenced data set.	Disabled

Buffer Time

Setting	Description	Factory Default
1 to 4294967295	The attribute Buffer Time (BufTm) shall specify the time interval in milliseconds for the buffering of internal notifications caused by data-change (dchg), quality-change (qchg), or data update (dupd) by the BRCB for inclusion into a single report.	1000

Integrity Period

Setting	Description	Factory Default
1 to 4294967295	If Integrity is set to enabled, the attribute Integrity Period (IntgPd) indicates the period in milliseconds used for logging caused by integrity scans.	5000

CID File Export

IEC 61850-6 defines 6 types of files: SSD, ICD, SCD, CID, IID, and SED. The Configured IED Description (CID) is generated by the MMS server. It contains a mandatory communication section of the addressed IED.

Click **Export** to download the Configured IED Description (CID) file.

4. Hardening Guide

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. Follow the instructions in the Quick Installation Guide included in the package to ensure the device is installed 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. 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. MX-NOS V5 - User Manual 706 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. Refer to Trusted Access section 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_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_RSA_WITH_AES_128_GCM_SHA256	RSA	RSA	AES128	SHA256
TLS_RSA_WITH_AES_256_GCM_SHA384	RSA	RSA	AES256	SHA384

   b. TLS v1.3

Cipher suite name	Key exchange	Authentication	Encryption	Hash function
TLS_AKE_WITH_AES_128_GCM_SHA256	ECDH	ECDH	AES128	SHA256
TLS_AKE_WITH_AES_256_GCM_SHA384	ECDH	ECDH	AES256	SHA384

2. Below is a list of the recommended secure browsers that support TLS v1.3 or higher:

Browser	Version
Microsoft Edge latest version	All
Microsoft Internet Explorer	v11 or above
Mozilla Firefox	v63 or above
Google Chrome	v80 or above
Apple Safari	v13 or above

   Reference: https://support.globalsign.com/ssl/general-ssl/tls-protocolcompatibility#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. Refer to Event Logs for more information.

   b. Syslog: this device supports syslog, and advanced secure TLS-based syslog for centralized SIEM integration. 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. 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 MX-NOS V5 - User Manual 709 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. 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. 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. Refer to SSH & SSL for more information.

8. A list of various protocols and their associated port numbers used for all external interfaces is given in the following tables:

   a. Protocol:TCP

Service Type	Port Number	Default State	Port can be modified
HTTP	80	Enabled	Y
HTTPS	443	Enabled	Y
Telnet	23	Enabled	Y
SSH	22	Enabled	Y
Moxa Service	4000	Enabled	N
Moxa Service (Encrypted)	443	Enabled	N
MMS	102	Disabled	N
Modbus TCP	502	Disabled	N

   b. Protocol: UDP

Service Type	Port Number	Default State	Port can be modified
SNMP	161	Disabled	N
DHCP	67	Disabled	N
NTP	123	Disabled	N
Moxa Service	4000	Enabled	N
Moxa Service (Encrypted)	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, go to: https://www.moxa.com/en/support/product-support/security-advisory

Decommissioning

To avoid disclosing sensitive information such as account passwords and certificates, reset the system settings to factory default before decommissioning the device or send it back to the Moxa RMA Service team.

A. MIB Groups

The Moxa switch comes with built-in SNMP (Simple Network Management Protocol) agent software that supports cold/warm start trap, line up/down trap, and RFC 1213 MIB-II.

The standard MIB groups that the Moxa switch supports are as follows:

MIB II.1—System Group

sysORTable

MIB II.2—Interfaces Group

ifTable

MIB II.4 – IP Group

ipAddrTable
ipNetToMediaTable
IpGroup
IpBasicStatsGroup
IpStatsGroup

MIB II.5—ICMP Group

IcmpGroup
IcmpInputStatus
IcmpOutputStats

MIB II.6—TCP Group

tcpConnTable
TcpGroup
TcpStats

MIB II.7—UDP Group

udpTable
UdpStats

MIB II.10—Transmission Group

dot3
dot3StatsTable

MIB II.11—SNMP Group

SnmpBasicGroup
SnmpInputStats
SnmpOutputStats

MIB II.17—dot1dBridge Group

dot1dBase
- dot1dBasePortTable

dot1dStp
- dot1dStpPortTable

dot1dTp
- dot1dTpFdbTable
- dot1dTpPortTable
- dot1dTpHCPortTable
- dot1dTpPortOverflowTable

pBridgeMIB
- dot1dExtBase
- dot1dPriority
- dot1dGarp

qBridgeMIB
- dot1qBase
- dot1qTp
  - dot1qFdbTable
  - dot1qTpPortTable
  - dot1qTpGroupTable
  - dot1qForwardUnregisteredTable
- dot1qStatic
  - dot1qStaticUnicastTable
  - dot1qStaticMulticastTable
- dot1qVlan
  - dot1qVlanCurrentTable
  - dot1qVlanStaticTable
  - dot1qPortVlanTable

The Moxa switch also provides a private MIB file, located in the file **Moxa-[switch's model name]-MIB.my** on the Moxa switch utility CD-ROM.

Public Traps

- Cold Start
- Link Up
- Link Down
- Authentication Failure
- dot1dBridge New Root
- dot1dBridge Topology Changed

Private Traps

- Configuration Changed
- Power On
- Power Off
- Traffic Overloaded
- Turbo Ring Topology Changed
- Turbo Ring Coupling Port Changed
- Turbo Ring Master Mismatch
- Multiple MRM Role in MRP Ring
- MRP Ring Open
- Supervision frame time different in A/B port
- PTP Synchronization Status Changed
- Grandmaster Changed
- Module Insert or Remove
- PortLoopDetectedTrap
- RateLimitedOnTrap
- LLDPChgTrap
- ABC-02 error
- Account Authentication Success,
- Account Authentication Failure,
- Number of Mac Sticky Address is over the threshold
- Fiber Warning
- Event Log is over capacity
- Account Information Changed
- Configuration is imported
- Remote Authentication success
- Remote Authentication fail
- Status of tracking object is changed
- Tracking VRRP changed
- Tracking Static Route Change
- Tracking port enable change
- EPS on
- EPS off
- GOOSE Check
- Dying Gasp