TN Series Managed Ethernet Switch User Manual

Version 3.0, October 2025

www.moxa.com/products

Models covered by this user's manual
TN-4500A Series
TN-5500A Series

TN Series Managed Ethernet Switch 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.

The following two chapters are covered in this user manual:

- **Getting Started**
  This chapter explains how the initial installation process for Moxa switch. There are three ways to access Moxa switch's configuration settings: the serial console, Telnet console, and web console.
- **Featured Functions**
  This chapter explains how to access Moxa switch's various configuration, monitoring, and administration functions. These functions can be accessed by serial, Telnet, or web console. The web console is the most user-friendly way to configure Moxa switch. In this chapter, we use the web console interface to introduce the functions.

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, Telnet console, or web console. 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 COM port with a short serial cable. You can open the Telnet or web console over an Ethernet LAN or over the Internet.

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

NOTE

- You cannot connect to the serial and Telnet console at the same time.
- You can connect to the web console and another console (serial or Telnet) at the same time. However, we strongly recommend that you do NOT do so. Following this advice will allow you to maintain better control over the Moxa switch's configuration.

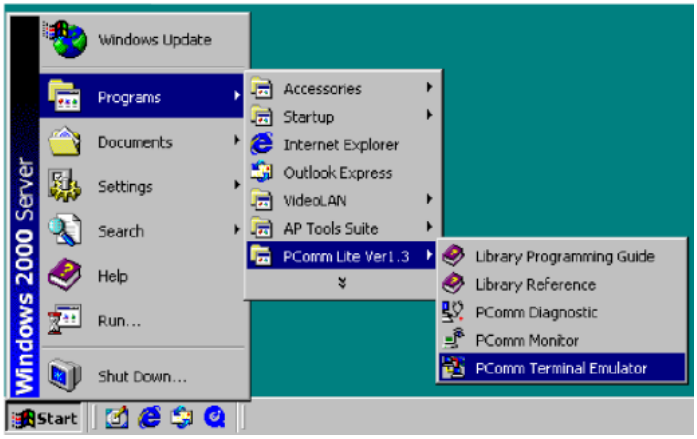
NOTE

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

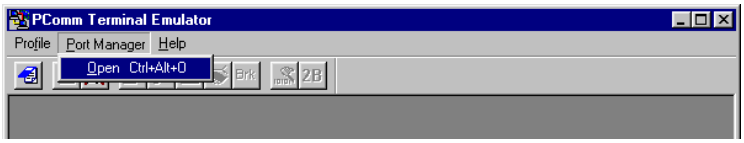
Before running PComm Terminal Emulator, use an RJ45 to DB9-F (or RJ45 to DB25-F) cable to connect the Moxa switch's console port to your PC's COM port (generally COM1 or COM2, depending on how your system is set up).

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

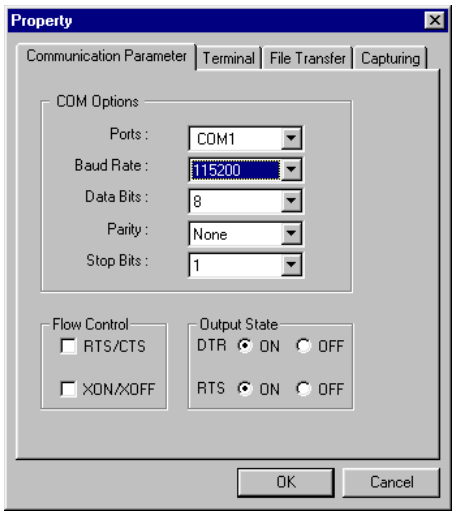
1. From the Windows desktop, click **Start > Programs > PComm Lite 1.3 > Terminal Emulator**.



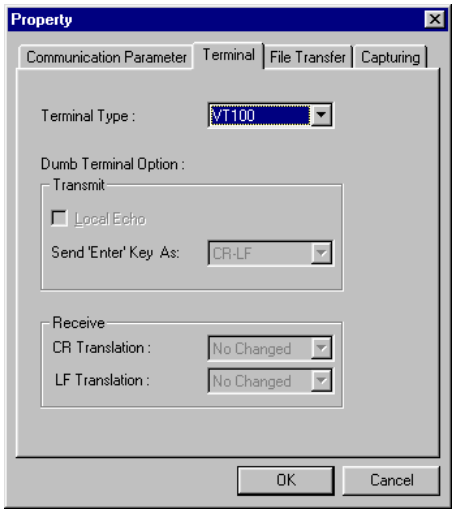
2. Select **Open** under the **Port Manager** menu to open a new connection.



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**.

```
MOXA ToughNet Switch  TN-4516A-12POE-4GPOE-T
Console terminal type (1: ansi/vt100, 2: vt52) : 1_
```

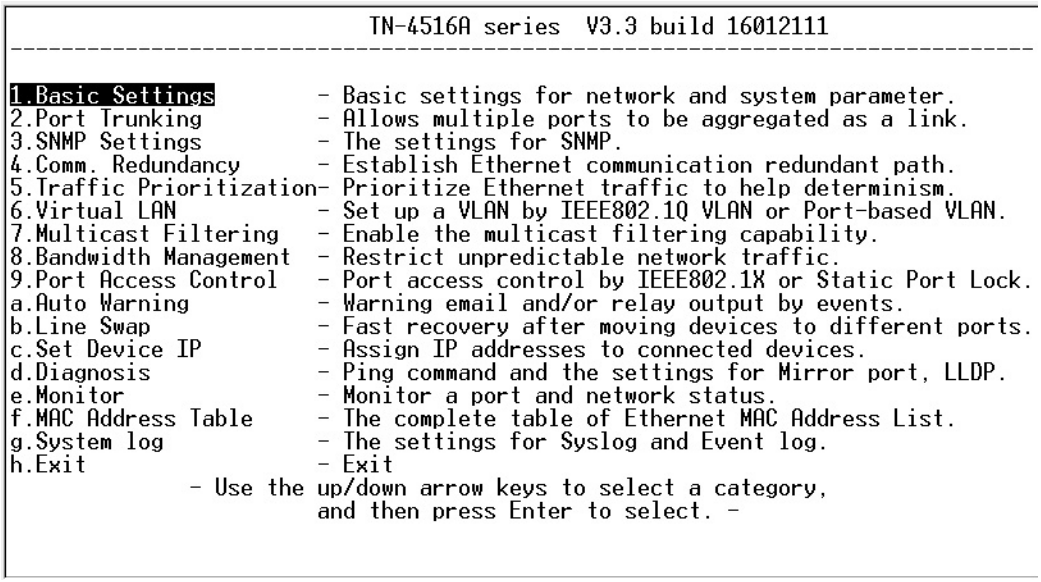
6. The serial console will prompt you to log in. Press **Enter** and select **admin** or **user**. Use the down arrow key on your keyboard to select the **Password** field and enter a password if desired. This password will be required to access any of the consoles (web, serial, Telnet). If you do not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

```
Model :              TN-4516A-12POE-4GPOE-T
Name :               Managed Redundant Switch 02135
Location :           Switch Location

Firmware Version :   V3.3 build 16012111
Serial No :          02135
IP :                 192.168.127.253
MAC Address :        00-90-E8-1F-C8-0A

  +------------------------------+
  | Account  : admin             |
  | Password :                   |
  +------------------------------+
```

7. The **Main Menu** of the Moxa switch's serial console should appear. (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 Telnet Console

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

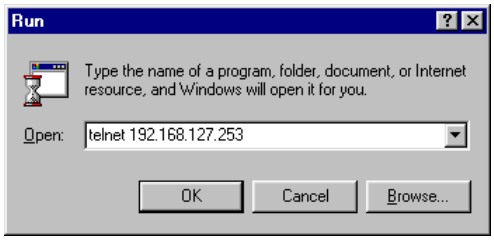
When connecting to the Moxa switch's Telnet or web console, first connect one of the Moxa switch's Ethernet ports to your Ethernet LAN, or directly to your PC's Ethernet port. You may use either a straight-through or cross-over Ethernet cable.

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 ToughNet Switch  TN-4516A-12POE-4GPOE-T
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**.

```
Model :              TN-4516A-12POE-4GPOE-T
Name :               Managed Redundant Switch 02135
Location :           Switch Location

Firmware Version :   V3.3 build 16012111
Serial No :          02135
IP :                 192.168.127.253
MAC Address :        00-90-E8-1F-C8-0A

  +------------------------------+
  | Account  : admin             |
  | Password :                   |
  +------------------------------+
```

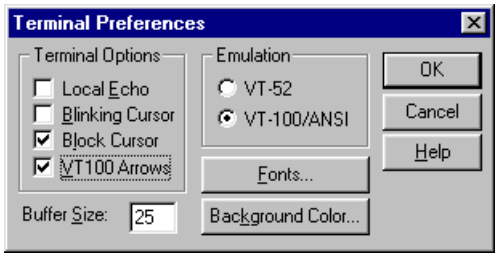
4. The **Main Menu** of the Moxa switch's Telnet console should appear.

```
                          TN-4516A series  V3.3 build 16012111
--------------------------------------------------------------------------------

1.Basic Settings          - Basic settings for network and system parameter.
2.Port Trunking           - Allows multiple ports to be aggregated as a link.
3.SNMP Settings           - The settings for SNMP.
4.Comm. Redundancy        - Establish Ethernet communication redundant path.
5.Traffic Prioritization- Prioritize Ethernet traffic to help determinism.
6.Virtual LAN             - Set up a VLAN by IEEE802.1Q VLAN or Port-based VLAN.
7.Multicast Filtering     - Enable the multicast filtering capability.
8.Bandwidth Management    - Restrict unpredictable network traffic.
9.Port Access Control     - Port access control by IEEE802.1X or Static Port Lock.
a.Auto Warning            - Warning email and/or relay output by events.
b.Line Swap               - Fast recovery after moving devices to different ports.
c.Set Device IP           - Assign IP addresses to connected devices.
d.Diagnosis               - Ping command and the settings for Mirror port, LLDP.
e.Monitor                 - Monitor a port and network status.
f.MAC Address Table       - The complete table of Ethernet MAC Address List.
g.System log              - The settings for Syslog and Event log.
h.Exit                    - Exit
              - Use the up/down arrow keys to select a category,
                          and then press Enter to select. -
```

5. In the terminal window, select **Preferences…** from the **Terminal** menu on the menu bar.

6. The **Terminal Preferences** window should appear. Make sure that **VT100 Arrows** is checked.



7. Use the following keys on your keyboard to navigate inside 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 Browser

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

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

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

NOTE

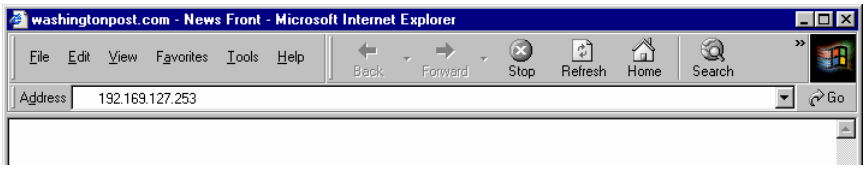
When connecting to the Moxa switch's Telnet or web console, first connect one of the Moxa switch's Ethernet ports to your Ethernet LAN, or directly to your PC's Ethernet port. You may use either a straight-through or cross-over Ethernet cable.

NOTE

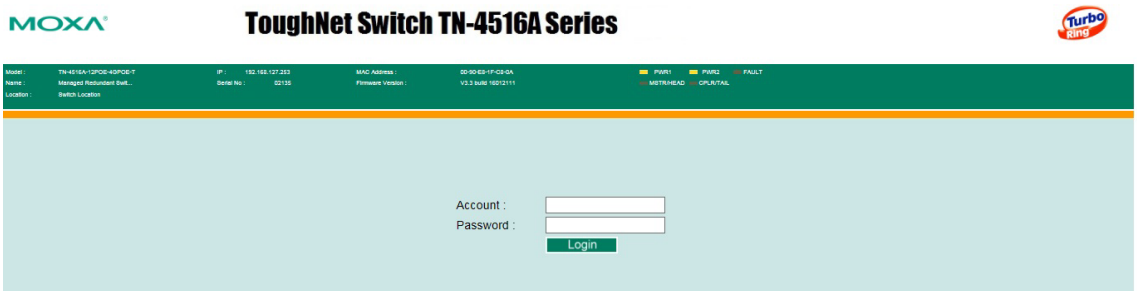
The Moxa switch's default IP address is 192.168.127.253.

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.



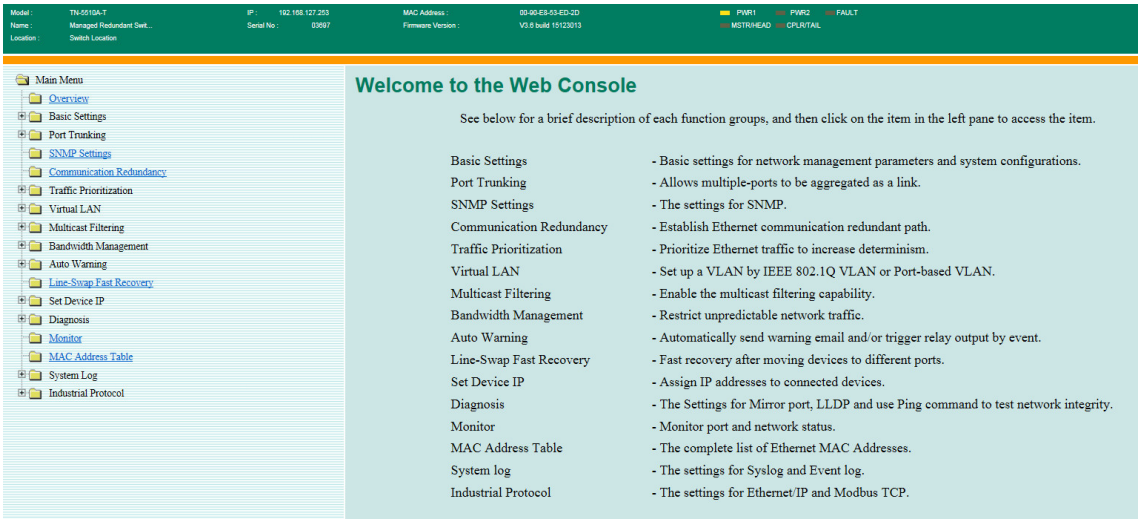
2. The Moxa switch's web console will open, and you will be prompted to log in. Select the login account (admin or user) and enter the **Password**. This password will be required to access any of the consoles (web, serial, Telnet). If you do not wish to create a password, leave the **Password** field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



NOTE

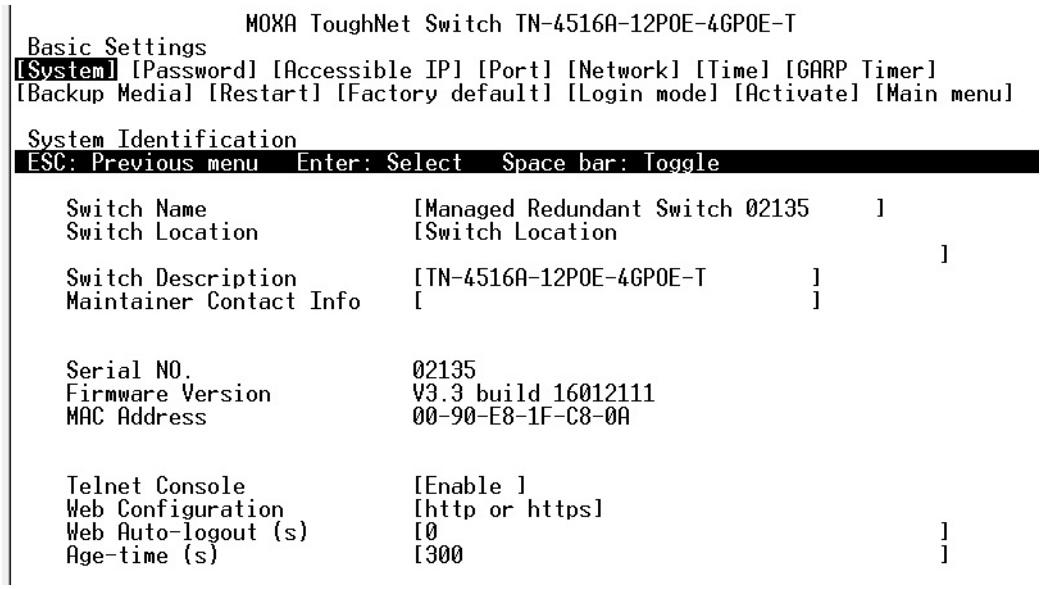
By default, the password assigned to the Moxa switch is moxa. Be sure to change the default password after you first log in to help keep your system secure.

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 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**. 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 administration functions. These functions can be accessed by serial, Telnet, or web console. The serial console can be used if you do not know the Moxa switch's IP address and requires that you connect the Moxa switch to a PC COM port. The Telnet and web consoles can be opened over an Ethernet LAN or the Internet.

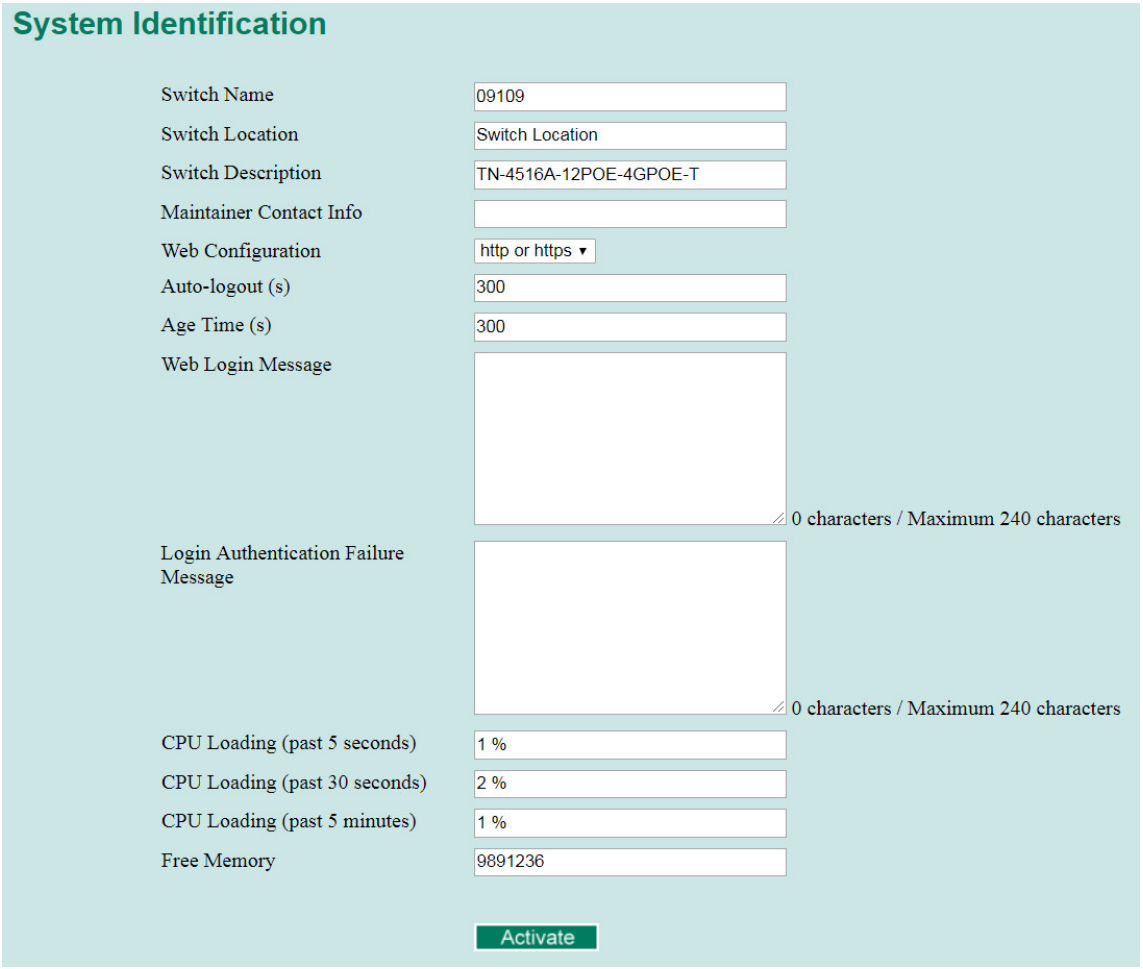
The web console is the most user-friendly interface for configuring a Moxa switch. In this chapter, we use the web console interface to introduce the functions. There are only a few differences between the web console, serial console, and Telnet console.

Configuring Basic Settings

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

System Identification

System Identification items are displayed at the top of the web console and will be included in alarm emails. You can configure the System Identification items to make it easier to identify different switches that are connected to your network.



Switch Name

Setting	Description	Factory Default
Max. 35 characters	This option is useful for differentiating between the roles or applications of different units. Example: Factory Switch 1.	Managed Redundant Switch [Serial no. of this switch]

Switch Location

Setting	Description	Factory Default
Max. 80 characters	This option is useful for differentiating between the locations of different units. 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

Maintainer Contact Info

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

Auto-logout (S)

Setting	Description	Factory Default
60 to 86400 (seconds)	Disable or extend the auto-logout time for the web management console.	300

Age Time (S)

Setting	Description	Factory Default
15 to 3825 (seconds)	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.	300

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.	None

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.	None

CPU Loading

Setting	Description	Factory Default
Read-only	The CPU usage volume in the past 5 seconds, 30 seconds, and 5 minutes	None

Free Memory

Setting	Description	Factory Default
Read-only	The immediately free memory of the switch	None

Auto Configuration

Auto Configuration is a Moxa-proprietary feature that enables zero-touch deployment and configuration management for network devices. It leverages the DHCP service to automate the provisioning process during device boot-up.

The key benefits of Auto Configuration include:

- **Reduced manual work**: Eliminates the need to manually configure each device individually, saving significant time and effort.
- **Faster deployment**: Streamlines the configuration process for quicker network setup, especially for large deployments.

How Auto Configuration Works

Auto Configuration streamlines configuration syncing across multiple switches by having the relevant switches retrieve and import the configuration file automatically. This is achieved by including the configuration file and storage server information in the DHCP Option 66/67 values. Option 66 specifies the IP address of the file server that hosts the configuration file, while Option 67 identifies the exact configuration file the device should download. When the device obtains this information after boot-up, it will automatically import and apply the corresponding configuration.

To initiate this process, the switch directly connected to the DHCP/file server — the control unit (CU) — obtains the Option 66/67 information when requesting an IP address after booting up. Once the switch has imported and applied the configuration, it will leverage LLDP to identify nearby switches to send DHCP offers to. Neighboring switches will subsequently receive the configuration file information when requesting their IP address and contact the file server. When imported, the switch will pass on this information to the next switch in the sequence. This process continues until all applicable switches have imported the configuration.

NOTE

Auto Configuration uses DHCP Option 61 Client-Identifier and LLDP information to determine who should offer the IP and related configuration. The device sends DHCP discover/request packets with Option 61 only through the control unit port connected to the DHCP and file server. DHCP discover/request packets sent through other ports will not contain Option 61.

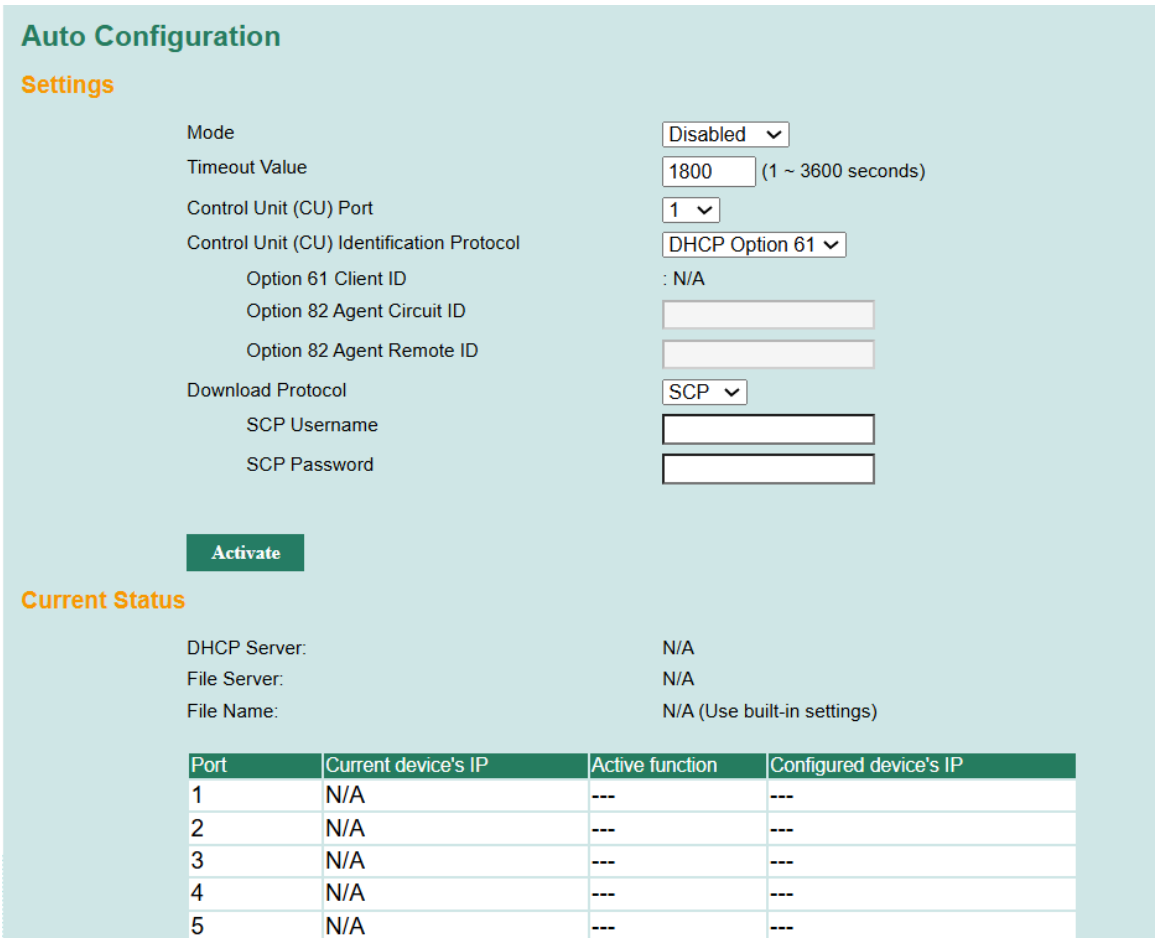
Auto Configuration supports two distinct modes: **Import** and **Propagate**.

- In **Import** mode, the Auto Configuration process will trigger after every power cycle.
- In **Propagate** mode, the device will not run the Auto Configuration process after restarting but will propagate the configuration file information via DHCP responses to requests from any neighboring device(s) identified through LLDP.

To ensure Auto Configuration works smoothly, refer to the following network design and device preparation tips:

- To streamline large-scale zero-touch deployments, using a custom default configuration is useful. If a custom default is set up, the switches can leverage Auto Configuration to align their default configuration and sync redundant protocol and VLAN settings. Once the switches boot up, the devices will retrieve the configuration automatically. Please refer to the **Using Auto Configuration for Multi-device Deployments** section for more information.
- You can set up multiple file servers within the network for faster file transfers and load balancing.
- To avoid conflicting DHCP offers, ensure each device will only get their DHCP offer from a single source. Please refer to the DHCP server settings for port-based offers.
- Keep in mind that time needed for the Auto Configuration process depends on several factors, including the size of the network, file transfer times, and the LLDP/DHCP timer.

Auto Configuration Settings



Mode

Setting	Description	Factory Default
Disabled	Disable the Auto Configuration function.	Disabled
Import	In this mode, the device will run the Auto Configuration process after device boot-up. The device only sends Option 61 or 82 packets over the control unit port depending on the selected Control Unit (CU) Identification Protocol. For Import mode, the following conditions must be met: • The CU Port cannot be a trunk group member port. • The CU Port cannot be a Turbo Ring v2 ring port. • **Auto IP Configuration** must be set to **By DHCP**. • **LLDP** must be enabled. When the device acts as a DHCP server, it will only respond to a DHCP client's request if the request originates from a directly connected neighbor. • **Auto Config Change Update** must be disabled. • **Conditional Auto IP Assignment** must be disabled.	
Propagate	In this mode, the device will not run Auto Configuration process after device boot-up. However, the device will anticipate some devices in the topology may initiate the Auto Configuration Change Update process due to device replacement or some configuration changes. For Propagate mode, the following conditions must be met: • **Auto IP Configuration** must be disabled. • **LLDP** must be enabled. When the device acts as a DHCP server, it will only respond to a DHCP client's request if the request originates from a directly connected neighbor. • **Conditional Auto IP Assignment** must be disabled.	

Timeout Value

Setting	Description	Factory Default
1 to 3600	If the mode is set to **Import**, specify the Auto Configuration timeout value (in seconds). This parameter defines how long the switch will wait for a DHCP offer during the bootup process. If the device fails to receive a DHCP offer within the specified timeout period, the Automatic Configuration process will be terminated. A log message will be recorded for troubleshooting purposes.	1800

NOTE

The overall duration of the Auto Configuration process can be affected by various factors, including the network size, file transfer times, and other network-related conditions.

Control Unit (CU) Port

Setting	Description	Factory Default
Port	Select the control unit port. This is the port that connects to the DHCP server.	1

Control Unit (CU) Identification Protocol

In the Auto Configuration process, the devices directly connected to the CU should be assigned an IP address first. Since DHCP communication uses broadcast packets, specific strings carried in DHCP Option 61 or Option 82 are needed for recognizing packets from devices directly connected to the CUs. Any DHCP client directly connected to the CU must send DHCP Discover/Request with Option 61 or 82 to the CU port and send DHCP Discover/Request without Option 61 or 82 to other ports. For Auto Configuration to work, the user should configure the DHCP server on the CU to recognize the specified DHCP Option (61 or 82) and assign an IP address only to the matched device. When a DHCP client has configured its IP settings, it will obtain the relevant Option 66/67 information from the DHCP assignment packet to request the specified configuration file (Option 67) from the designated file server (Option 66).

Setting	Description	Factory Default
DHCP Option 61	Set the CU identification protocol to DHCP Option 61. When DHCP Option 61 is selected as the CU Identification Protocol, the original DHCP Client Option 61 functionality will not be active on non-CU ports when the Auto Configuration mode is set to **Import**. For DHCP Option 61, the following conditions must be met: • **Auto IP Configuration** must be set to **By DHCP**. • **Enable Option 61** in **IP Settings** must be enabled. • The **Client ID** in **IP Settings** must be configured.	None
DHCP Option 82	Set the CU identification protocol to DHCP Option 82. When DHCP Option 82 is chosen as the CU Identification Protocol, it operates independently from the original Option 82 mechanism in the DHCP Relay Agent feature. In Auto Configuration, Option 82 is included in the DHCP Discover/Request sent by the device when requesting an IP assignment through a CU port. However, in DHCP Relay Agent, Option 82 is added to the DHCP Discover/Request that the device receives and attempts to relay. Because Auto Configuration specifies dedicated Auto Configuration strings as the Option 82 sub-option values, it can be distinguished from the standard DHCP relay agent functionality, ensuring that the two applications do not interfere with each other.	None

NOTE

For easier long-term system maintenance, we strongly recommend using DHCP Option 61 as the protocol for Auto Configuration, especially if this is your first time using this feature on a Moxa device.

Option 82 Agent Circuit ID

Setting	Description	Factory Default
0 to 32 characters	If the **CU Identification Protocol** is set to **DHCP Option 82**, specify the Option 82 Agent Circuit ID. This string cannot contain any spaces.	None

Option 82 Agent Remote ID

Setting	Description	Factory Default
0 to 32 characters	If the **CU Identification Protocol** is set to **DHCP Option 82**, specify the Option 82 Agent Remote ID. This string cannot contain any spaces.	None

Download Protocol

Setting	Description	Factory Default
SCP	Select SCP as the download protocol.	SCP
TFTP	Select TFTP as the download protocol.	

SCP Username

Setting	Description	Factory Default
1 to 16 characters	If the **Download Protocol** is set to **SCP**, enter the SCP username. The username can be up to 16 characters long and cannot contain spaces.	None

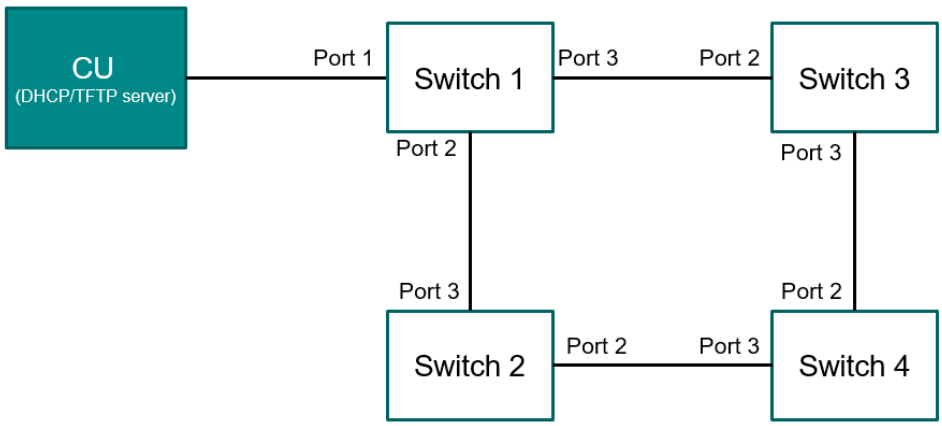
SCP Password

Setting	Description	Factory Default
1 to 48 characters	If the **Download Protocol** is set to **SCP**, enter the SCP password. The password can be up to 48 characters long and cannot contain spaces.	None

Scenario 1: Using Auto Configuration for Multi-device Deployments

This section explains how to use Auto Configuration to automatically update the configuration of multiple devices. The reference setup is divided into two stages, setting up the devices for Auto Configuration and configuring the switches for deploying Auto Configuration for an operational environment.

Refer to the example topology below.



Before you begin:

- Set up a DHCP server with Option 61, 66, and 67.
- Set up a TFTP server to host the configuration files.
- The DHCP server is reachable via the control unit port.

Stage 1: Configuring the switches for Auto Configuration during operations

The following steps will guide you in how to prepare the configuration file and how to use the custom default configuration for creating an Auto Configuration environment on each of the switches.

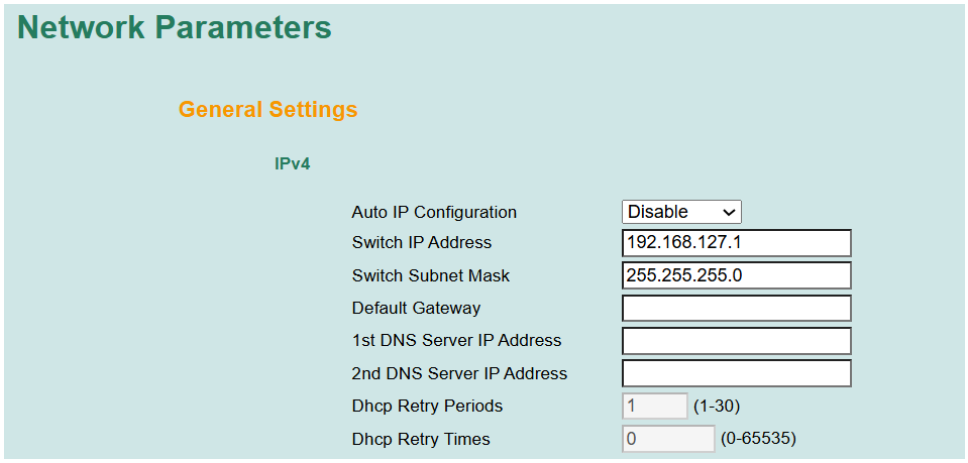
NOTE

- If the configuration file sets the Auto Configuration mode to **Import**, the device will run the Auto Configuration procedure after every power cycle.
- If the configuration file sets the Auto Configuration mode to **Propagate**, the device will not run the Auto Configuration procedure after a power cycle but will only assign IP addresses to directly connected neighboring devices.

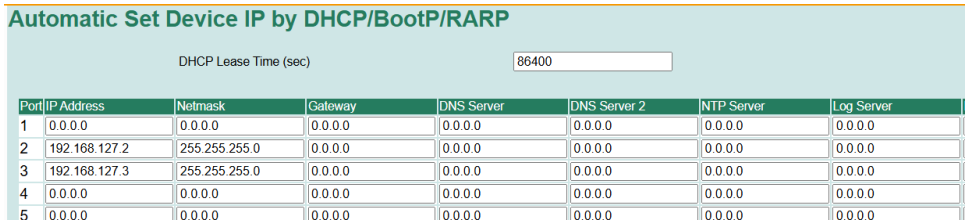
For this reference scenario, we will configure the switch to be in **Propagate** mode after importing the configuration, as we do not want the device to import the configuration again after completing the first **Auto Configuration** cycle.

These settings should be configured on all switches, unless otherwise specified.

1. Go to **Basic Settings > Provisioning > Auto Configuration**.
2. Set the **Mode** to **Propagate**.
3. Click **Activate**.
4. Go to **Basic Settings > Network > IP Settings**.
5. Set **Auto IP Configuration** to **Disable**. This allows you to configure a static IP for the device.
6. Configure the device's static IP address.
   In this example, we configured Switch 1 with the static IP 192.168.127.1 with subnet 255.255.255.0.



7. Click **Activate**.
8. Go to **Communication Redundancy**.
9. Select **Turbo Ring V2** as the **Protocol**.
10. Enable **Ring 1** and select port 2 and port 3 as the **Redundant Ports**.
11. Click **Apply**.
12. Set **LLDP** to **Enable**.
13. Set the **Message Transmit Interval** to 10.
14. Click **Activate**.
15. Go to **Set Device IP > DHCP/BootP/RARP**.
16. Configure the IP and subnet assignments for the switches connected on the ring ports. In this example, we assign 192.168.127.1, 192.168.127.2, 192.168.127.3, 192.168.127.4 to Switch 1, 2, 3, and 4 respectively.
    Refer to the following reference settings for switch 1.



Port	IP Address	Netmask	Gateway	DNS Server	DNS Server 2	NTP Server	Log Server
1	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0
2	192.168.127.2	255.255.255.0	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0
3	192.168.127.3	255.255.255.0	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0
4	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0
5	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0

In this example, the configuration for all 4 switches looks as follows:

Switch	Port	IP Address	Subnet Mask	Lease Time
Switch 1	2	192.168.127.2	24 (255.255.255.0)	86400
	3	192.168.127.3	24 (255.255.255.0)	86400
Switch 2	2	192.168.127.4	24 (255.255.255.0)	86400
	3	192.168.127.1	24 (255.255.255.0)	86400
Switch 3	2	192.168.127.1	24 (255.255.255.0)	86400
	3	192.168.127.4	24 (255.255.255.0)	86400
Switch 4	2	192.168.127.3	24 (255.255.255.0)	86400
	3	192.168.127.2	24 (255.255.255.0)	86400

17. Go to **Set Device IP > DHCP Server Option 66/67**.
18. Set **DHCP Option 66** to **Issued by DHCP** and the **DHCP Option 67** to **IP Address**. In this configuration, we expect switch 1 to propagate DHCP Option 66 value containing the file server address and DHCP Option 67 value containing the configuration filename (192.168.127.2) to switch 2 via port 2.
19. Click **Activate**.
20. Go to **Configuration Back and Restore**.
21. Enter ''192.168.127.X'' (without the quotes) as the configuration file name, with X representing the IP address of the switch.
22. Back up the configuration to the TFTP server.

Stage 2: Configuring the switches for the initial Auto Configuration cycle

The following steps will guide you in how to configure the switches for initiating the Auto Configuration process.

These settings should be configured on all switches, unless otherwise specified.

1. Go to **Basic Settings > Provisioning > Auto Configuration**.
2. Set the **Mode** to **Import**.
3. For the switch connected to the CU (Switch 1 in this scenario), also configure the following settings:
   a. Set the **Control Unit (CU) Port** to 1.
4. Click **Activate**.
5. Go to **Basic Settings > Network > IP Settings**.
6. Set **Auto IP Configuration** to **By DHCP**.
7. For the switch connected to the CU (Switch 1 in this scenario), also configure the following settings:
   a. Check the **Enable Option 61** option.
   b. Enter "MOXA" (without quotes) as the **Client ID**.
8. Click **Activate**.
9. Go to **Communication Redundancy**.
10. Select **Turbo Ring V2** as the Protocol.
11. Enable **Ring 1** and select port 2 and port 3 as the **Redundant Ports**.
12. Click **Apply**.
13. Go to **Diagnosis > LLDP**.
14. Set **LLDP** to **Enable**.
15. Set the **Message Transmit Interval** to 10.
16. Click **Activate**.
17. Go to **Configuration Backup and Restore** and enter *Custom Default demo* as the **Configuration Name**.
18. Go to **Basic Settings > Custom Default**.
19. Click **Copy**.
20. Restart all switches to trigger the Auto Configuration process.

Result: After restarting the switches, the switch connected to the CU will request and receive the configuration file and file server through the DHCP Option 66/67 values added to the DHCP response. As the switches are configured to be in **Import**, the neighbor switches in the ring topology identified via LLDP will

similarly request and receive the configuration file information in the DHCP via the ring ports. After applying the imported configuration, the Auto Configuration mode will be set to **Propagate**, to prevent the switches from initiating the Auto Configuration process after subsequent reboots.

Auto Config Change Update

The **Auto Config Change Update (ACCU)** feature provides a way to automatically update the configurations of devices in the topology during the boot-up sequence. This feature is useful when replacing a faulty switch or when updating the configuration of specific switches. By reducing the need for DHCP server interactions and unnecessary configuration file downloading and importing, ACCU can speed up configuration updates. This function will only apply to devices that have ACCU enabled.

ACCU requires a Configuration File Identifier (CFID) file, which is the checksum of the configuration file. When the ACCU feature is enabled, an additional **Auto Config Change Update Setting** section will become available on the **Configuration Backup and Restore** page. Refer to the **CFID File Naming and Extension Rules** section. The CFID file must be placed together with the associated configuration file on the storage server for ACCU to work.

The standard ACCU process works as follows:

1. When powered on, any switches with ACCU enabled will check if the file server is alive by sending ICMP Request packets at the specified Check-alive interval.
2. If the file server responds, the device will request its CFID file to determine if a new configuration file needs to be downloaded.
3. If the CFID is new it means the configuration was modified since the last import. In this case, the switch will attempt to download the configuration corresponding to the new CFID.
4. If the file server does not respond after the specified number of check-alive attempts, the ACCU process will stop.

CFID File Naming and Extension Rules

The CFID filename and extensions must follow several rules. An invalid CFID file name or file extension could result in ACCU not working properly.

Rule	Description
Name Format	[Configuration File Name]_*cfid.ini*.
Extension	.ini
Filename Length	54 characters (max.)
Supported Characters	Letters (a-z, A-Z), numbers (0-9), underscores (_), periods (.) and hyphens (-). Spaces must be replaced by underscores (_).

For example:

- Configuration file: **demo switch1.ini**
- CFID file: **demo_switch1_cfid.ini**

NOTE

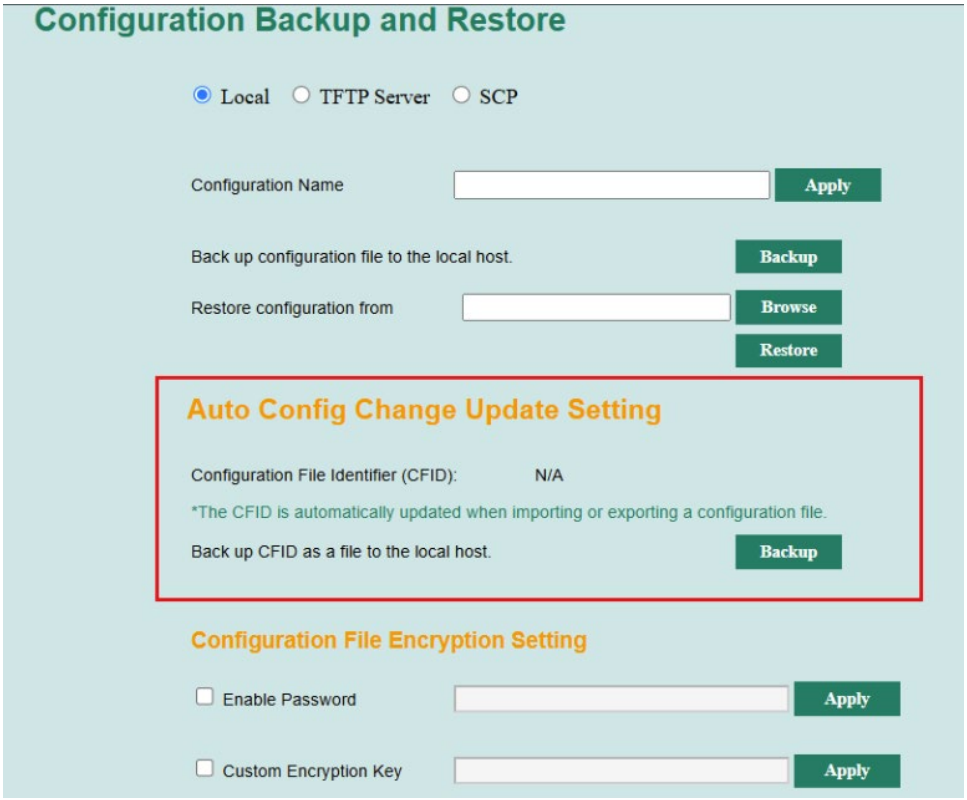
Whenever the exported configuration file stored on the SCP server is modified, the corresponding CFID file also must be updated.

NOTE

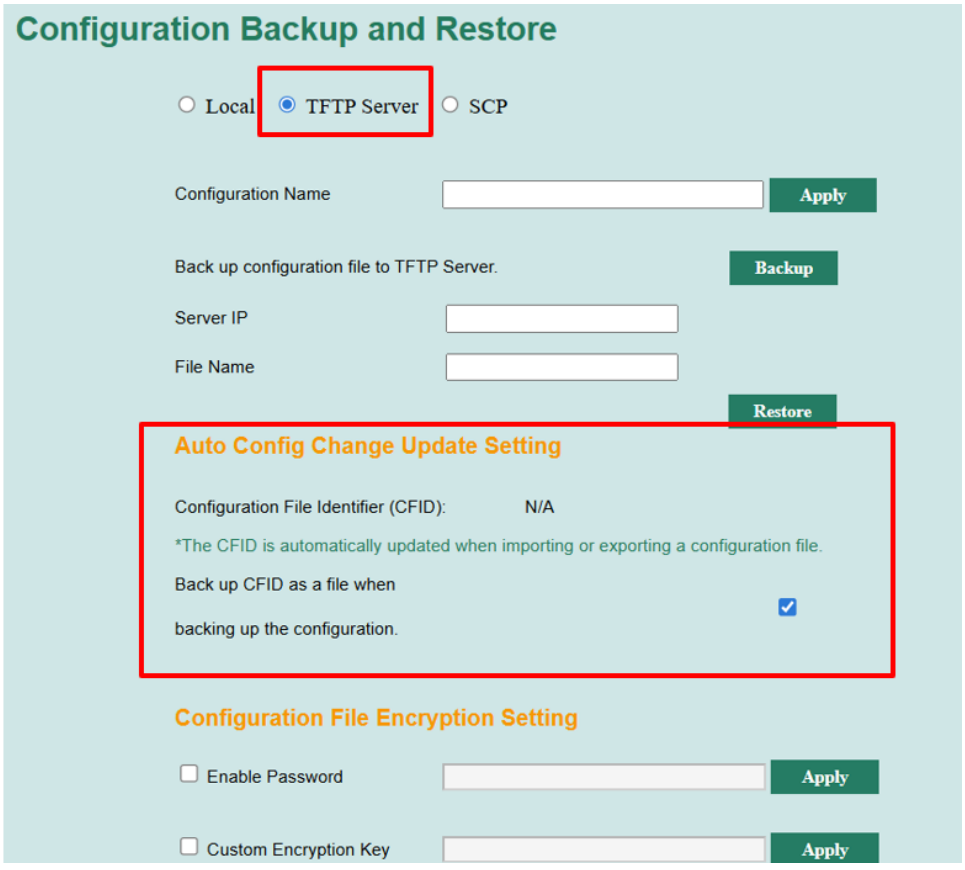
A valid CFID file can only be backed up after the configuration file has been successfully exported.

The CFID file can be generated from the **Configuration Backup and Restore** page.

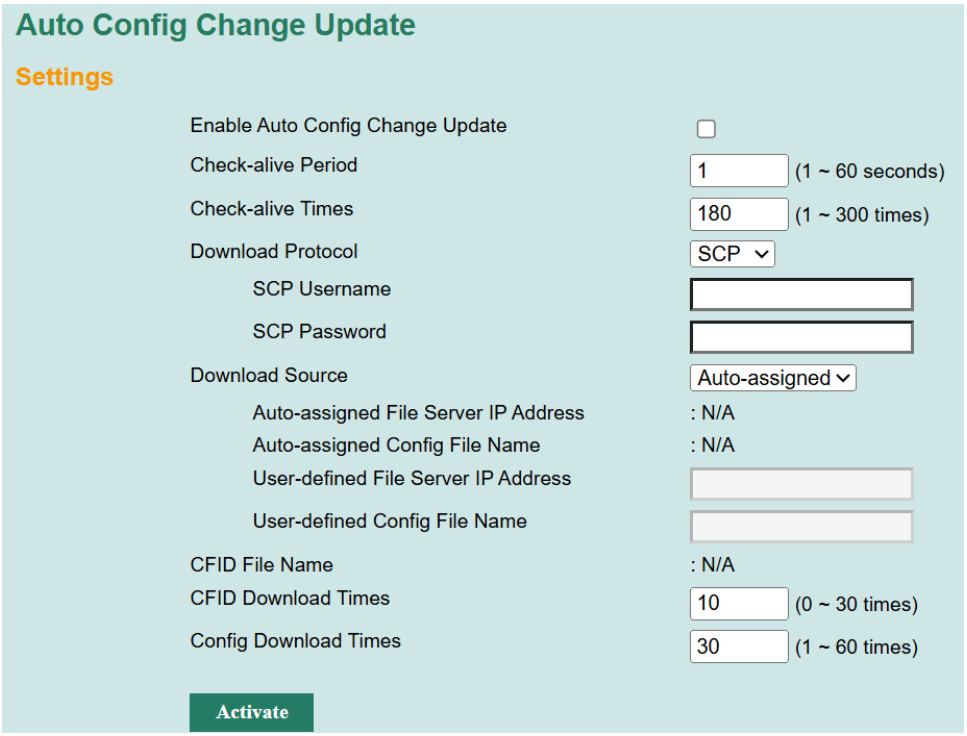
To download the CFID file to the local host, select **Local** and click **Backup** in the **Auto Config Change Update Setting** section.



If ACCU is enabled, and the configuration backup/restore source is set to **TFTP**, if the **Back up CFID as a file when backing up the configuration** option is checked, the CFID will be sent to the TFTP server as a file along with the configuration file when backing up the configuration.



Settings



Enable Auto Config Change Update

Setting	Description	Factory Default
Enable or Disable	Enable or disable the Auto Configure Change Update (ACCU) feature. If enabled, the following settings must be configured: • **Auto IP Configuration** must be disabled. • The **Auto Configuration** mode must be set to **Propagate** or **Disabled**. • **Conditional Auto IP Assignment** must be disabled.	Disabled

Check-alive Period

Setting	Description	Factory Default
1 to 60	Specify the interval (in seconds) to check if the file server is available.	1

Check-alive Times

Setting	Description	Factory Default
1 to 300	Specify the number of times the system will perform a check-alive check at the specified interval.	180

Download Protocol

Setting	Description	Factory Default
SCP	Select SCP as the download protocol.	SCP
TFTP	Select TFTP as the download protocol.	

SCP Username

Setting	Description	Factory Default
1 to 16 characters	If the **Download Protocol** is set to **SCP**, enter the SCP username. The username can be up to 16 characters long and cannot contain spaces.	None

SCP Password

Setting	Description	Factory Default
1 to 48 characters	If the **Download Protocol** is set to **SCP**, enter the SCP password. The password can be up to 48 characters long and cannot contain spaces.	None

Download Source

Select the download source to determine how to retrieve the IP address of the file server and configuration filename.

Setting	Description	Factory Default
Auto-assigned	Retrieve server and file information via a DHCP server, which provides Options 66/67, whether from a neighbor switch or a remote DHCP server. If the switch obtained its IP via a neighbor switch, the system will use the filename and file server information specified in the DHCP Option 66/67 values configured for **Auto Configuration** on the switch providing the DHCP response. If the switch obtained its IP from a remote DHCP server, it will instead receive the filename and server information from the DHCP Option 66/67 provided by the DHCP server. In this mode, the switch will populate the **Auto-assigned File Server IP Address** and **Auto-assigned File Name** fields with the information it received from DHCP Option 66/67 when it obtained its IP address. Once ACCU is enabled, it will use these locally stored values to identify the file server and configuration file.	Auto-assigned
User-defined	Specify the file server and configuration file name.	

User-defined File Server IP Address

Setting	Description	Factory Default
Read-only	If the **Download Source** is set to **User-defined**, specify the file server IP address.	None

User-defined Config File Name

Setting	Description	Factory Default
Read-only	If the **Download Source** is set to **User-defined**, specify the configuration filename.	None

CFID Download Times

Setting	Description	Factory Default
0 to 30	Specify the number of retry times for downloading the CFID file. If unsuccessful, the system will attempt to download the CFID file until the specified retry limit is reached. If set 0, the device will skip the CFID file and directly download the configuration file.	10

Config Download Times

Setting	Description	Factory Default
1 to 60	Specify the number of retry times for downloading the configuration file. If unsuccessful, the system will attempt to download the configuration file until the specified retry limit is reached.	30

Conditional Auto IP Assignment

NOTE

This feature is unrelated to the **Auto Configuration** and **Auto Configuration Change Update** functions.

A train is composed of basic units called cars. For certain projects, these cars can be added to or removed from a train for operational reasons. The Conditional Auto IP Assignment feature allows the network configuration to automatically adjust itself when the train car composition is altered to ensure seamless operation. You can customize the car type and UID information to more easily recognize the train car. Refer to **Train Information** for more information.

How Does Conditional Auto IP Assignment Work?

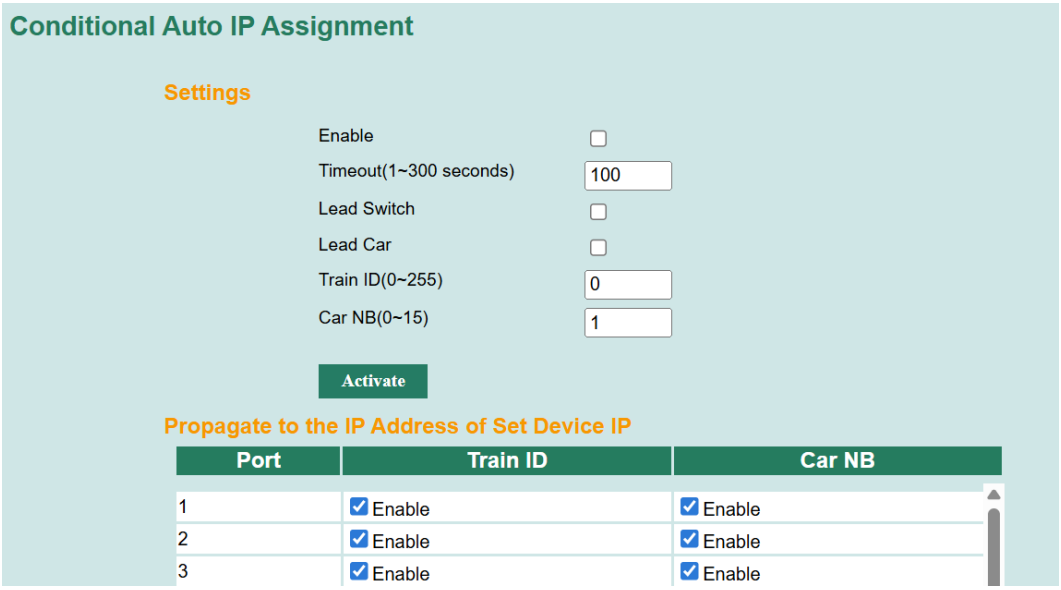
Before going into details on how this feature works, let's first go over some key terms.

- **Train ID**: An unique identifier for the whole train vehicle.
- **Car NB**: An unique identifier that indicates the car's position within the train vehicle.
- **Car Type**: The type of train car where the switch can be installed.
- **Lead Switch**: Indicates that the switch is assigned to start the Conditional Auto IP Assignment process.
- **Lead Car**: Indicates that the switch belongs to the car containing the Lead Switch and therefore should only accept information propagation via ring ports and not via coupling ports (train-level coupling ports). You can designate one car as the Lead Car, which must be located at either end of the train.

Conditional Auto IP Assignment works by creating an environment in which a designated Lead switch in the lead car will propagate the user-specified train parameters —the Train ID and Car NB— to neighboring switches connected via ring or coupling ports in the ring topology. When a switch has obtained the train parameters from an adjacent switch and configured its static IP, it will then propagate this information to its neighbor switches, until all switches are configured. When the train composition is changed, and a switch is moved or a new switch is added, the adjacent switch will propagate the current train parameters to the new switch so it can configure its IP accordingly. The Lead switch will only re-initiate the auto IP assignment process if either the Train ID or Car NB, or both, was modified on the Lead switch.

Refer to the **How to Configure Conditional Auto IP Assignment** section for how to configure this function for different scenarios.

Conditional Auto IP Assignment Settings



Settings

Enable

Setting	Description	Factory Default
Enable or Disable	Enable or disable the Conditional IP Assignment function.	Disabled

Timeout

Setting	Description	Factory Default
1 to 300	Specify the timeout value (in seconds) to determine whether to proceed with or terminate the Conditional Auto IP Assignment process. Any switch that is not designated as the Lead switch should receive the Train ID and Car NB from the adjacent switch after it boots up. If the switch does not receive the relevant Train ID and Car NB within the specified timeout period, the system will terminate the Conditional IP Assignment process and keep the device's original Train ID and Car NB information.	100

Lead Switch

Setting	Description	Factory Default
Enable or Disable	Check to assign the switch as the Lead switch, indicating the switch is allowed to initiate the Conditional IP Assignment procedure. The Lead switch will propagate the Train ID and Car NB to neighboring switches via ring and coupling ports after it boots up. Non-lead switches will propagate those values to other switches once they have received the relevant information from the Lead switch.	Disabled

Lead Car

Setting	Description	Factory Default
Enable or Disable	Check to indicate the switch is located in the car containing the Lead switch.	None

Train ID

Setting	Description	Factory Default
0 to 255	Specify a unique identifier for the train vehicle.	0

Car NB

Setting	Description	Factory Default
0 to 15	Specify a unique identifier for the train car, indicating its position within the train vehicle.	1

Propagate to the IP Adress of Set Device IP

Train ID

Setting	Description	Factory Default
Enable or Disable	Enable or disable propagation of the Train ID. If enabled, the Train ID will be propagated to the IP address configured for this port in the **Set Device IP** settings.	Enabled

Car NB

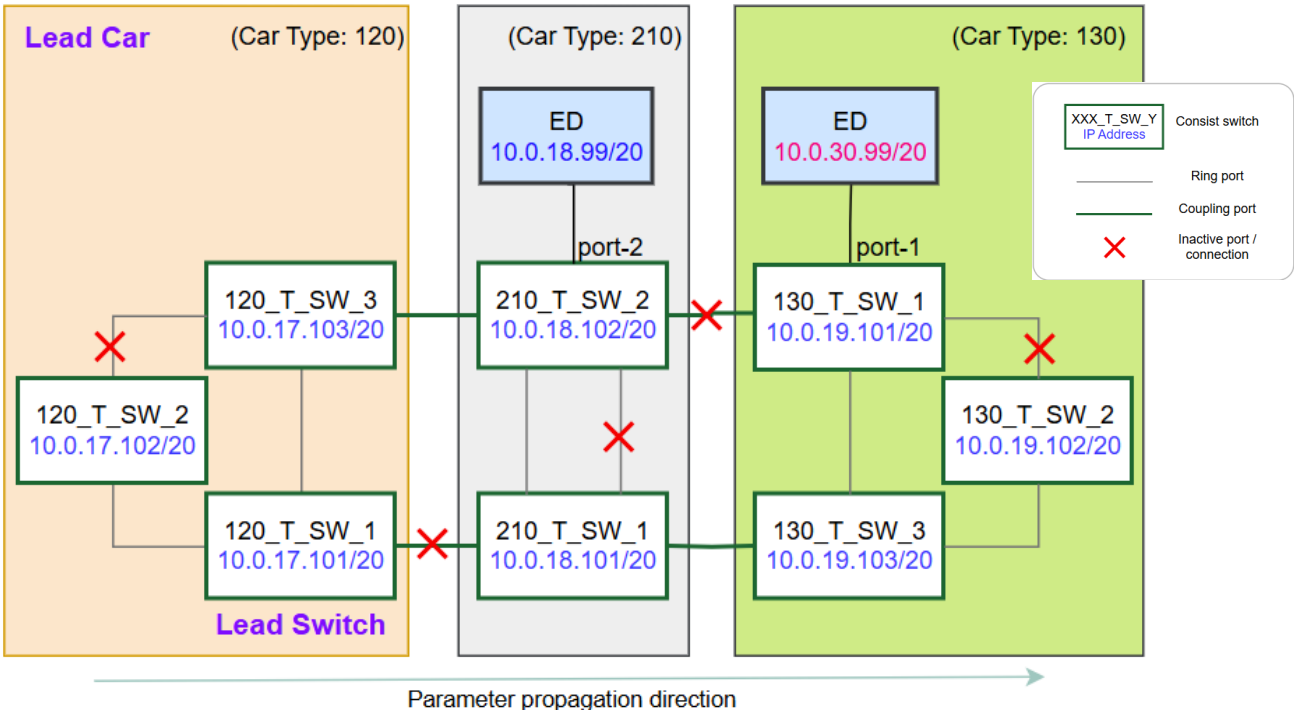
Setting	Description	Factory Default
Enable or Disable	Enable or disable propagation of the Car NB. If enabled, the Car NB will be propagated to the IP address configured for this port in the **Set Device IP** settings.	Enabled

How to Configure Conditional Auto IP Assignment

The following section explains how to configure Conditional Auto IP Assignment for different train composition scenarios.

Scenario 1: Conditional Auto IP assignment on a 3-car train

The following reference diagram illustrates the switch and end device IP assignment in a 3-car train.



Refer to the following reference instructions for setting up Conditional Auto Configuration on the switches for this scenario.

These settings should be configured on all switches, unless otherwise specified.

1. Go to **Communication Redundancy**.
2. Select **Turbo Ring V2** as the **Protocol**.
3. Configure the static coupling settings between the train cars.

> **NOTE**
>
> Dynamic Ring Coupling (DRC) is not supported when using Conditional Auto IP Configuration.

4. Go to **Basic Settings > Provisioning > Conditional Auto IP Assignment** and configure the following settings:
   a. Enable **Conditional Auto IP Assignment**.
   b. Specify the **Train ID** for all switches. In this example, the Train ID is 0.
   c. Specify the **Car NB** for all switches. In this example, the Car NB is 1.
   d. On all switches installed in the lead car, check the **Lead Car** option. In this example, we specify 120_T_SW_1, 120_T_SW_2, and 120_T_SW_3 as lead car switches.
   e. Check the **Lead Switch** option for the designated lead switch. In this example, we designate 120_T_SW_1 as the Lead Switch.
   f. For all non-lead switches, configure the timeout value.
   g. In the **Propagate to the IP Address of Set Device IP** section, check the **Train ID** and **Car NB** options for port 2 for switch 210_T_SW_2. This will allow the switch to assign IP addresses to connected end devices based on the inherited Train ID and Car NB values.

NOTE

The switch will calculate the IP addresses for the switch and connected devices based on inherited Train ID and Car NB values specified on the Lead switch. The switch will convert the IP based on the following binary format: xxxx xxxx.*trainid*.xxxx cccc.xxxx xxxx

- **x**: Assigned IP address value, non-inheritable
- **trainid**: Train ID, 8 bits, inheritable (depending on configuration)
- **c**: Car NB, 4 bits, inheritable (depending on configuration)
  The Car NB will propagate from the Lead Car via coupling ports and adds an increment of 1 for each consecutive car.

The IP address digits are generated by converting the Train ID and Car NB values during the IP address calculation from binary to decimal format. Refer to the IP conversion behavior in the following scenarios.

a) If the switch acts as a DHCP Client with a preconfigured static IP address: In this example, the switch has the IP 10.1.17.101 (0000 1010. **0000 0001**. 0001 **0001.** 0110 0101). The bolded binary values represent inherited values that will determine the converted IP address. All other values will remain unchanged during conversion. When inheriting the train information Train ID=0 and Car NB=2, the switch's IP will subsequently change to 10.0.18.101 (0000 1010. **0000 0000**. 0001 **0002**. 0110 0101)

b) If the switch acts as a DHCP Server: In this example, the static IP address 10.1.17.99 (0000 1010. **0000 0001**. 0001 **0001**. 0110 0011) has been configured on a specific port for a connected DHCP Client. The bolded binary values represent inherited values that will determine the converted IP address. All other values will remain unchanged during conversion. When propagating the train information Train ID=0 and Car NB=2, the IP address assigned to a DHCP client will change to 10.0.18.99 (0000 1010. **0000 0000**. 0001 **0002**. 0110 0011)

h. For this scenario, we want the ED on 130_T_SW_1 to have a static IP, so it is not modified when the switch propagates the train parameters. Only check the **Train ID** option in the **Propagate to the IP Address** for port 1 for switch 130_T_SW_1. This will skip the Car NB for the IP calculation for the end device.

5. On switch 210_T_SW_2, go to **Set Device IP > DHCP/BootP/RARP**.

   a. Configure port 2 with the following parameters. For demonstrational purposes, we will configure this switch to be in a different subnet, as if we plan to relocate this switch to a different train with a different subnet. If configured correctly, Conditional Auto IP Assignment will modify its IP address to be in the subnet of the current train based on the inherited Train ID and Car NB values from the lead switch.

Setting	Value
IP Address	10.1.19.99
Subnet Mask	255.255.240.0
Gateway	10.1.17.253

6. On switch 130_T_SW_1, go to **Set Device IP > DHCP/BootP/RARP**.

   b. Configure port 1 with the following parameters.

Setting	Value
IP Address	10.0.30.99
Subnet Mask	255.255.240.0

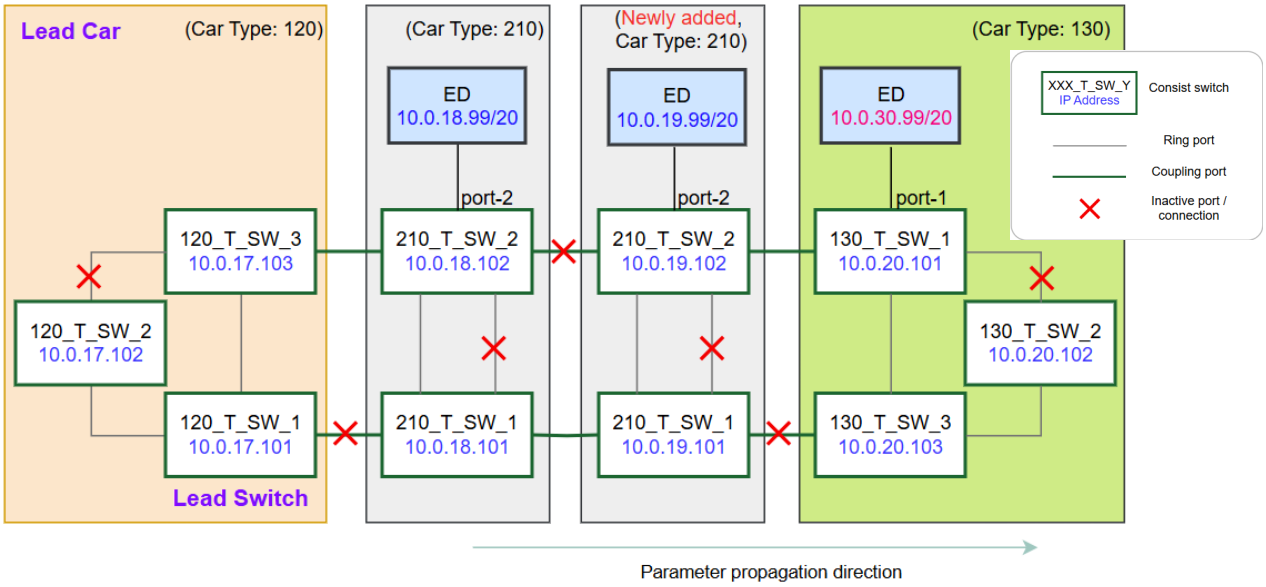
Result: Next time the switches boot up, static IP addresses for switches will be adjusted automatically depending on the specified Train ID and Car NB. The IP assignment process will start at the Lead Switch and will sequentially configure switches until the last switch at the opposite end of the train is configured. When all switches are configured, the Conditional Auto IP Assignment process will be completed. Additionally, because port 1 on switch 130_T_SW_1 did not propagate the Car NB, the static IP address assigned to the connected end device remains unchanged.

NOTE

After the next power cycle, unless the Train ID and Car NB were modified on the lead switch, the Conditional Auto IP Assignment procedure will not trigger.

Scenario 2: Conditional Auto IP assignment with a newly added train car

The following reference diagram illustrates the switch and end device IP assignment when adding a new car train to the train vehicle.



In this scenario, we are building on the original configuration illustrated in **scenario 1** by adding a new train car (Car Type 210) to the existing configuration. The switches in the newly added car are configured identical to the switches in the existing middle car (car type: 210).

For demonstrational purposes, we will assume that the switches have already been preconfigured for Conditional Auto IP Assignment prior to deployment. For reference, the following settings have been configured on the new switches:

- Turbo Ring V2 is enabled and the static coupling settings between cars have been configured.
- **Conditional Auto IP Assignment** is enabled and the **Train ID**, **Car NB**, and timeout values are configured.
- The Train ID and Car NB propagation settings are configured for switches with connected end devices.
- The **Set Device IP** settings are configured for switches with connected end devices to assign an IP address to end devices.

Result: Next time the switches boot up, the switches in all cars will adjust their IP based on the increased Car NB increment. Switch 210_T_SW_2 in the new car adjusted the IP of its connected end device based on the propagated Train ID and Car NB.

> **NOTE**
>
> After the next power cycle, unless the Train ID and Car NB were modified on the lead switch, the Conditional Auto IP Assignment procedure will not trigger.

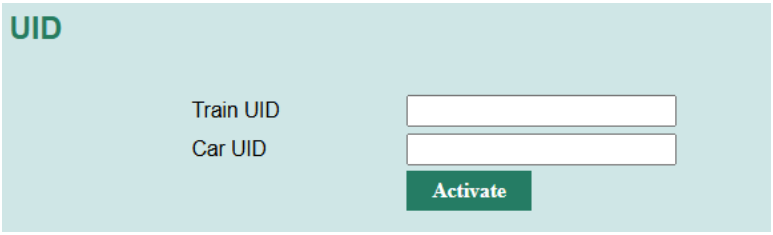
Train Information

In addition to the standard settings, you can configure extra parameters for **Conditional Auto IP Assignment**. The **Train Information** section is separated into two pages: **UID** and **Car Information**.

> **NOTE**
>
> The **Train Information** parameters (Train UID, Car UID, Car Type) are exclusively for user annotation and do not affect functionality in any way.

UID

This page lets you add a train and car unique identifier (UID) to indicate the location of the device in the topology.



Train UID

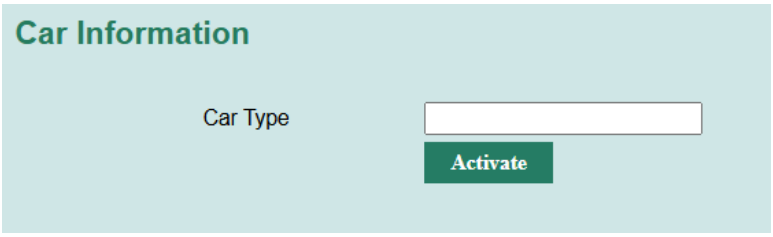
Setting	Description	Factory Default
1 to 32 characters	Specify the Train UID in a format consistent with the device serial number or the consist UUID. Only letters (a-z, A-Z), numbers (0-9), underscores (_), and hyphens (-) are allowed.	None

Car UID

Setting	Description	Factory Default
1 to 32 characters	Specify the Car UID in a format consistent with the device serial number. Only letters (a-z, A-Z), numbers (0-9), underscores (_), and hyphens (-) are allowed	None

Car Information

This page lets you add a description to more easily identify the train car type.



Car Type

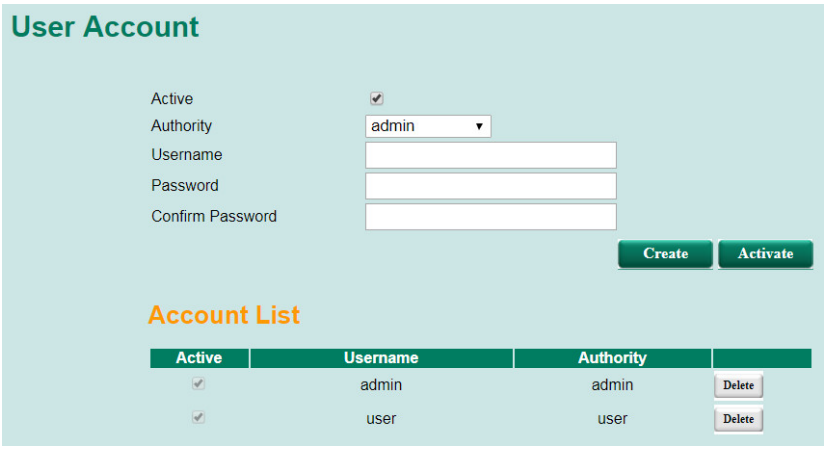
Setting	Description	Factory Default
1 to 16 characters	Enter a description for the train car to more easily identify the car type. Only letters (a-z, A-Z), numbers (0-9), underscores (_), and hyphens (-) are allowed.	None

Password (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.	

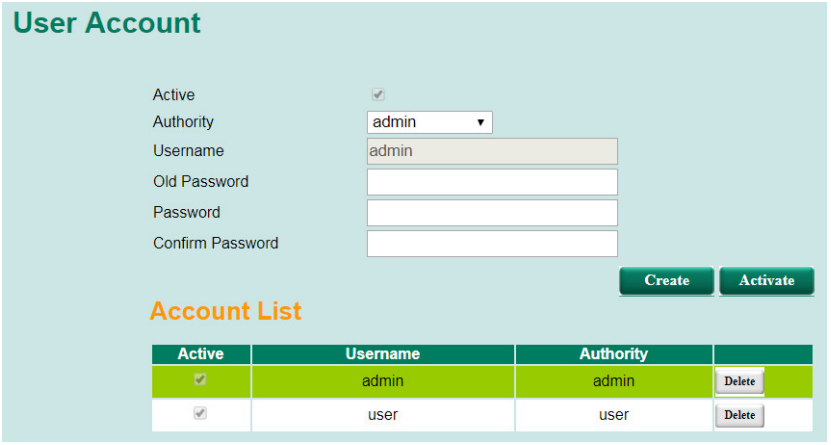
Creating a New Account

Click **Create**, type in the user name 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. 30 characters)	User Name	None
Password	Password for the user account (between 4 and 16 characters)	None

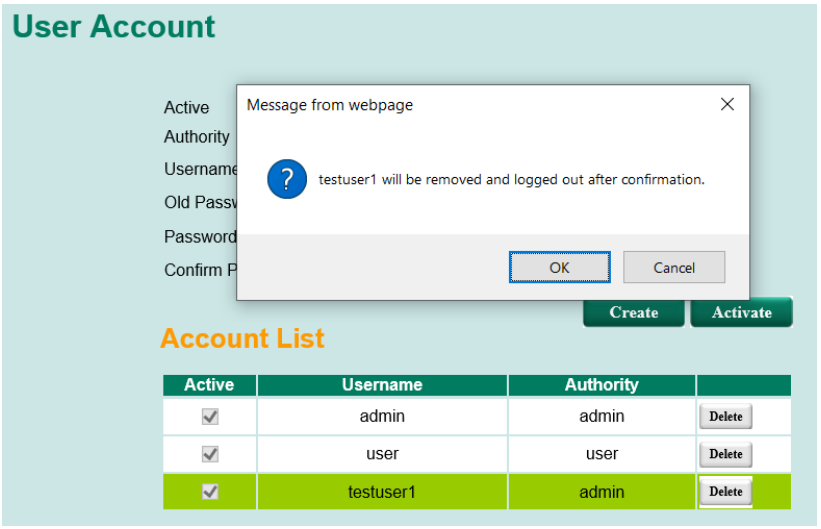
Modifying an Existing Account

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



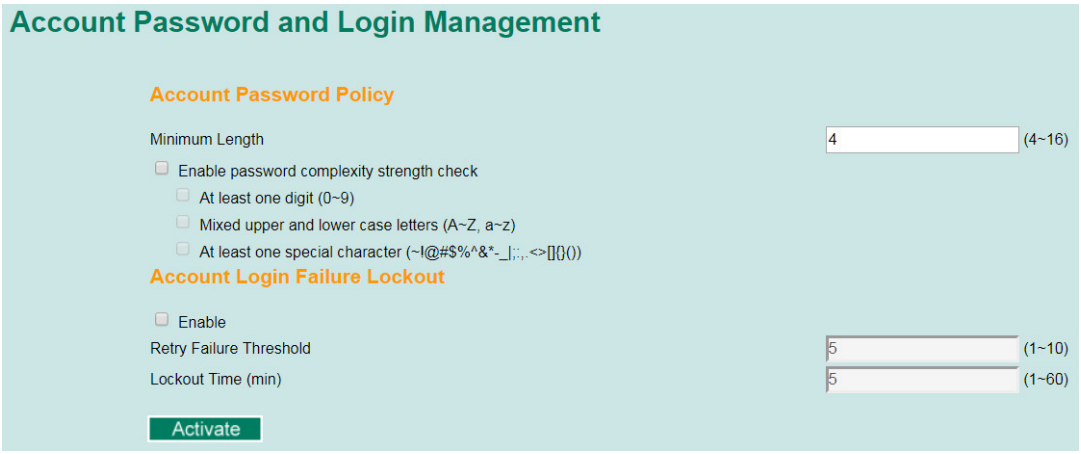
Deleting an Existing Account

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



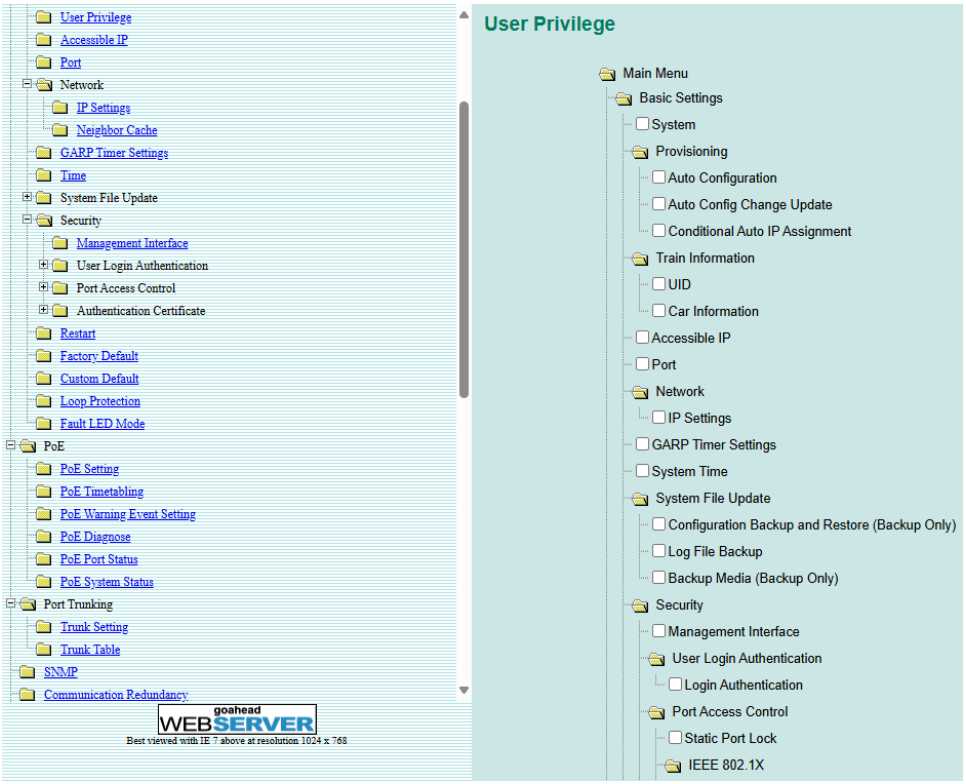
Password Login Policy

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.



User Privilege

This page lets users with administrator (admin) privileges configure write permissions for configuration pages for users with "user" account privileges. To provide more granular and flexible access management, permissions are configured for individual configuration pages.

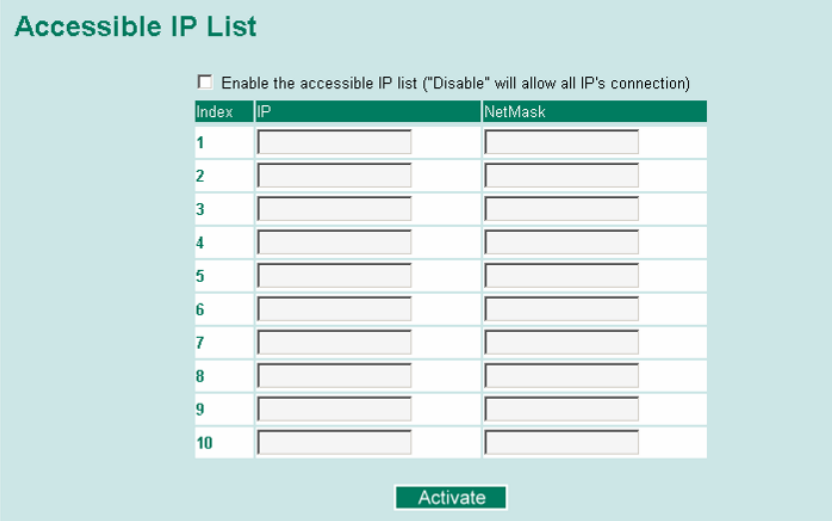


User Privilege

Setting	Description	Factory Default
Checked/Unchecked	Enable or disable writing permissions for the corresponding configuration page for users with "user" privilege. User privileges cannot be configured for the following pages: • Password • Password Login Policy • User Privilege • Neighbor Cache • Firmware Upgrade • Factory Default • Custom Default • PoE Diagnose • PoE Port Status • PoE System Status • Trunk Table • VLAN Table • IGMP Table • GMRP Table • Warning List • Ping • MAC Address Table • Access Control Rule Show	Unchecked

Accessible IP List

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 accessible IP 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 accessible IP list is not enabled. Remove the checkmark from **Enable the accessible IP list**.

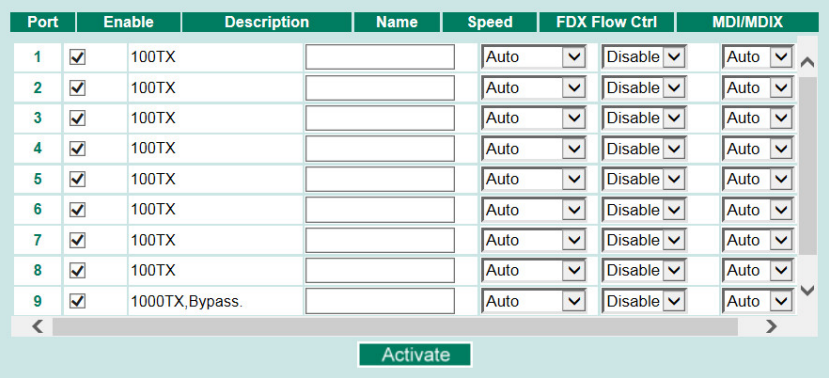
The following table shows additional configuration examples:

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

Port Settings

Ethernet 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.	Enabled
Unchecked	Immediately shuts off port access.	

ATTENTION

If a connected device or sub-network is wreaking havoc on the rest of the network, the **Disable** option under **Advanced Settings/Port** gives the administrator a quick way to shut off access through this port immediately.

Description

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

Name

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
1G-Full	Choose one of these fixed speed options if the connected Ethernet device has trouble auto-negotiating for line speed.	
100M-Full		
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.	

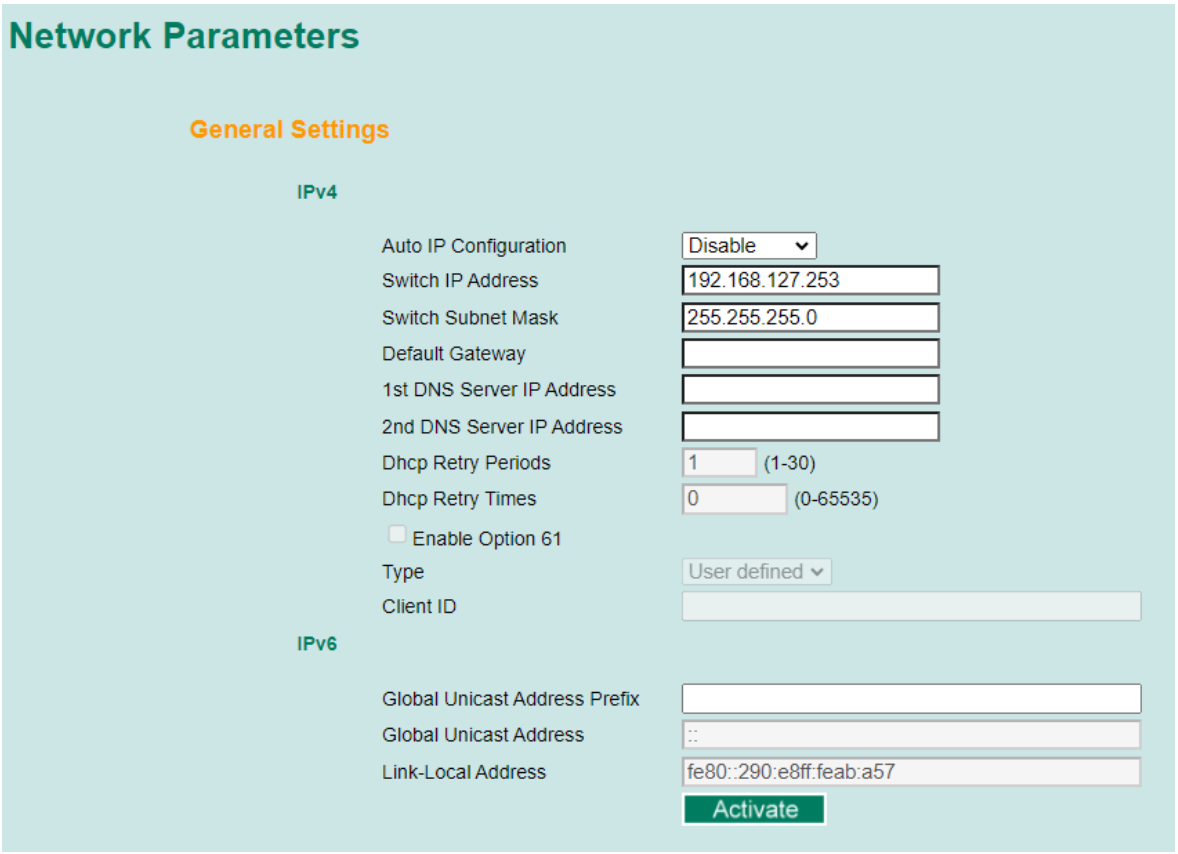
MDI/MDIX

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		

Network Parameters

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.

A brief explanation of each configuration item is given below.



IPv4

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.

Auto IP Configuration

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

Switch 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

Switch 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).	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 IP Address

Setting	Description	Factory Default
IP address for 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
IP address for 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

DHCP Retry Periods

Setting	Description	Factory Default
1 to 30	Users can configure the DHCP retry period manually.	1

DHCP Retry Times

Setting	Description	Factory Default
0 to 65535	Users can configure the times of DHCP retry manually.	0

DHCP Option 61

Setting	Description	Factory Default
Enable/Disable	Enable or disable DHCP Option 61 support.	Disable

DHCP Option 61 Type

Setting	Description	Factory Default
User-defined	Users can configure the DHCP Option 61 value manually.	User-defined
Client ID	This ID is used as a unique identifier for the DHCP client.	None

IPv6

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.

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 the 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

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

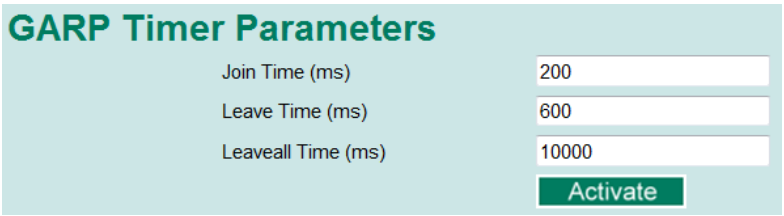
Link-Local Address

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

Neighbor Cache

Setting	Description	Factory Default
None	The information in the neighbor cache that includes the neighboring node's IPv6 address, the corresponding Link-Layer address, and the current state of the entry.	None

GARP Timer Parameters



Join Time

Setting	Description	Factory Default
None	Specifies the period of the join time	200

Leave Time

Setting	Description	Factory Default
None	Specifies the period of leave time	600

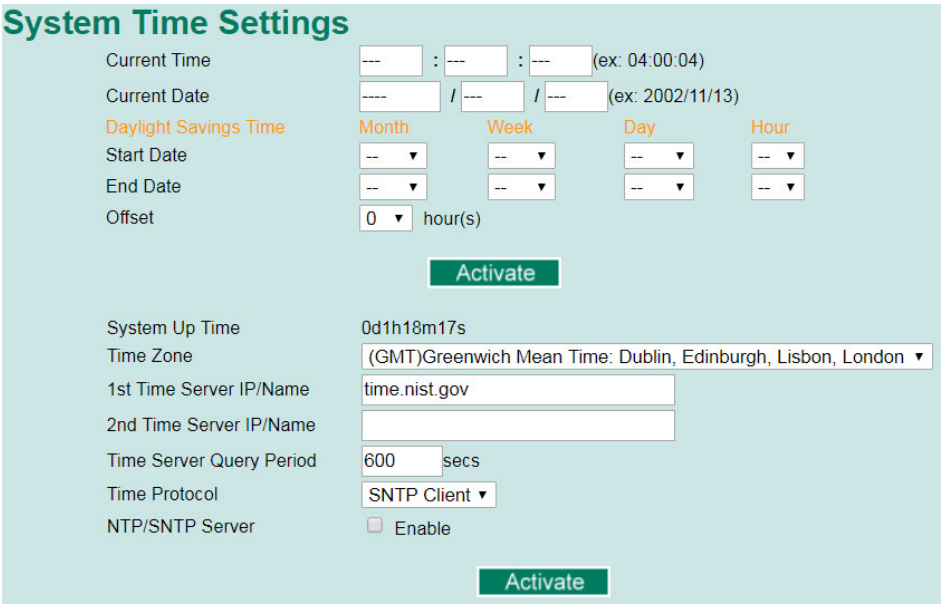
Leaveall Time

Setting	Description	Factory Default
None	Specifies the period of leaveall time	10000

NOTE

Leave Time should be at least two times more than **Join Time**, and **Leaveall Time** should be larger than **Leave Time**.

System Time Settings



The Moxa switch has a time calibration function based on information from an NTP server or user specified time and date. Functions such as automatic warning emails can therefore include 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 NTP server, LAN, or Internet connection.

Current Time

Setting	Description	Factory Default
User-specified time	Allows configuration of the local time in local 24-hour format.	None

Current Date

Setting	Description	Factory Default
User-specified date	Allows configuration of the local date in yyyy-mm-dd format.	None

Daylight Saving Time

The Daylight Saving Time settings are used to automatically set the Moxa switch's time forward 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

System Up Time

Indicates how long the Moxa switch remained up since the last cold start. The up time is indicated in seconds.

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)

NOTE

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

Time Server IP/Name

Setting	Description	Factory Default
IP address or name of time 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 NTP server if the first NTP server fails to connect.	

Time Server Query Period

Setting	Description	Factory Default
1 to 9999 seconds	Specifies the query period of the time server	600 seconds

Time Protocol

Setting	Description	Factory Default
Disable/SNTP Client/NTP Client	Specifies the time protocol	SNTP Client

Enable NTP/SNTP Server

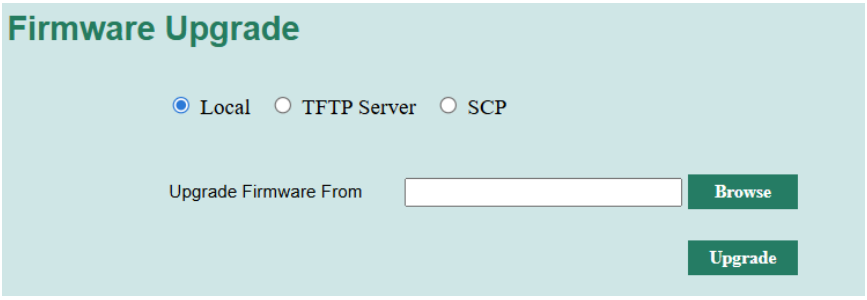
Setting	Description	Factory Default
Enable/Disable	Enables SNTP/NTP server functionality for clients	Disabled

System File Update

Firmware Upgrade

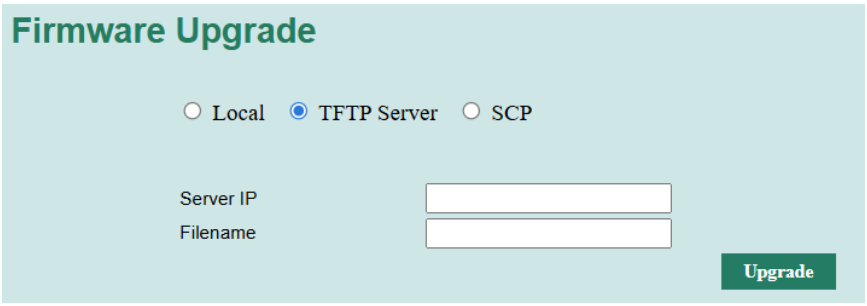
There are two ways to update your Moxa switch’s firmware: from a local *.rom file, and by remote TFTP server.

Local



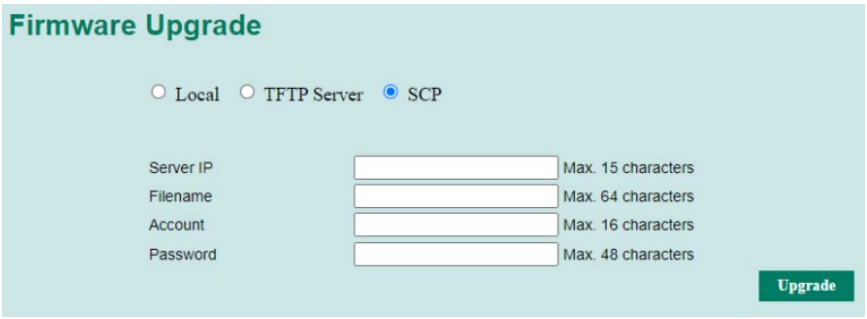
1. Download the updated firmware (*.rom) file from Moxa's website (www.moxa.com).
2. Browse for the (*.rom) file, and then click the **Upgrade** button

TFTP Server



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

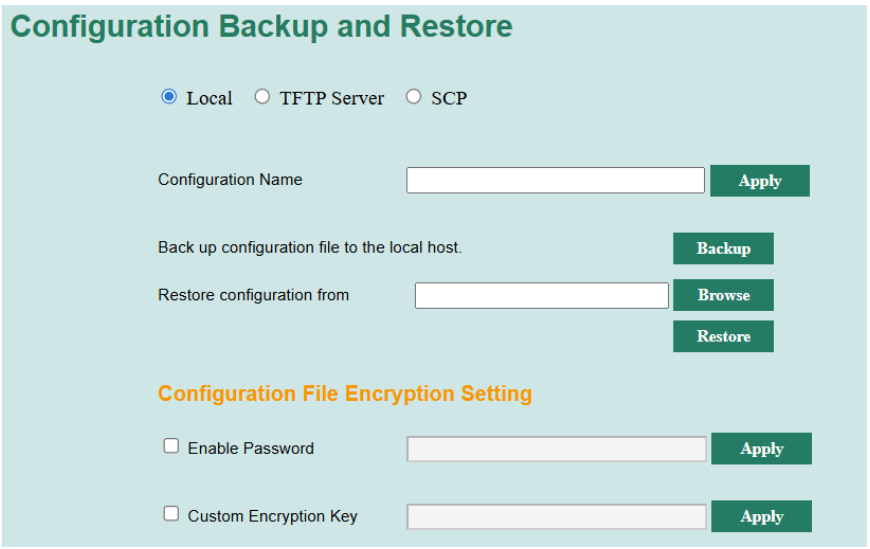
SCP Server



1. Enter the SCP server's IP address.
2. Input the firmware file name (*.rom).
3. Enter the SCP server authentication user account and password.
4. Click the **Upgrade** button.

Configuration Backup and Restore

There are three ways to back up and restore your Moxa switch's configuration: from a local configuration file, by remote TFTP server, or SCP server. From this page, you can also configure the configuration name and file encryption settings.



Method

Setting	Description	Factory Default
Local	Back and restore the configuration from a local file. Refer to **Local**.	Local
TFTP	Back and restore the configuration via a TFTP server. Refer to **TFTP Server**.	
SCP	Back and restore the configuration via an SCP server. Refer to **SCP Server**.	

Configuration Name

The Configuration Name field lets users easily distinguish different configuration file versions. This is useful when maintaining several configuration files with specific settings for different applications. This feature does not act as a version management system and does not support native version numbering. However, users can use this function to label configuration files alongside a user-maintained versioning system.

If a configuration name has been specified, it will also be shown on the **Custom Default** page.

Setting	Description	Factory Default
0 to 32 characters	Enter a name for the configuration. Only letters (a-z, A-Z), numbers (0-9), underscores (_), and hyphens (-) are supported.	None

Enable Password

Setting	Description	Factory Default
0 to 30 characters	Enable or disable the file encryption passphrase. This passphrase encrypts the entire configuration file. If enabled, enter the password.	None

Custom Encryption Key

The Custom Encryption Key is an additional measure to enhance the security of sensitive data stored within configuration files by means of a user-defined encryption key, reducing the risk of unauthorized access. If enabled, the custom encryption will replace the Moxa default encryption key, and the device will use this key for all subsequent password encryption operations.

The custom encryption key covers the following sensitive information:

- Login password
- Auto Configuration SCP password
- Auto Config Change Update SCP password
- SNMPv1, v2c community string
- SNMPv3 data encryption key
- SNMPv3 Trap authentication password
- SNMPv3 Trap encryption Key
- Email warning - account password (SMTP)
- 802.1X - RADIUS shared key

- 802.1X - user password
- Authentication - RADIUS shared key
- Authentication - TACACS+ shared key

Setting	Description	Factory Default
8 characters	Enable or disable the custom encryption key. If enabled, specify the key string. The string length must be exactly 8 characters.	None

NOTE

When using the Custom Encryption Key feature, it is important to note that configuration files encrypted with a custom key cannot be directly imported onto another device unless the same encryption key is specified on the new device. To ensure a smooth import process, follow these two steps:

1. Specify the same Custom Encryption Key on the new device via the web interface or CLI.
2. Import the configuration file encrypted with the custom key.

If done correctly, the new device will be able to decrypt and apply the configuration file correctly.

NOTE

For users who wish to avoid the two-step procedure for setting up the custom encryption key on new devices, an additional parameter, "Custom Encryption Key" can be added to the configuration file to specify the custom encryption key. This allows the new device to automatically configure the encryption key during the configuration import process. When using this approach, ensure that the sensitive data in the configuration file is already encrypted with the specified encryption key specified in the "Custom Encryption Key" parameter. If the encryption key does not match, the import process will fail.

Below is an example of how to specify a custom encryption key in the configuration file:

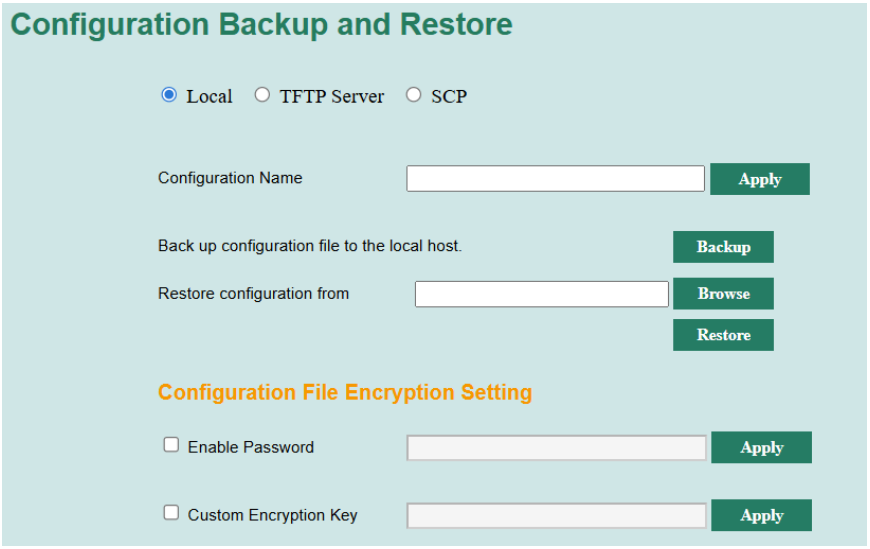
```
[EtherDevice Server Configuration File]
# Model Name
ModelName TN-4520A-16POE-4GPOE-T
Custom Encryption Key Moxa5678
...
```

In this example, the custom encryption key "Moxa5678" is defined using the "Custom Encryption Key" parameter. This key will be used to encrypt sensitive data in the configuration file.

NOTE

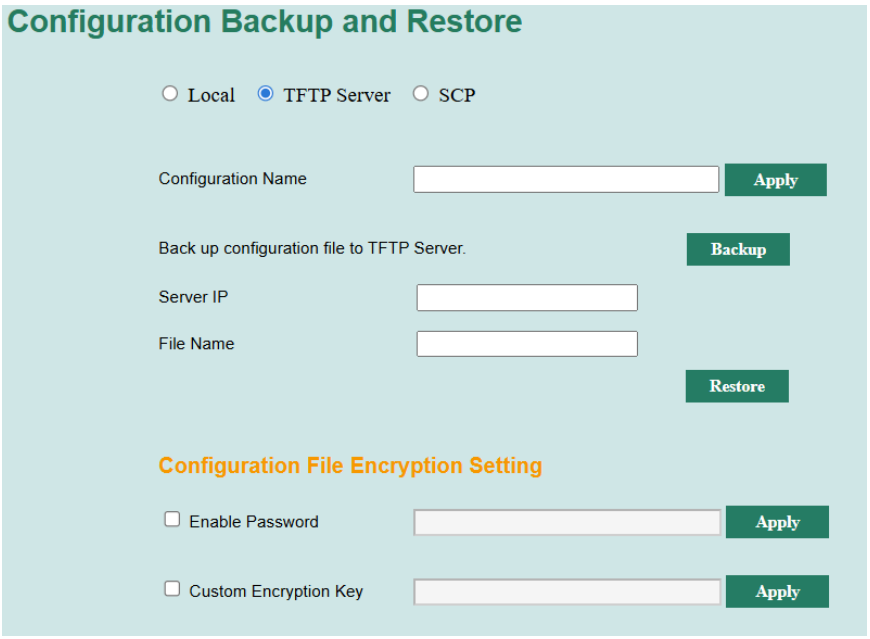
- For security purposes, the Custom Encryption Key will never be exported or displayed in any form. This improves confidentiality and helps prevent the risk of the encryption being obtained by unauthorized users.
- Users are fully responsible for safeguarding the custom encryption key, especially if it is included in the configuration file. Unauthorized access to the key could pose a potential cybersecurity risk. It is strongly recommended to store the configuration file securely and limit access to authorized personnel only.

Local



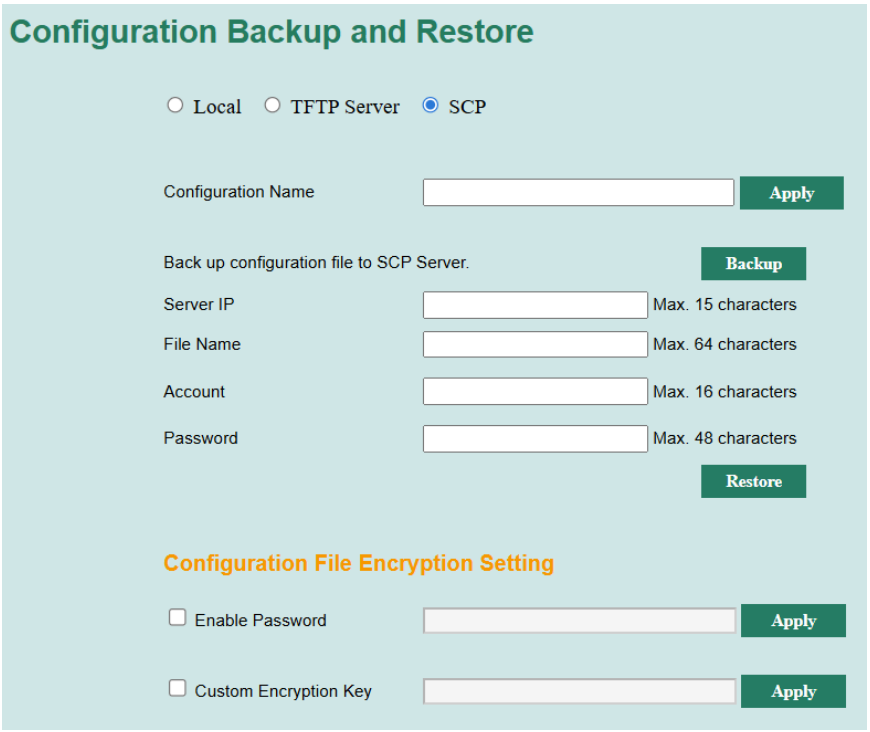
1. Click the **Backup** button to back up the configuration file to a local drive.
2. Browse for a configuration on a local disk, and then click the **Restore** button.

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 Server

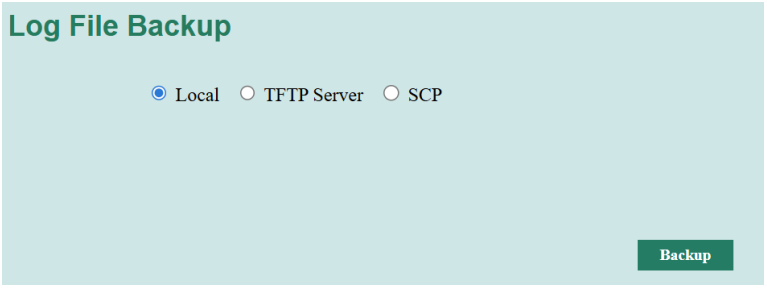


1. Enter the SCP server's IP address.
2. Input the firmware file name (*.rom).
3. Enter the SCP server authentication user account and password.
4. Click the **Restore** button.

Log File Backup

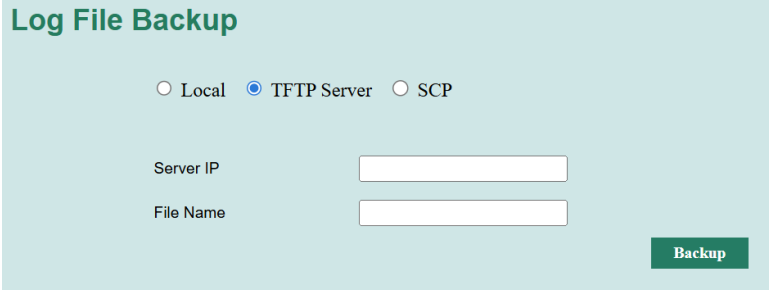
There are two ways to back up Moxa switch's log files: from a local drive and by remote TFTP server.

Local



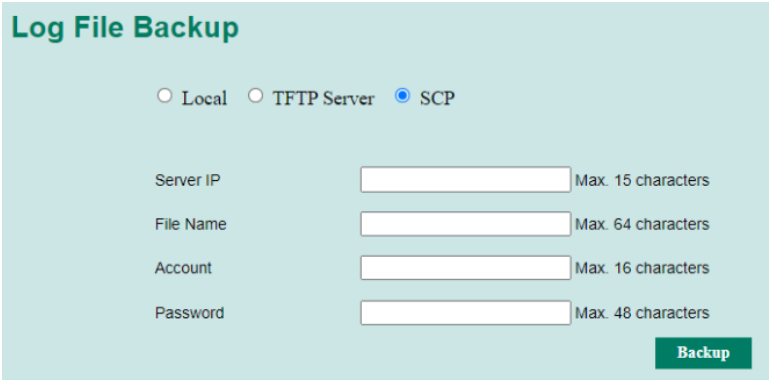
Click the **Backup** button to back up the log file to a local drive.

TFTP Server



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

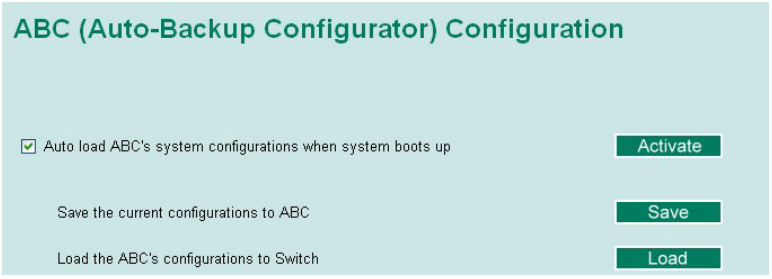
SCP Server



1. Enter the SCP server's IP address.
2. Input the firmware file name (*.rom).
3. Enter the SCP server authentication user account and password.
4. Click the **Backup** button.

ABC (Auto-Backup Configurator) Configuration

You can use Moxa's Automatic Backup Configurator to save and load the Moxa switch's configurations through the switch's RS-232 console port.



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, SSL/SSH Authentication certificate, Login Authentication, Static Port Lock, IEEE 802.1X, Accessible IP, Broadcast Storm Protection, Loop Protection, and Access Control List.

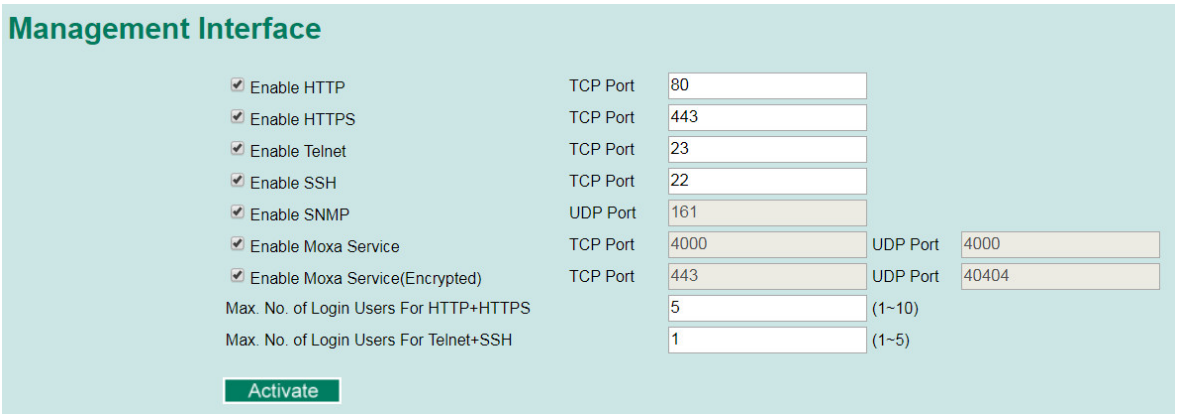
NOTE

Accessible IP, Broadcast Storm Protection, Loop Protection, and Access Control List are described in other chapters.

Management Interface

NOTE

The HTTP and Telnet interfaces transmit data over unsecure, non-encrypted channels. We highly recommend using the secure HTTPS and SSH interfaces instead.



Enable HTTP

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

Enable HTTPS

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

Enable Telnet

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

Enable SSH

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

Enable SNMP

Setting	Description	Factory Default
Select/Deselect	Select the appropriate checkboxes to enable SNMP	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.	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.	TCP Port: 443 UDP Port: 40404

Max. No. of Login Users For HTTP+HTTPS

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

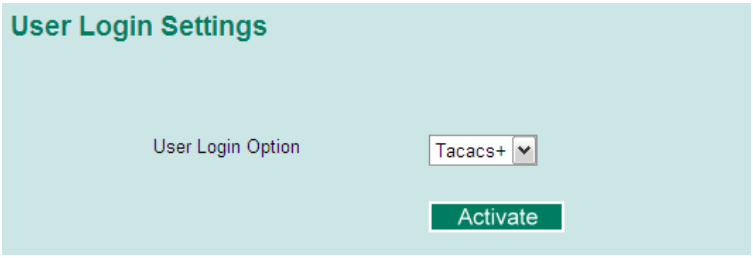
Max. No. of Login Users For Telnet+SSH

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

User Login Authentication

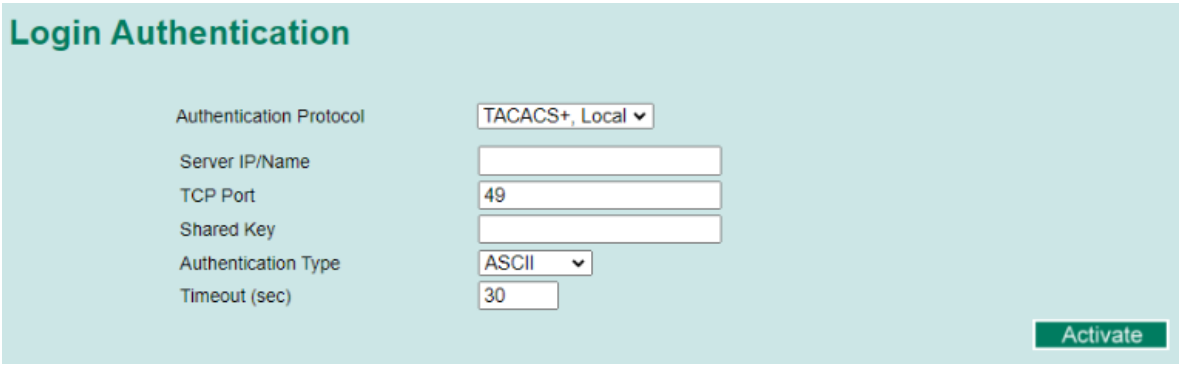
User Login Authentication – User Login Settings

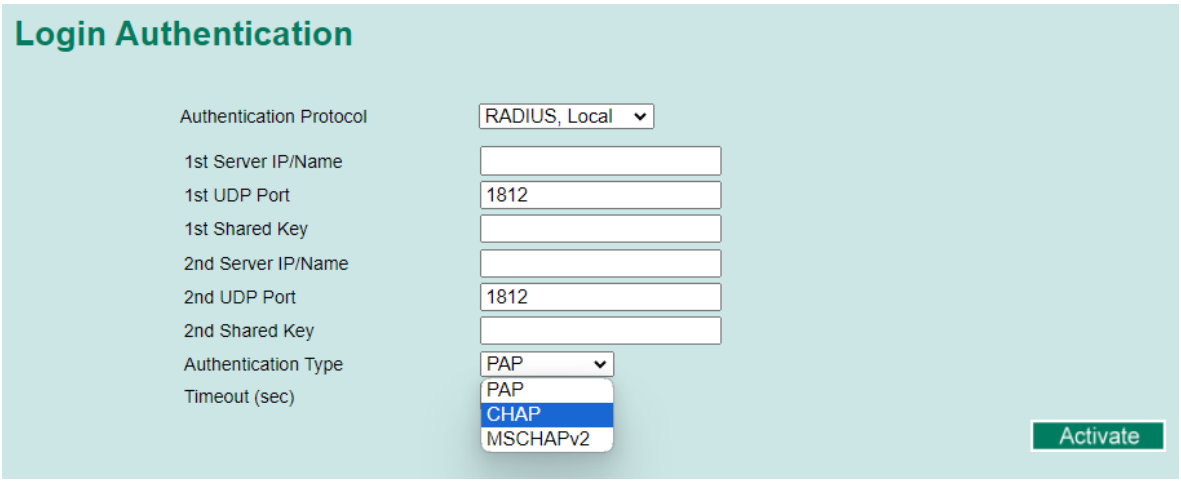
Both TACAS+ and RADIUS are options here.



User Login Authentication – Auth Server Setting

The detailed configuration settings of TACACS+ and RADIUS are displayed in the table below:





Setting	Description	Factory Default
Authentication Protocol	Select the authentication type: TACACS+, Local and RADIUS, Local.	TACACS+, Local
Server IP/Name	Set IP address of an external TACACS+/RADIUS server as the authentication database.	Localhost
TCP Port	Set the communication port of an external TACACS+ server as the authentication database.	TACACS+: 49
Shared Key	Set specific characters for server authentication verification.	None
1st server IP/Name	Set the IP address of the 1st external RADIUS server as the authentication database.	None

Setting	Description	Factory Default
1st UDP port	Set a communication port of the 1st external RADIUS server as the authentication database.	RADIUS: 1812
1st shared key	Set specific characters for the 1st external RADIUS server authentication verification.	None
2nd server IP/Name	Set the IP address of the 2nd external RADIUS server as the authentication database.	None
2nd UDP port	Set a communication port of the 2nd external RADIUS server as the authentication database.	RADIUS: 1812
2nd shared key	Set specific characters for the 2nd external RADIUS server authentication verification.	None
Authentication Type	The authentication mechanism used between the authentication server and client.	TACACS+: ASCII RADIUS: PAP, CHAP, MSCHAPv2
Timeout	Specify the timeout period to wait for a server response.	TACACS+: 30 RADIUS: 5

Port Access Control

The Moxa switch provides two kinds of Port-Based Access Control: Static Port Lock and IEEE 802.1X.

Static Port Lock

In this case, the Moxa switch can also be configured to protect static MAC addresses for a specific port. With the Port Lock function, these locked ports will not learn any additional addresses, but only allow traffic from preset static MAC addresses, helping to block hackers and careless usage.

IEEE 802.1X

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.

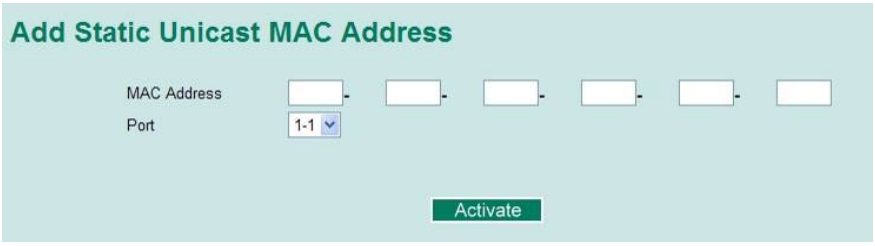
Authenticator: Edge switch or wireless access point that acts as a proxy between the supplicant and the authentication server, requesting identity information from the supplicant, verifying the information with the authentication server, and relaying a response to the supplicant.

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 between each other.

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.

Configuring Static Port Lock

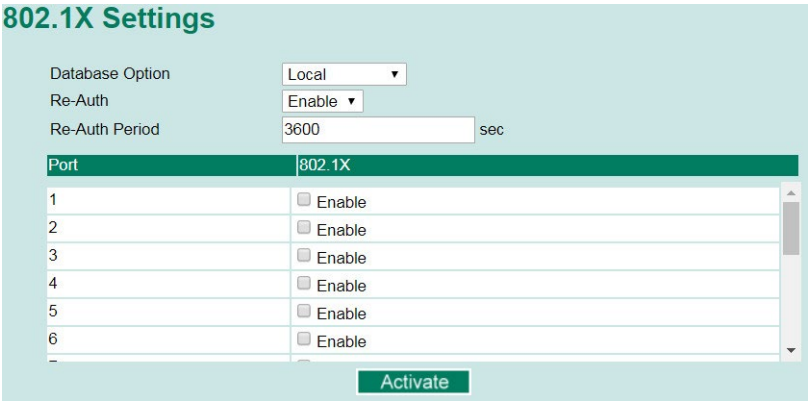
The Moxa switch supports adding unicast groups manually if required.



Static Unicast MAC Address

Setting	Description	Factory Default
MAC Address	Adds the static unicast MAC address into the address table.	None
Port	Associates the static address to a dedicated port.	1 or 1-1

Configuring IEEE 802.1X



Database Option

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

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

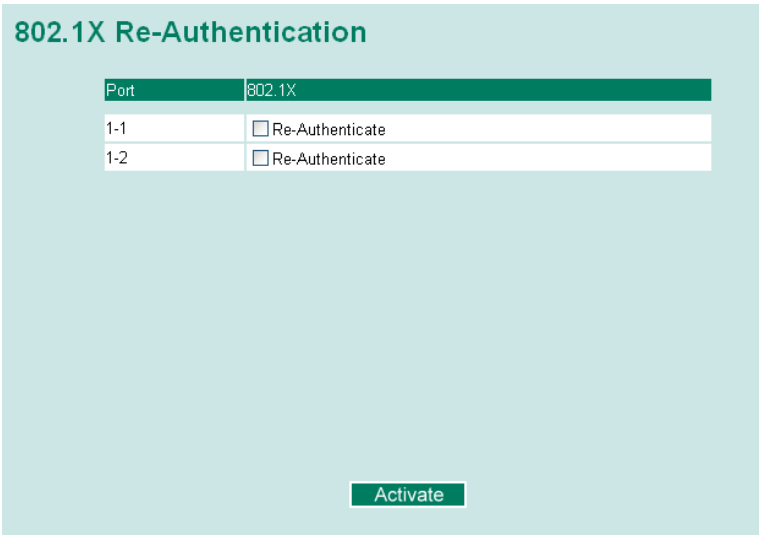
Setting	Description	Factory Default
Numerical (60 to 65535 sec.)	Specify how frequently the end stations need to reenter usernames and passwords in order to stay connected.	3600

802.1X

Setting	Description	Factory Default
Enable/Disable	Checkmark 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.	Disable

802.1X Re-Authentication

The Moxa switch can force connected devices to be re-authorized manually.

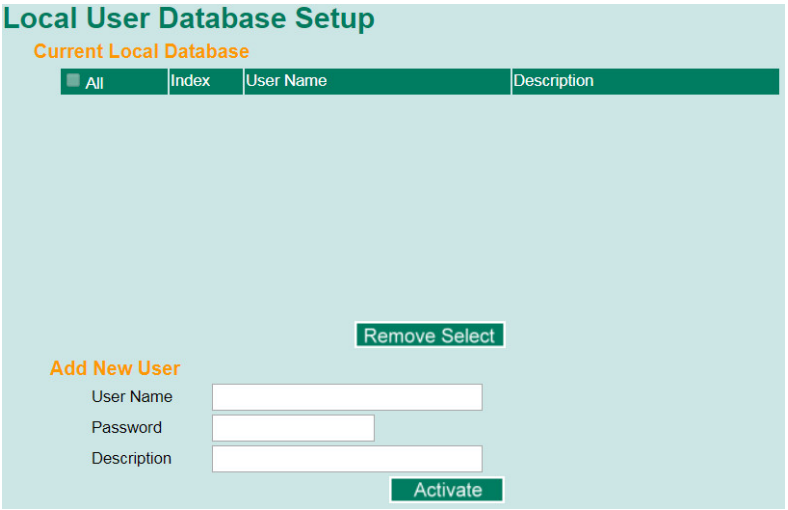


802.1X Re-Authentication

Setting	Description	Factory Default
Enable/Disable	Enables or disables 802.1X Re-Authentication	Disable

Local User Database Setup

When setting the Local User Database as the authentication database, set the database first.



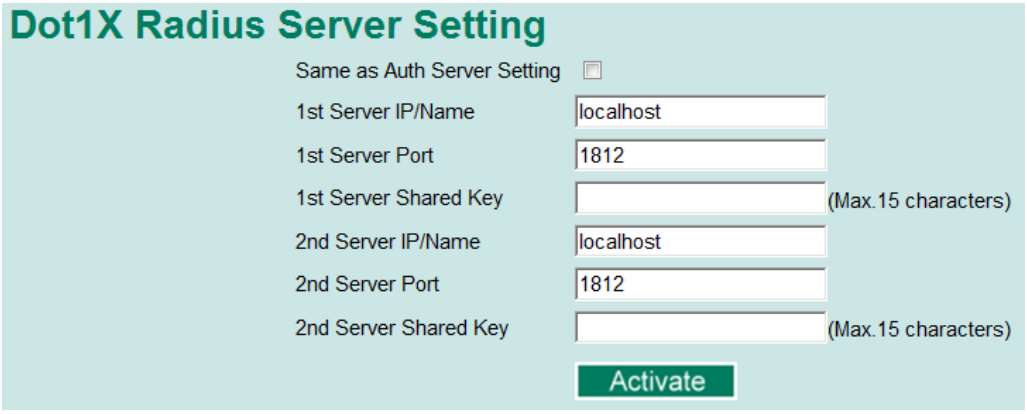
Local User Database Setup

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

NOTE

The user name for the Local User Database is case-insensitive.

Dot1X Radius Server Setting



Same as Auth Server Setting

Setting	Description	Factory Default
Enable/Disable	Enable to use the same setting as Auth Server	Disable

Server Setting

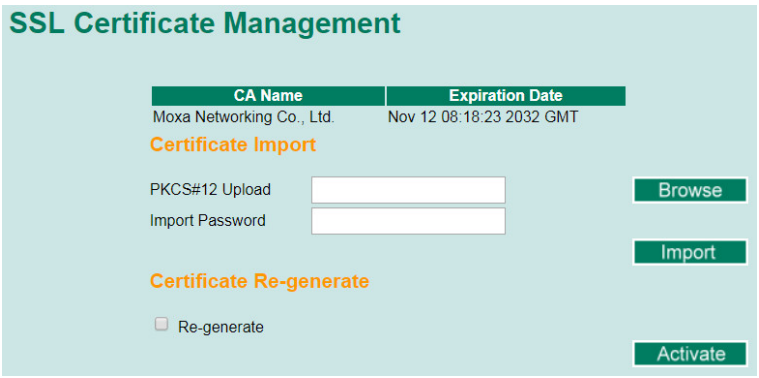
Setting	Description	Factory Default
Server IP/Name	Specifies the IP/name of the server	localhost
Server Port	Specifies the port of the server	1812
Server Shared Key	Specifies the shared key of the server	None

Port Access Control Table

The port status will show authorized or unauthorized.

Authentication Certificate

SSL Certificate Management



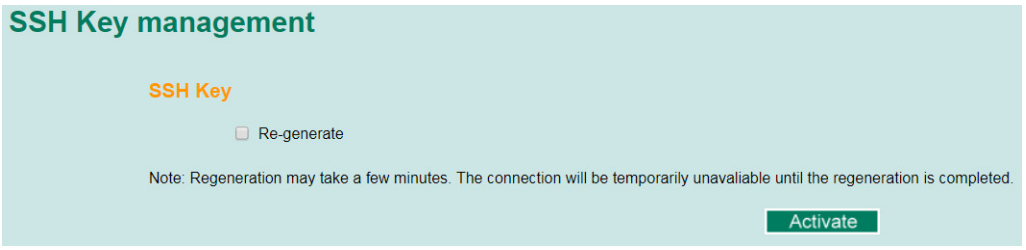
Certificate Import

- Click **Browse** and select Public-Key Cryptography Standard PKCS#12 certificate file
- Enter the **Import Password** and click **Import**
- The SSL certificate will be updated

Certificate Re-generate

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

SSH Key Management



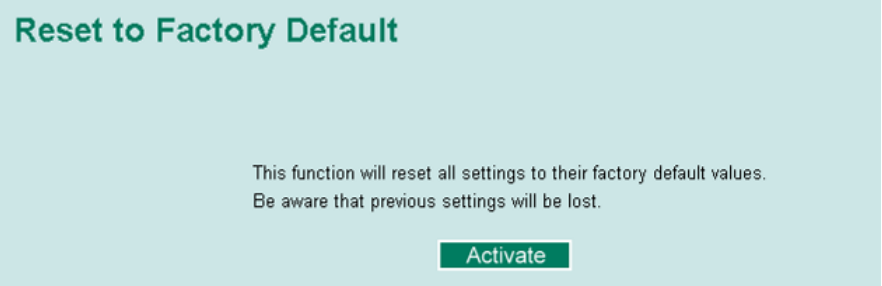
SSH Key Re-generate

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

Restart

This function provides users with a quick way to restart the system.

Reset to Factory Default



This function provides users with a quick way of restoring the Moxa switch's configuration to factory defaults. The function is available in the serial, Telnet, and web consoles.

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.

Custom Default

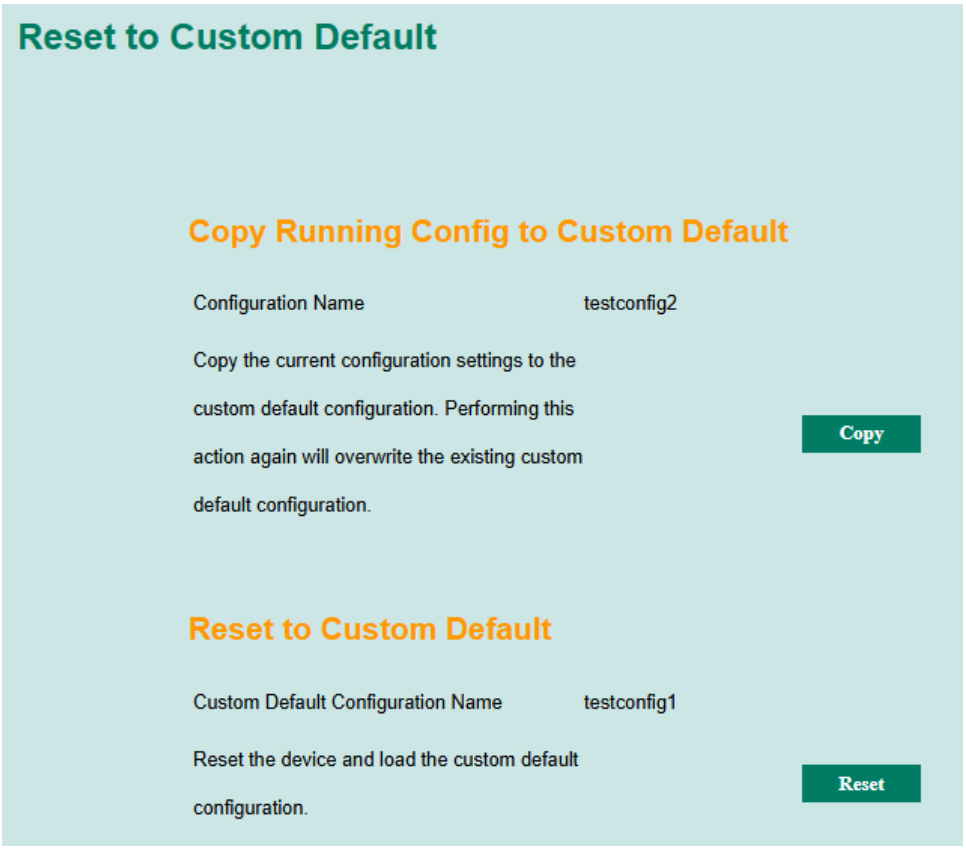
This function allows you to save the current startup configuration to the non-volatile memory as a custom default configuration. When set, the custom default configuration overwrites the Moxa factory default configuration. The device will load the custom default settings after restarting.

NOTE

The device can only hold one custom default configuration at any given time.

NOTE

Resetting to factory default settings will clear the custom default settings and revert to the Moxa factory-default settings. Refer to **Reset to Factory Default** for more information.



The **Configuration Name** shows the currently saved running configuration if specified on the **Configuration Backup and Restore** page. If no backup configuration is saved, this field will be blank. We recommend specifying a configuration name to more easily identify the configuration.

Click **Copy** to copy the current running configuration to the custom default settings. This will also overwrite any existing custom default configuration.

The **Custom Default Configuration Name** shows the currently applied custom default configuration. If no running configuration name is specified, this field will be blank.

Click **Reset** to restart the device and load the custom default settings. This will take effect immediately without confirmation prompt. If no custom default configuration is saved, clicking **Reset** will not have any effect.

Loop Protection

The switch is designed with a loop checking mechanism whereby it sends a control BPDU from the Ethernet port and checks if this control BPDU will be sent back to the switch again. If the looping occurs, the switch will automatically block the Ethernet port to prevent looping.

Enable Loop Protection

Setting	Description	Factory Default
Enable/Disable	Enable/Disable the Loop Protection Function	Disable

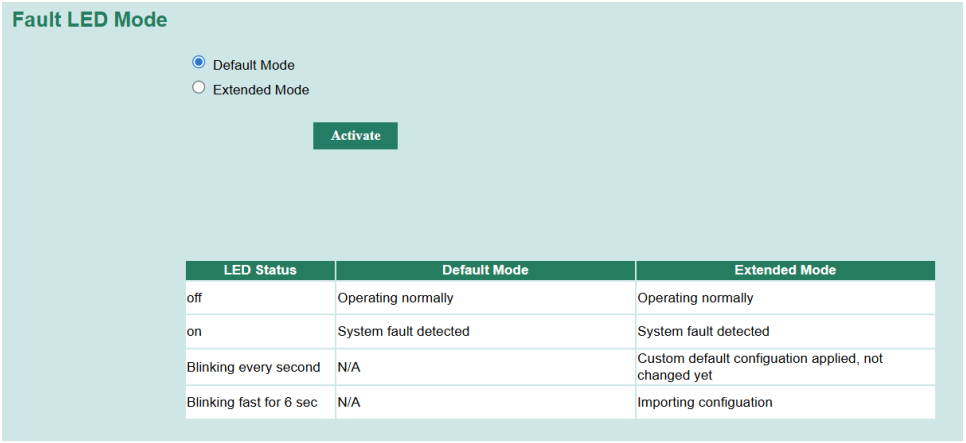
Fault LED Mode

This page lets you configure the display mode of the device's Fault LED.

- **Default Mode**: In this mode, the Fault LED only has two statuses (on/off). This is the default mode.
- **Extended Mode**: Besides on/off, the Fault LED will show additional blinking patterns to visually indicate the status of configuration changes. This mode makes it easier for maintenance staff to verify if the configuration was imported and applied successfully.

Select the Fault LED mode and click **Activate**.

> **NOTE**
>
> This function will only take effect after applying the Custom Default function. Refer to **Custom Default**.



LED Status	Default Mode	Extended Mode
off	Operating normally	Operating normally
on	System fault detected	System fault detected
Blinking every second	N/A	Custom default configuation applied, not changed yet
Blinking fast for 6 sec	N/A	Importing configuation

Using Port Trunking

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.

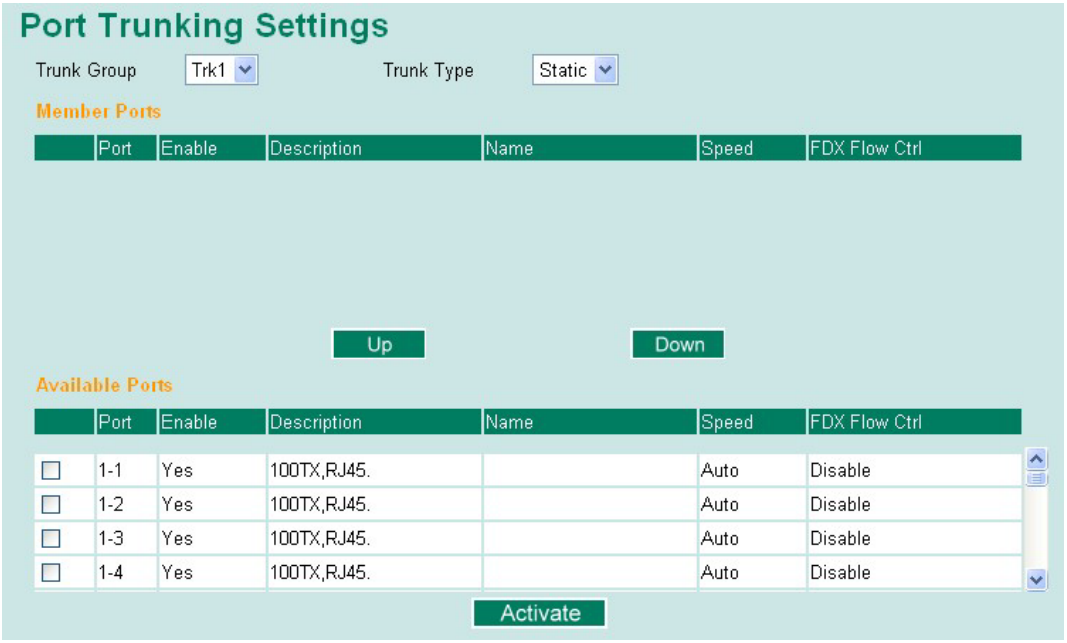
Each Moxa switch can set a maximum of 4 port trunking groups. When you activate port trunking, certain settings on each port will be reset to factory default values or disabled:

- 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 Settings

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 desired ports under **Available Ports** and click **Up** to add to the Trunk Group.

Step 4: Select the desired ports under **Member Ports** and click **Down** to remove from the group.

Trunk Group (maximum of 4 trunk groups)

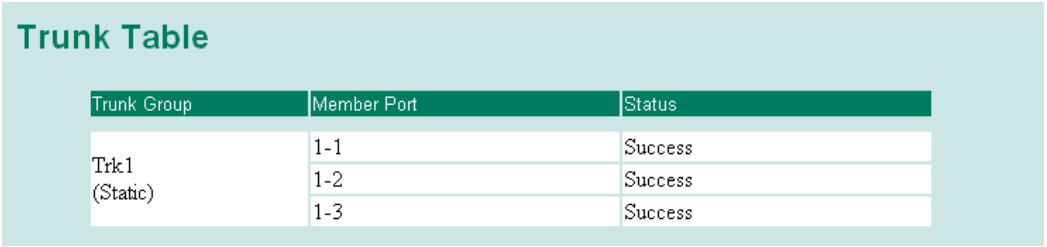
Setting	Description	Factory Default
Trk1, Trk2, Trk3, Trk4 (depends on switching chip capability; some Moxa switches only support 3 trunk groups)	Specifies the current trunk group.	Trk1

Trunk Type

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

Available Ports/Member Ports

Setting	Description	Factory Default
Member/Available ports	Lists the ports in the current trunk group and the ports that are available to be added.	N/A
Check box	Selects the port to be added or removed from the group.	Unchecked
Port	How each port is identified.	N/A
Port description	Displays the media type for each port.	N/A
Name	Displays the specified name for each port.	N/A
Speed	Indicates the transmission speed for each port (1G-Full, 100M-Full, 100M-Half, 10M-Full, or 10M-Half).	N/A
FDX flow control	Indicates if the FDX flow control of this port is enabled or disabled.	N/A
Up	Add selected ports into the trunk group from available ports.	N/A
Down	Remove selected ports from the trunk group.	N/A



Trunk Table

Setting	Description
Trunk group	Displays the trunk type and trunk group.
Member port	Displays the member ports that belong to the trunk group.
Status	• Success means port trunking is working properly. • Fail means port trunking is not working properly.

Configuring 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.

ATTENTION

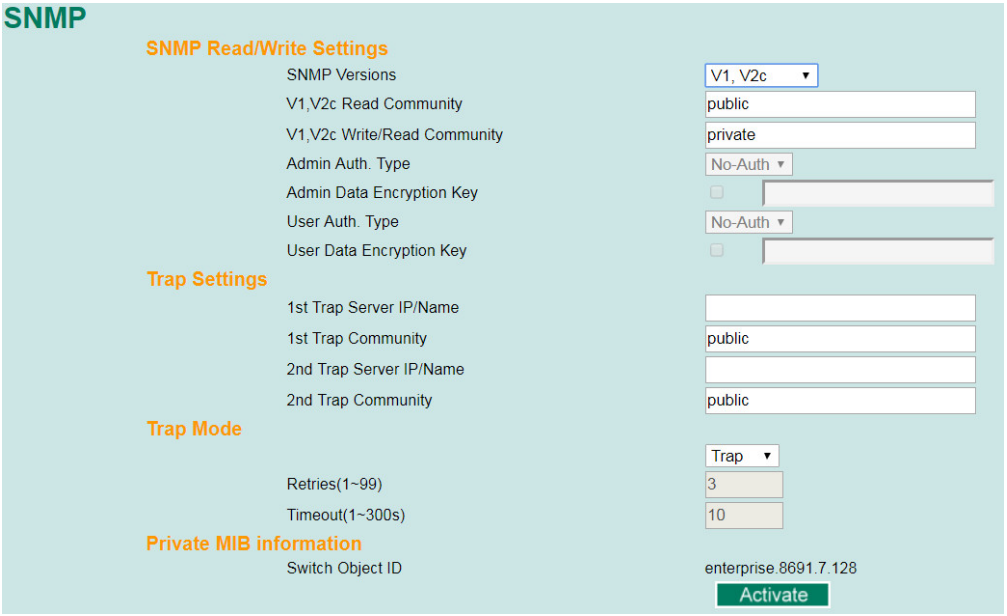
For security reasons, we strongly recommend changing the default community strings and device password when using the device for the first time.

Using the default community strings and password may expose the device to malicious users.

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.
SNMP V3	No-Auth	No	No	Uses an account with admin or user to access objects
	MD5 or SHA	Authentication based on MD5 or SHA	No	Provides authentication based on HMAC-MD5, or HMAC-SHA algorithms. (Note: The website login password must be at least 8-characters and must be set up in advance)
	MD5 or SHA	Authentication based on MD5 or SHA	Data encryption key	Provides authentication based on HMAC-MD5 or HMAC-SHA algorithms, and data encryption key. (Note: The website login password must be at least 8-characters and must be set up in advance)

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 accessing the Moxa switch. **Admin** privilege provides access and authorization to read and write the MIB file. **User** privilege allows reading of the MIB file only.

Admin Auth. Type (for SNMP V1, V2c, V3, and V3 only)

Setting	Description	Factory Default
No-Auth	Allows the admin account to access objects without authentication.	No
MD5-Auth	Authentication will be based on the HMAC-MD5 algorithms. 8-character passwords are the minimum requirement for authentication.	No
SHA-Auth	Authentication will be based on the HMAC-SHA algorithms. 8-character passwords are the minimum requirement for authentication.	No

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

Setting	Description	Factory Default
Enable	Enables data encryption using either DES, AES 128, or AES 256 encryption.	No
Disable	Specifies that data will not be encrypted.	No

User Auth. Type (for SNMP V1, V2c, V3 and V3 only)

Setting	Description	Factory Default
No-Auth	Allows the admin account and user account to access objects without authentication.	No
MD5-Auth	Authentication will be based on the HMAC-MD5 algorithms. 8-character passwords are the minimum requirement for authentication.	No
SHA-Auth	Authentication will be based on the HMAC-SHA algorithms. 8-character passwords are the minimum requirement for authentication.	No

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

Setting	Description	Factory Default
Enable	Enables data encryption using either DES, AES 128, or AED 256 encryption.	No
Disable	No data encryption	No

Trap 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

In Trap mode, the SNMP agent sends an SNMPv1 trap PDU to the NMS. No acknowledgment is sent back from the NMS so the agent has no way of knowing if the trap reached the NMS.

SNMP Trap Mode—Inform

SNMPv2 provides an inform mechanism. When an inform message is sent from the SNMP agent to the NMS, the receiver sends a response to the sender acknowledging receipt of the event. This behavior is similar to that of the get and set requests. If the SNMP agent does not receive a response from the NMS for a period of time, the agent will resend the trap to the NMS agent. The maximum timeout time is 300 sec (default is 10 seconds), and the maximum number of retries is 99 times (default is 3 times). When the SNMP agent receives acknowledgement from the NMS, it will stop resending the inform messages.

1st Trap Server IP/Name

Setting	Description	Factory Default
IP or name	Specifies the IP address or name of the primary trap server used by your network.	None

1st Trap Community

Setting	Description	Factory Default
Max. 30 characters	Specifies the community string to use for authentication.	Public

2nd Trap Server IP/Name

Setting	Description	Factory Default
IP or name	Specifies the IP address or name of the secondary trap server used by your network.	None

2nd Trap Community

Setting	Description	Factory Default
Max. 30 characters	Specifies the community string to use for authentication.	Public

Private MIB Information

Switch Object ID

Setting	Description	Factory Default
Specific Moxa Switch ID	Indicates the Moxa switch's enterprise value.	Depends on switch model type

NOTE

The Switch Object ID cannot be changed.

Using PoE (PoE Models Only)

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

Power over Ethernet can be used with:

- 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 into 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, 24 VDC direct power input, and 20 ms fast recovery redundancy, Turbo Ring and Turbo Chain.

Please note that two types of PoE function settings are available, depending on the specific model of switch.

Type	Models Supported
Type 1	TN-5524 Series, TN-5800A Series
Type 2	TN-5508A Series, TN-5510A Series, TN-5516A Series, TN-5518A Series
Type 3	TN-4516A Series, TN-4524A Series, TN-4528A Series

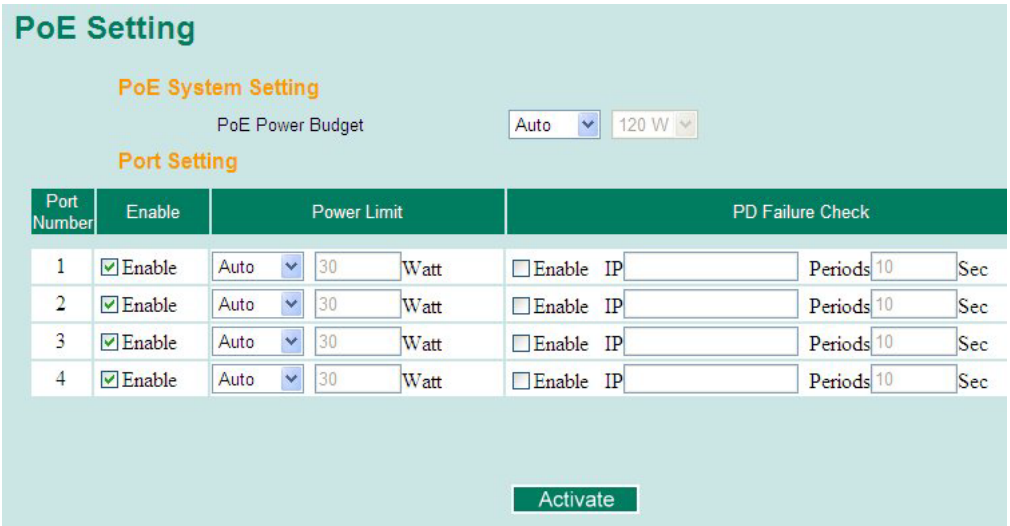
Patent http://www.moxa.com/doc/operations/Moxa_Patent_Marking.pdf

Type 1

PoE Setting

The settings are included to give the user control over the system's PoE power budget, PoE port access, PoE port power limit and PD failure check.

An explanation of each configuration item follows:



PoE Power Budget

Indicates the PoE power that can be supplied by the system

Setting	Description	Factory Default
Auto	Allows users to set the actual Power Limit value by each individual PoE port.	Auto
Manual	The user can set the power limit value that indicates the power supplied by the system.	

Port Setting

Enable

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

Power Limit

Setting	Description	Factory Default
Auto	The amount of power assigned is determined according to the class that is read from the powered device.	Auto
Manual	The user can set the power limit value that indicates the maximum amount of power available to the port.	Auto

The PoE Ethernet switch can monitor PD working status via its IP conditions. If the PD fails, the switch will not receive a PD response after the defined period, and the authentication process is restarted. This is an excellent function to ensure your network reliability and reduce management burden.

PD Failure Check

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

IP

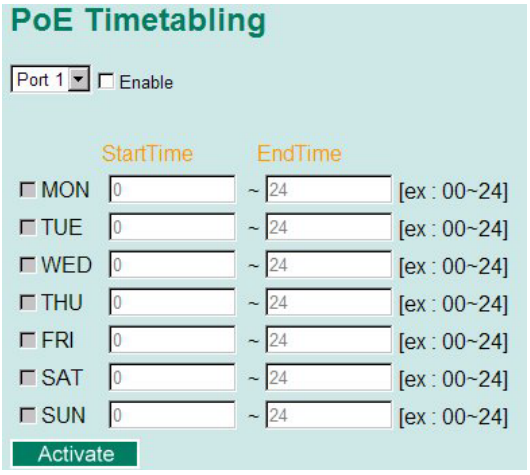
Setting	Description	Factory Default
Max. 15 Characters	Enter the IP for the PD	None

Period

Setting	Description	Factory Default
Max. 5 Characters	Enter the time span for IP checking period	None

PoE Timetabling

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



Port

Setting	Description	Factory Default
Port	Enable a dedicated port	Port 1

Enable

Setting	Description	Factory Default
Checked	Enables the port for a defined time period	Disable
Unchecked	Disables the port for a defined time period	

Weekly Timetabling

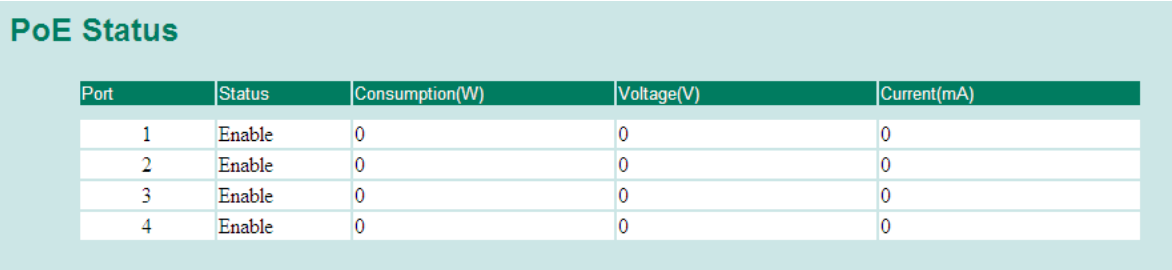
Day

Setting	Description	Factory Default
Checked	Enables the port for a defined number of days	Disable
Unchecked	Disables the port for a defined number of days	

Start/End Time

Setting	Description	Factory Default
Time for working period	Allows users to enter the start and end time for the PD's working period	0-24

PoE Status

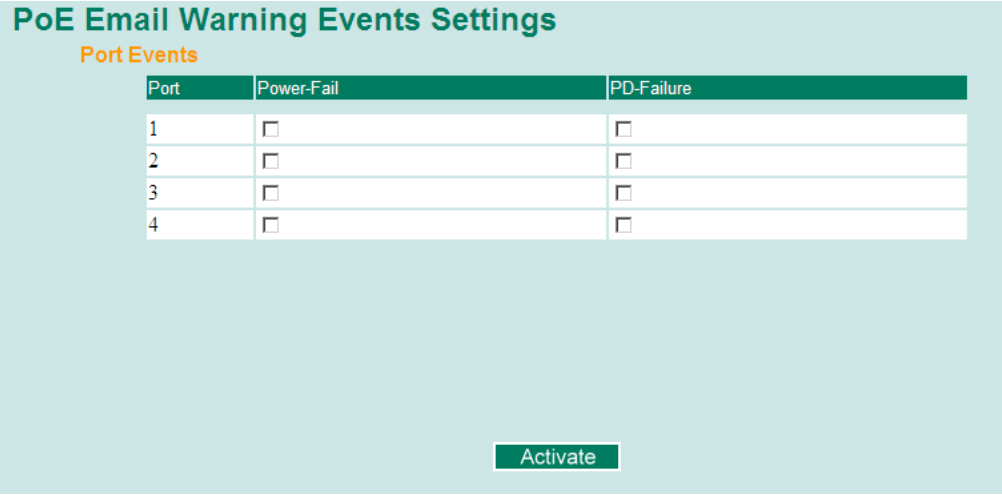


Item	Description
Enable/Disable	Indicates the PoE port status
Consumption (W)	Indicates the actual Power consumed value for PoE port
Voltage (V)	Indicates the actual Voltage consumed value for PoE port
Current (mA)	Indicates the actual Current consumed value for PoE port

PoE Email Warning Events 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, such as email and relay output. It also supports two digital inputs to integrate sensors into your system to automate alarms using email and relay output.

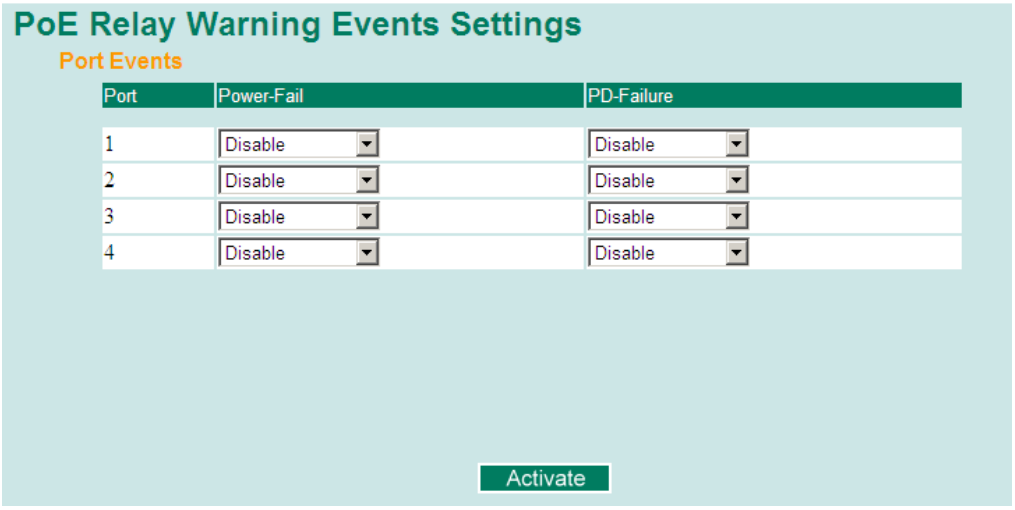
Email Warning Event Types can be divided into two basic groups: Power-Fail and PD-Failure.



Port Events	Warming e-mail is sent when...
Power-Fail	When actual PD power consumption exceeds related PD power limit setting.
PD-Failure	When the switch cannot receive a PD response after the defined period.

PoE Relay Warning Events Settings

Relay Warning Event Types can be divided into two basic groups: Power-Fail and PD-Failure.



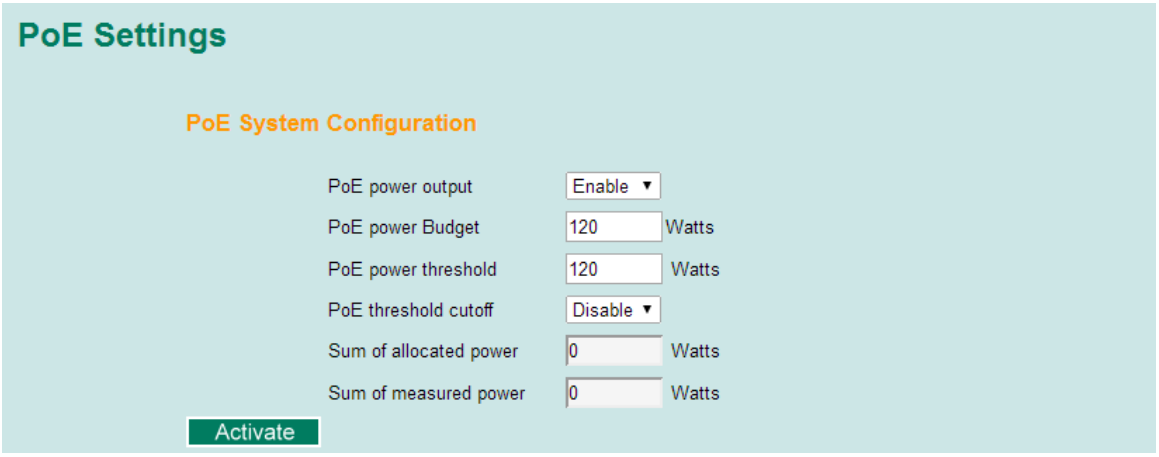
Port Events	Warning e-mail is sent when…
Power-Fail	When actual PD power consumption exceeds related PD power limit settings.
PD-Failure	When the switch cannot receive a PD response after the defined period.

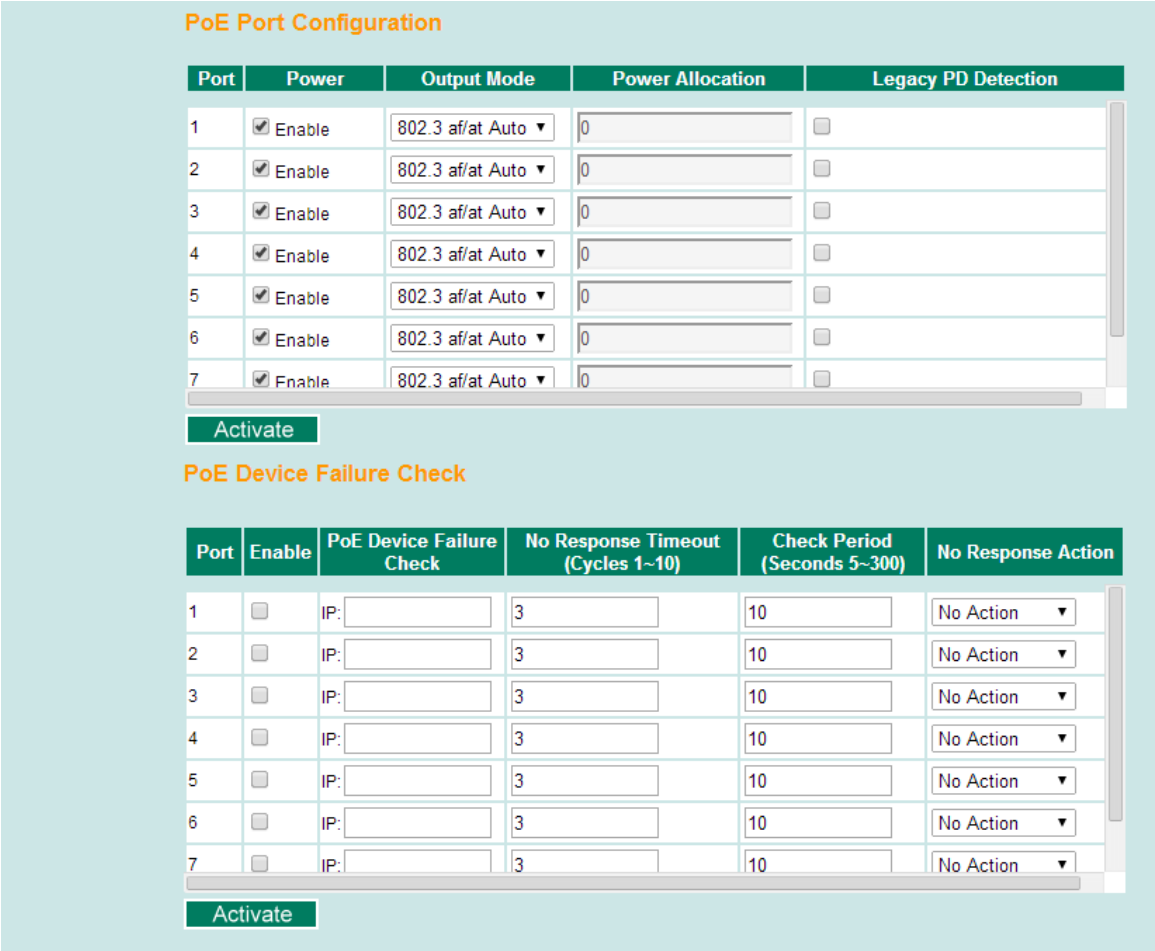
Type 2

PoE Setting

The setting are included to give the user control over the system's PoE power output, PoE power threshold, PoE port configuration, and PD failure check.

An explanation of each configuration item follows:





PoE System Configuration

PoE power output

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

PoE power budget

Setting	Description	Factory Default
120	It shows the total PoE power budget of the switch	120

PoE power threshold

Setting	Description	Factory Default
30 to 120	Set the threshold of total PoE power output	120

PoE threshold cutoff

Setting	Description	Factory Default
Enable	Cutoff the PD's power while its over the threshold	Disable
Disable	No cutoff while the PD's power over the threshold	

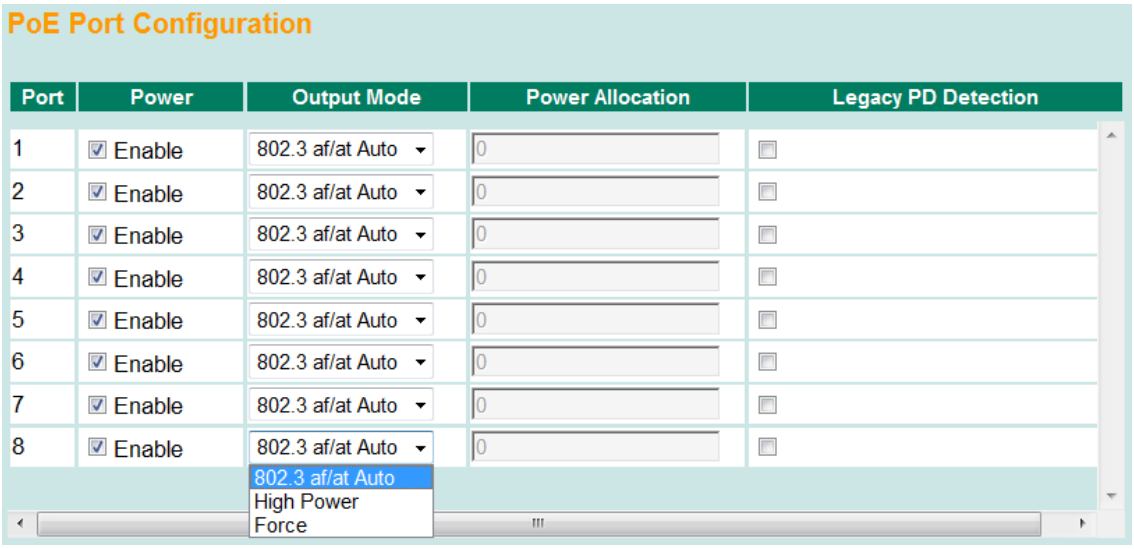
Sum of allocated power

Setting	Description
Allocated power	This item shows the total allocated power of PDs

Sum of measured power

Setting	Description
Measured power	This item shows the total measured power of PDs

PoE Port Configuration



Power

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

Output Mode

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

Power Allocation

Setting	Description	Factory Default
0 to 36	In the Force output mode, the power allocation can be set from 0 to 36 Watts	36

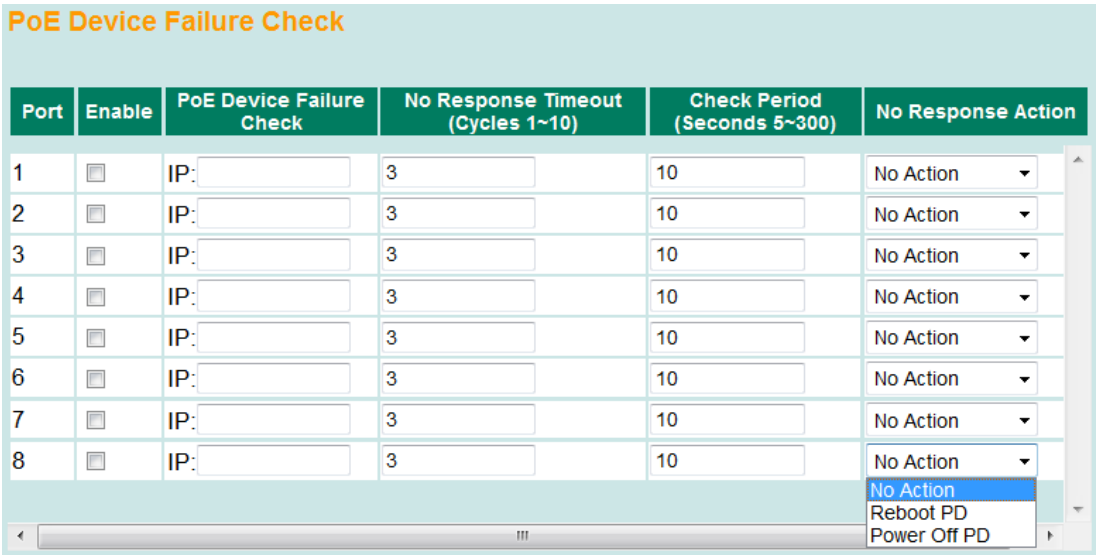
Legacy PD Detection

The PoE Ethernet Switch provides the **Legacy PD Detection** function. When the capacitance of PD is higher than 2.7μF, checking the **Legacy PD Detection** enables system to output power to PD. If you check the Legacy PD Detection, it will take longer detection time from 10 to 15 seconds before PoE power output.

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

PoE Device Failure Check

The PoE Ethernet Switch can monitor PD working status via its IP conditions. If the PD fails, the switch will not receive a PD response after the defined period, and the authentication process is restarted. This is an excellent function to ensure your network reliability and reduce management burden.



Enable

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

PoE Device IP Address

Setting	Description	Factory Default
Max. 15 Characters	Enter the IP for the PD	None

No Response Timeout

Setting	Description	Factory Default
1 to 10	Enter the cycles for IP checking	3

Check Period

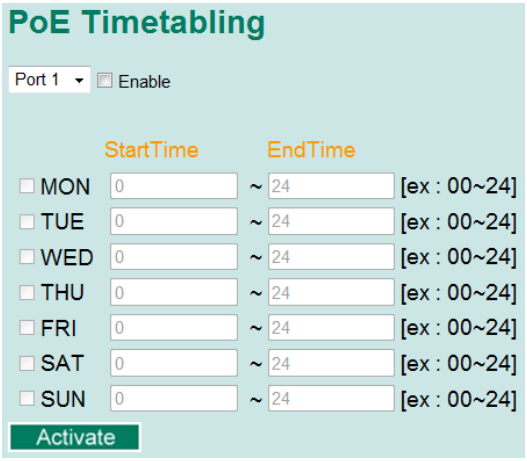
Setting	Description	Factory Default
5 to 300	Enter the time span for IP checking period	10

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 to let users set a flexible working schedule for each PoE port to economize the system's power burden.



Port

Setting	Description	Factory Default
Port	Enable a dedicated port	Port 1

Enable

Setting	Description	Factory Default
Checked	Enables the port for a defined time period	Disable
Unchecked	Disables the port for a defined time period	

Weekly Timetabling

Day

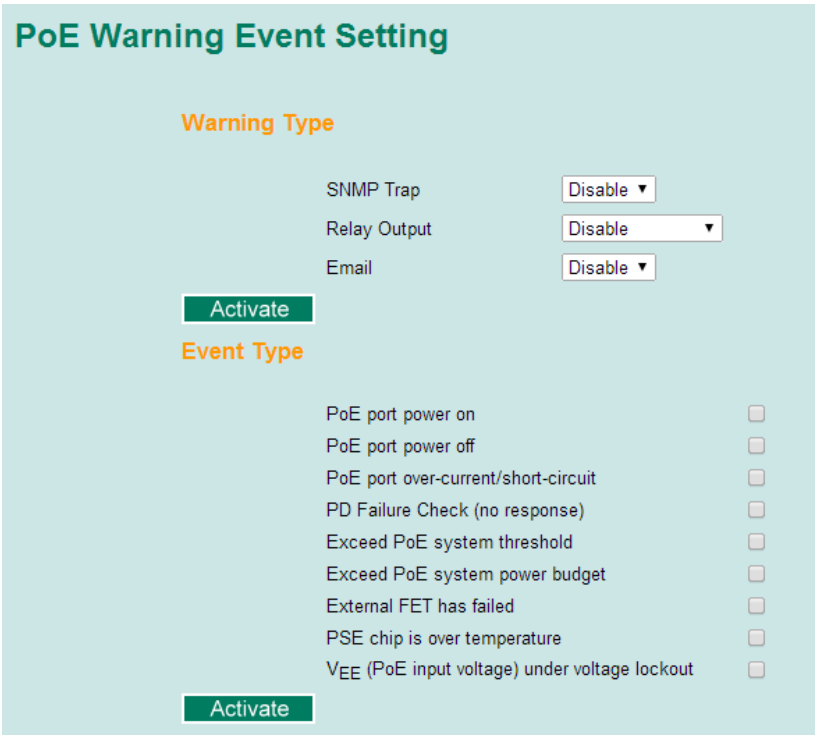
Setting	Description	Factory Default
Checked	Enables the port for a defined number of days	Disable
Unchecked	Disables the port for a defined number of days	

Start/End Time

Setting	Description	Factory Default
Time for working period	Allows users to enter the start and end time for the PD's working period	0 to 24

PoE Warning Event Setting

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, such as SNMP trap, email, and relay output. It also supports two digital inputs to integrate sensors into your system to automate alarm using email and relay output.



Warning Type

SNMP Trap

Setting	Description	Factory Default
Enable	Enables the SNMP trap function of PoE warning	Disable
Disable	Disables the SNMP trap function of PoE warning	

Relay Output

Setting	Description	Factory Default
Enable	Enables the relay output function of PoE warning*	Disable
Disable	Disables the relay output function of PoE warning	

*__Enable (relay 1)__ and __Enable (relay 2)__ can be selected if the switch supports multi-relay output (i.e., the TN-5500A PoE series).

Email

Setting	Description	Factory Default
Enable	Enables the email alarm function of PoE warning	Disable
Disable	Disables the email alarm function of PoE warning	

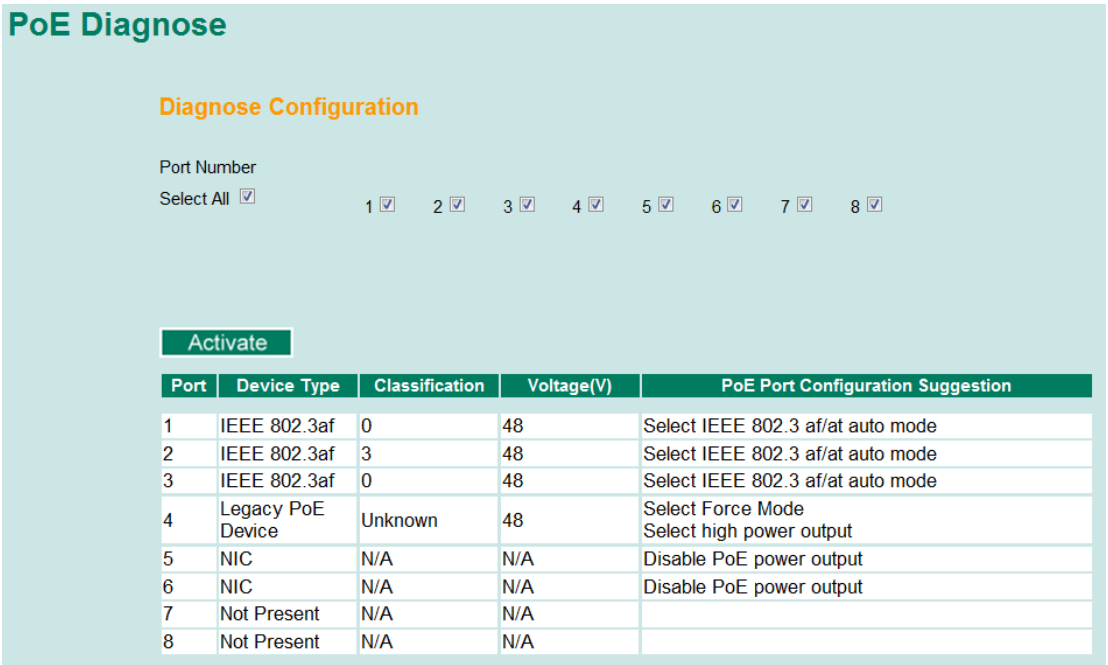
Event Type

Port Events	Description
PoE port power on	Power outputs to PD
PoE port power off	Cut off PoE power output
PoE port over-current/short-circuit	When the current of the port exceeds the limitation: 802.3 af – 350mA 802.3 at – 600mA High Power – 720mA Force – 600mA
PD Failure Check (no response)	When the switch cannot receive a PD response after the defined period
Exceed PoE system threshold	When sum of all PD power consumption exceeds the threshold of total PoE power output
Exceed PoE system power budget	When "sum of allocated power" exceeds the PoE power budget
External FET has failed	When the MOSFET of the port is out of order, please contact Moxa for technical service
PSE chip is over temperature	Please check the environmental temperature. If it is over 75oC, please operate the switch at an adequate temperature. If not, please contact Moxa for technical service.
V_{EE} (PoE input voltage) under voltage lockout	The voltage of the power supply drops down below 44VDC. Adjust the voltage between 46 and 57VDC to eliminate this issue.

NOTE

The Relay Output does not support three Event Types: **External FET has failed, PSE chip is over temperature**, and **V_{EE} (PoE input voltage) under voltage lockout**.

PoE Diagnose



PoE Diagnose helps users to figure out the PD conditions, and the system provides users configuration suggestions to select the best setting for the PDs.

Following steps help users to diagnose the PD conditions:

Step 1: Check the port numbers which will be diagnosed

Step 2: Click **Activate**

Step 3: The system shows the selected PD conditions

Diagnose Configuration

Port Number

Setting	Description	Factory Default
Checked	Enable the port to diagnose	Unchecked
Unchecked	Disable the port to diagnose	

Device Type

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

Classification

Item	Description
N/A	No classification on the port
0 to 4	Class from 0 to 4
Unknown	Unknown class to the port, normally higher than class 4

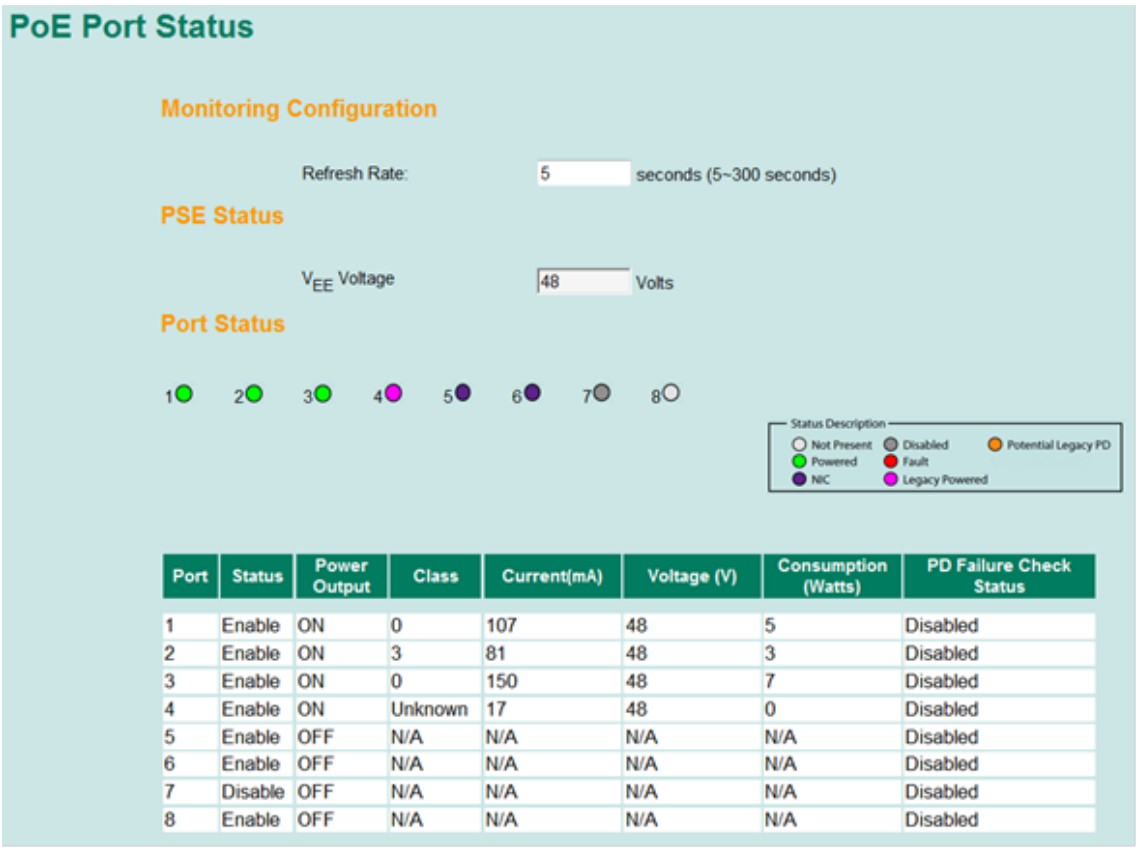
Voltage (V)

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 an 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 802.3 af/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 external power supply voltage > 46 VDC	When detecting the external supply voltage is below 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
1	Enable	ON	0	107	48	5	Disabled
2	Enable	ON	3	81	48	3	Disabled
3	Enable	ON	0	150	48	7	Disabled
4	Enable	ON	Unknown	17	48	0	Disabled
5	Enable	OFF	N/A	N/A	N/A	N/A	Disabled
6	Enable	OFF	N/A	N/A	N/A	N/A	Disabled
7	Disable	OFF	N/A	N/A	N/A	N/A	Disabled
8	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 which the system refreshes the PoE Port Status	5

PSE Status

VEE Voltage

Setting	Description	Factory Default
Read-only	Display the VEE supply voltage of PSE	None

NOTE

The TN-5500A PoE series does not provide VEE voltage information.

PoE Port Status

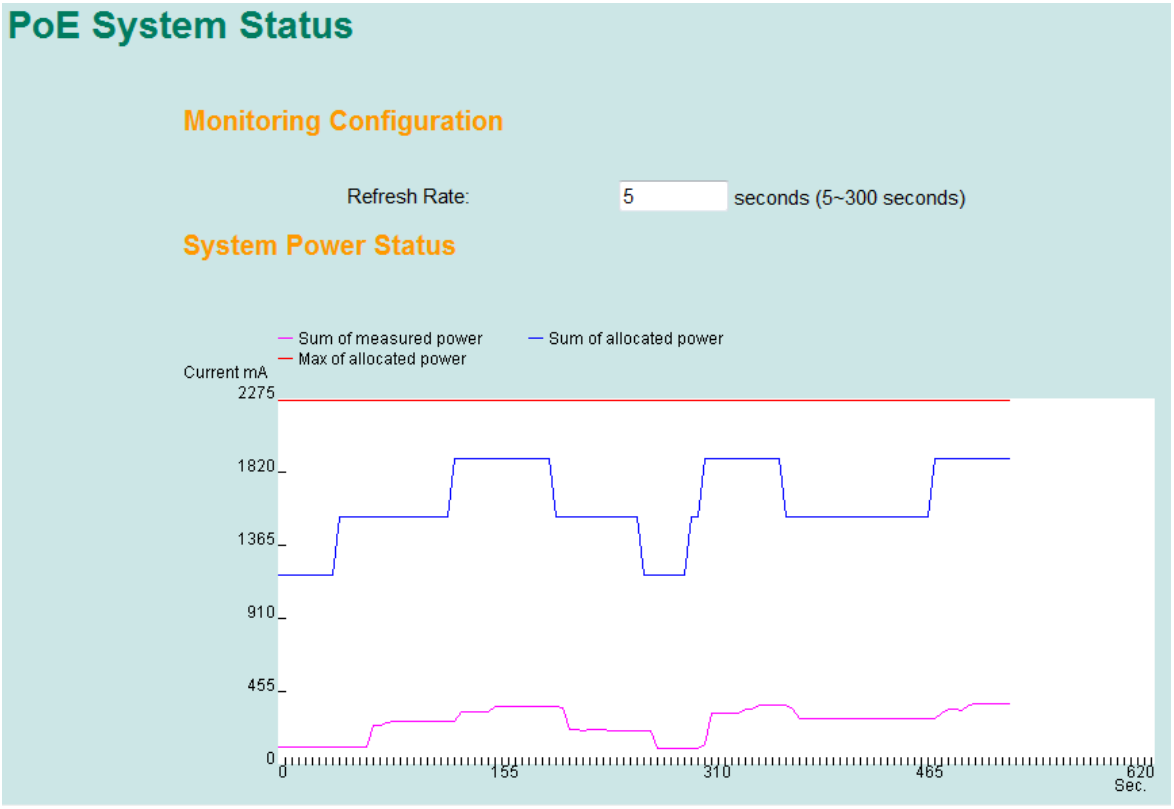
Status Description

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

Port Description

Item	Description
Status	Indicates if the PoE function is enable
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 value of each PoE port
Voltage (V)	Indicates the actual Voltage consumed value of each PoE port
Consumption (Watts)	Indicates the actual Power consumed value of each PoE port
PD Failure Check Status	Indicates the PD Failure Check status of each PoE port. Alive: The PD is pinged by system continuously Not Alive: The PD is not pinged by system Disable: The PD Failure Check is not activated

PoE System Status



Monitoring Configuration

Refresh Rate

Setting	Description	Factory Default
5 to 300	The period of time which the system refreshes the PoE System Status	5

System Power Status

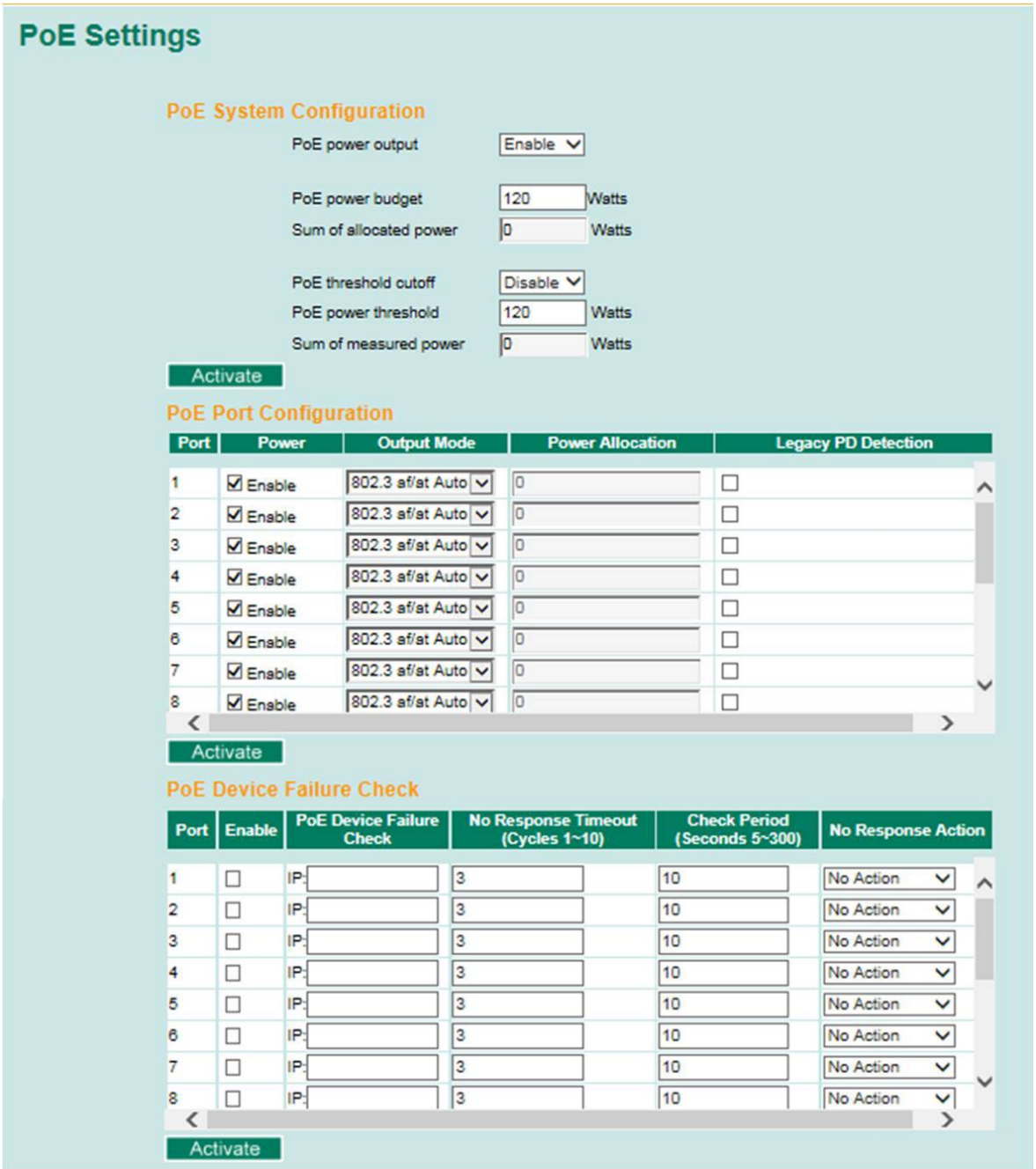
System power status allows users to view a graph which includes **Sum of measured power**, **Sum of allocated power**, and **Max of allocated power**. Sum of measured power (in pink color) indicates total measured power of PDs, Sum of allocated power (in blue color) indicates total allocated power, and Max of allocated power (in red color) indicates the threshold of total PoE power output. The graph displays these powers by showing **Current (mA)** versus **Sec. (second)**, and it is refreshed frequently by the Refresh Rate.

Type 3

PoE Setting

The setting are included to give the user control over the system's PoE power output, PoE power threshold, PoE port configuration, and PD failure check.

An explanation of each configuration item follows:



PoE System Configuration

PoE power output

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

PoE power budget

Setting	Description	Factory Default
120	It shows the total PoE power budget of the switch	120

Sum of allocated power

Setting	Description
Allocated power	This item shows the total allocated power of PDs

PoE threshold cutoff

Setting	Description	Factory Default
Enable	Cutoff the PD's power while it is over the threshold	Disable
Disable	No cutoff while the PD's power over the threshold	

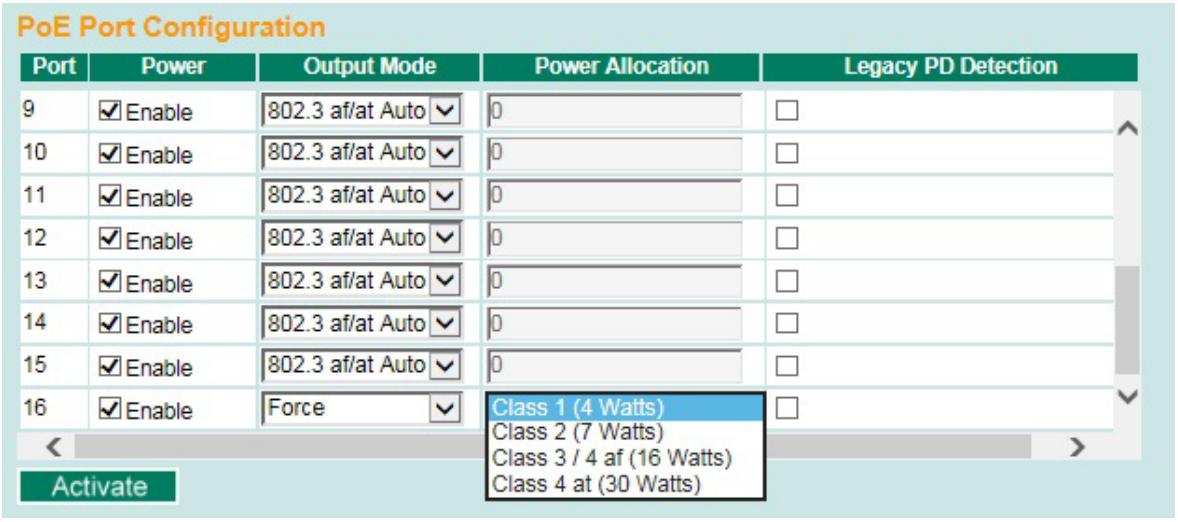
PoE power threshold

Setting	Description	Factory Default
30 to 240	Set the threshold of total PoE power output	240

Sum of measured power

Setting	Description
Measured power	This item shows the total measured power of PDs

PoE Port Configuration



Power

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

Output Mode

Setting	Description	Factory Default
802.3 af/at Auto	Power transmission on IEEE 802.3 af/at protocols. The acceptable PD resistance range is 17kΩ to 29kΩ.	802.3 af/at Auto
Force	Force mode allows users to output power to a non 802.3 af/at PD. The acceptable PD resistance range is over 2.4kΩ, and the range of power allocation can be set to Class 1 (4 W), Class 2 (7 W), Class 3 / 4af (16 W), or Class 4 (30 W).	

Power Allocation

Setting	Description	Factory Default
Class 1 to 4	In the Force output mode, the range of power allocation can be set from Class 1 (4 W), Class 2 (7 W), Class 3 / 4af (16 W), or Class 4 (30 W)	Class 1 (4 Watts)

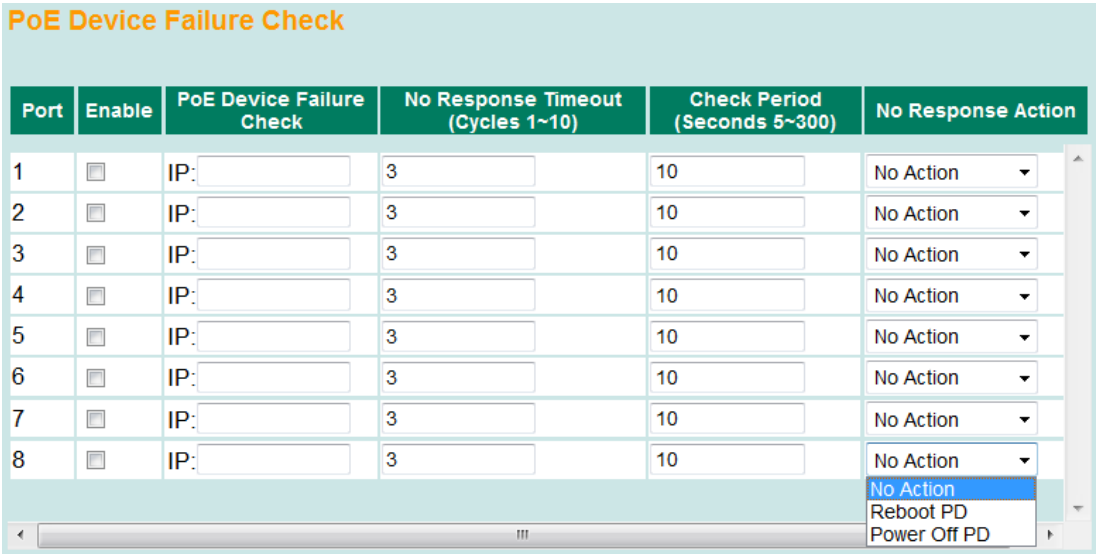
Legacy PD Detection

The PoE Ethernet Switch provides the **Legacy PD Detection** function. When the capacitance of PD is higher than 2.7μF, checking the **Legacy PD Detection** enables system to output power to PD. If you check the Legacy PD Detection, it will take longer detection time from 10 to 15 seconds before PoE power output.

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

PoE Device Failure Check

The PoE Ethernet Switch can monitor PD working status via its IP conditions. If the PD fails, the switch will not receive a PD response after the defined period, and the authentication process is restarted. This is an excellent function to ensure your network reliability and reduce management burden.



Enable

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

PoE Device IP Address

Setting	Description	Factory Default
Max. 15 Characters	Enter the IP for the PD	None

No Response Timeout

Setting	Description	Factory Default
1 to 10	Enter the cycles for IP checking	3

Check Period

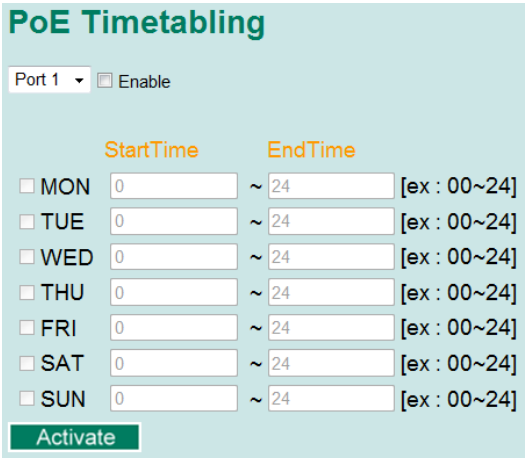
Setting	Description	Factory Default
5 to 300	Enter the time span for IP checking period	10

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 to let users set a flexible working schedule for each PoE port to economize the system's power burden.



Port

Setting	Description	Factory Default
Port	Enable a dedicated port	Port 1

Enable

Setting	Description	Factory Default
Checked	Enables the port for a defined time period	Disable
Unchecked	Disables the port for a defined time period	

Weekly Timetabling

Day

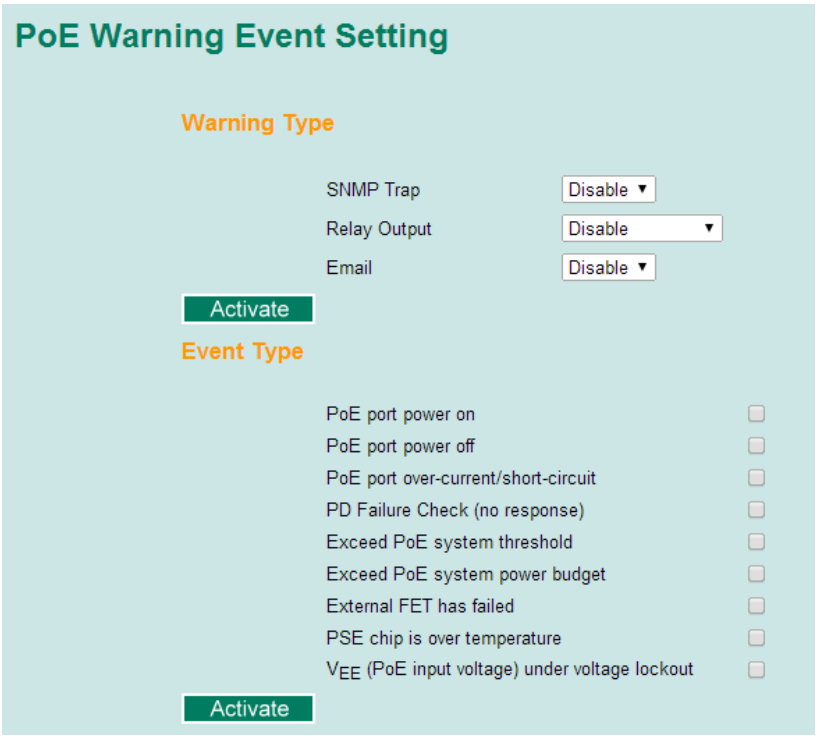
Setting	Description	Factory Default
Checked	Enables the port for a defined number of days	Disable
Unchecked	Disables the port for a defined number of days	

Start/End Time

Setting	Description	Factory Default
Time for working period	Allows users to enter the start and end time for the PD's working period	0 to 24

PoE Warning Event Setting

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, such as SNMP trap, email, and relay output. It also supports two digital inputs to integrate sensors into your system to automate alarm using email and relay output.



Warning Type

SNMP Trap

Setting	Description	Factory Default
Enable	Enables the SNMP trap function of PoE warning	Disable
Disable	Disables the SNMP trap function of PoE warning	

Relay Output

Setting	Description	Factory Default
Enable	Enables the relay output function of PoE warning*	Disable
Disable	Disables the relay output function of PoE warning	

*__Enable (relay 1)__ and __Enable (relay 2)__ can be selected if the switch supports multi-relay output.

Email

Setting	Description	Factory Default
Enable	Enables the email alarm function of PoE warning	Disable
Disable	Disables the email alarm function of PoE warning	

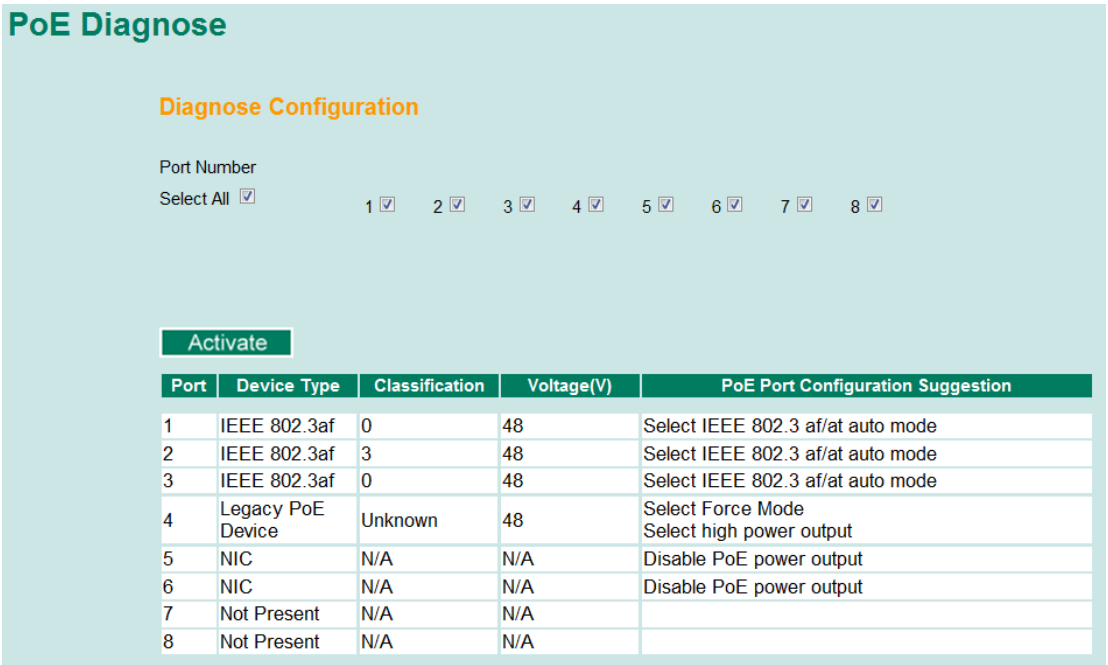
Event Type

Port Events	Description
PoE port power on	Power outputs to PD
PoE port power off	Cut off PoE power output
PoE port over-current/short-circuit	When the current of the port exceeds the limitation: 802.3 af – 350mA 802.3 at – 600mA High Power – 720mA Force – 600mA
PD Failure Check (no response)	When the switch cannot receive a PD response after the defined period
Exceed PoE system threshold	When sum of all PD power consumption exceeds the threshold of total PoE power output
Exceed PoE system power budget	When "sum of allocated power" exceeds the PoE power budget
External FET has failed	When the MOSFET of the port is out of order, please contact Moxa for technical service
PSE chip is over temperature	Please check the environmental temperature. If it is over 75oC, please operate the switch at an adequate temperature. If not, please contact Moxa for technical service.
V_{EE} (PoE input voltage) under voltage lockout	The voltage of the power supply drops down below 44VDC. Adjust the voltage between 46 and 57VDC to eliminate this issue.

NOTE

The Relay Output does not support three Event Types: **External FET has failed, PSE chip is over temperature**, and **V_{EE} (PoE input voltage) under voltage lockout**.

PoE Diagnose



PoE Diagnose helps users to figure out the PD conditions, and the system provides users configuration suggestions to select the best setting for the PDs.

Following steps help users to diagnose the PD conditions:

Step 1: Check the port numbers which will be diagnosed

Step 2: Click **Activate**

Step 3: The system shows the selected PD conditions

Diagnose Configuration

Port Number

Setting	Description	Factory Default
Checked	Enable the port to diagnose	Unchecked
Unchecked	Disable the port to diagnose	

Device Type

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

Classification

Item	Description
N/A	No classification on the port
0 to 4	Class from 0 to 4
Unknown	Unknown class to the port, normally higher than class 4

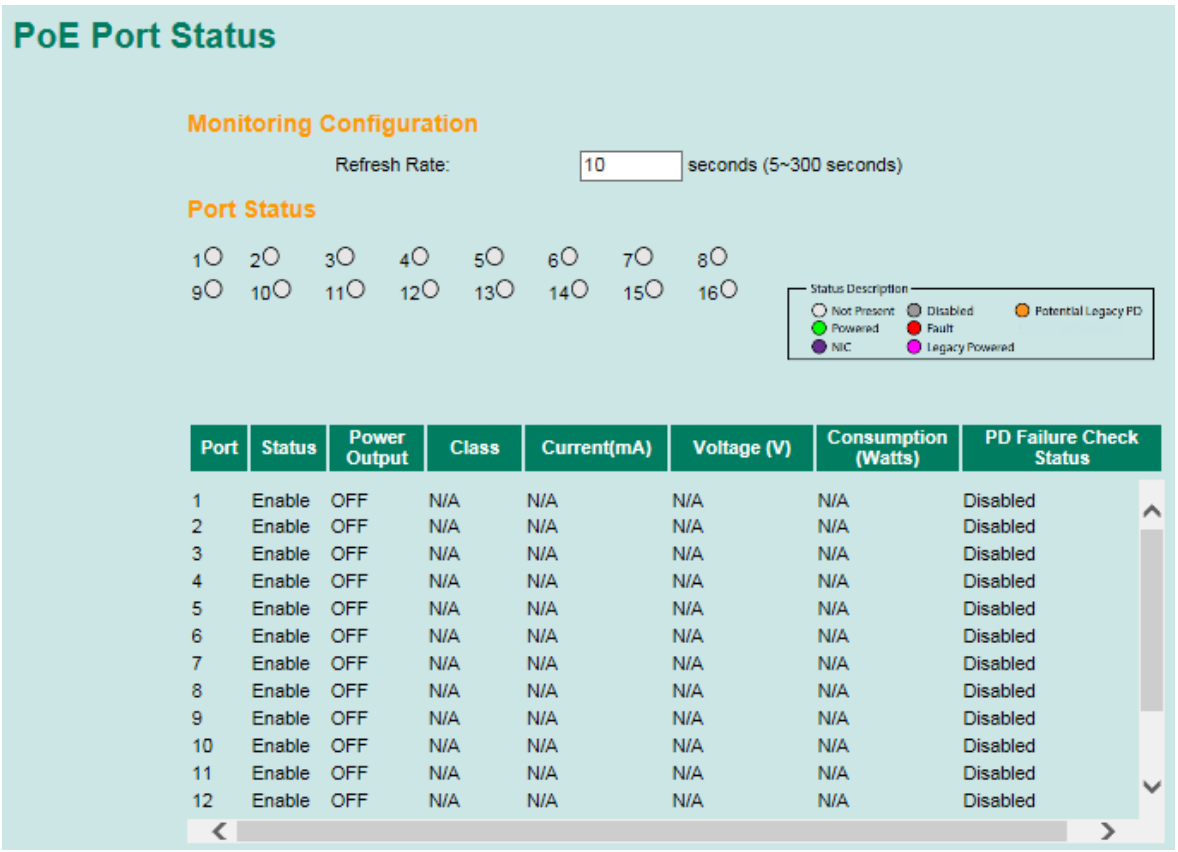
Voltage (V)

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 an 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 802.3 af/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 external power supply voltage > 46 VDC	When detecting the external supply voltage is below 46 V, the system suggests raising the voltage.
Enable PoE function for detection	The system suggests enabling the PoE function.

PoE Port Status



Monitoring Configuration

Refresh Rate

Setting	Description	Factory Default
5 to 300	The period of time which the system refreshes the PoE Port Status	5

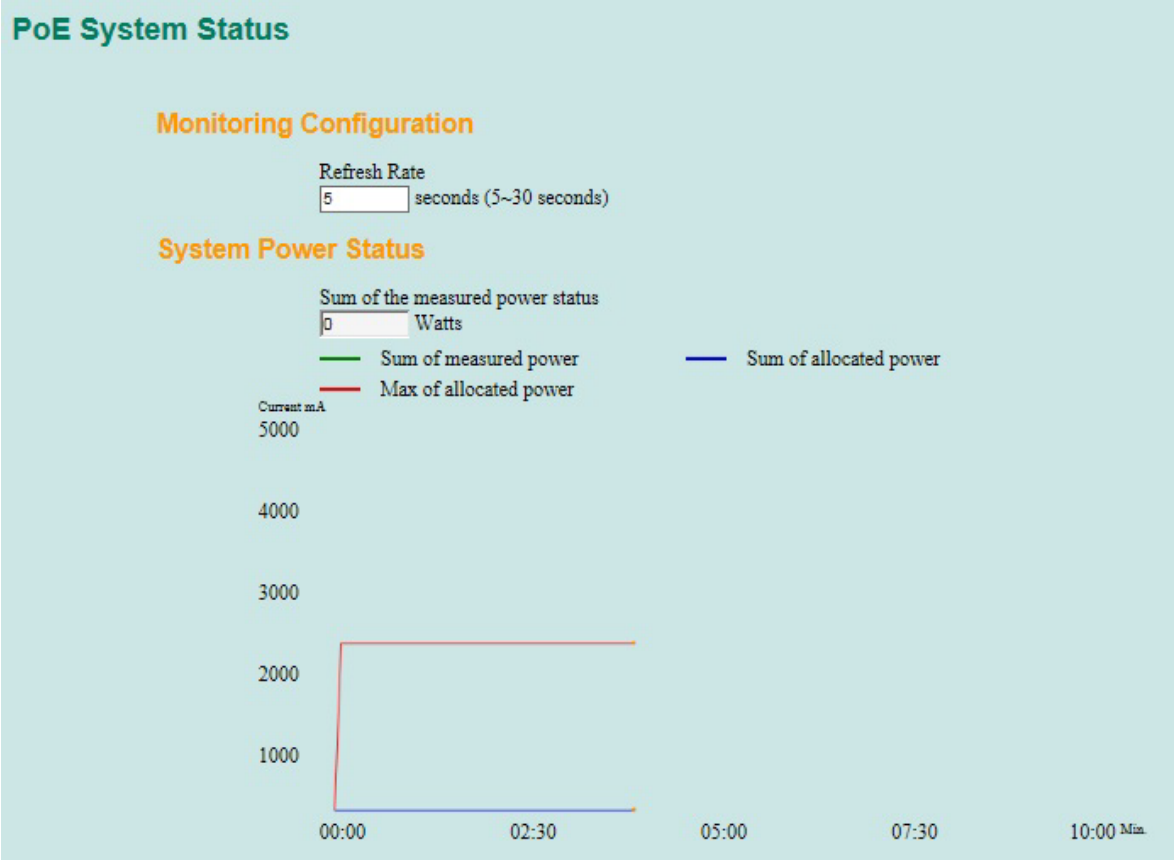
Status Description

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

Port Description

Item	Description
Status	Indicates if the PoE function is enable
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 value of each PoE port
Voltage (V)	Indicates the actual Voltage consumed value of each PoE port
Consumption (Watts)	Indicates the actual Power consumed value of each PoE port
PD Failure Check Status	Indicates the PD Failure Check status of each PoE port. Alive: The PD is pinged by system continuously Not Alive: The PD is not pinged by system Disable: The PD Failure Check is not activated

PoE System Status



Monitoring Configuration

Refresh Rate

Setting	Description	Factory Default
5 to 30	The period of time which the system refreshes the PoE System Status	5

System Power Status

System power status allows users to view a graph which includes **Sum of measured power**, **Sum of allocated power**, and **Max of allocated power**. Sum of measured power (in pink color) indicates total measured power of PDs, Sum of allocated power (in blue color) indicates total allocated power, and Max of allocated power (in red color) indicates the threshold of total PoE power output. The graph displays these powers by showing **Current (mA)** versus **Sec. (second)**, and it is refreshed frequently by the Refresh Rate.

Using Traffic Prioritization

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 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 table below 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 in the LAN environment, 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:

- 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.

TN-4500A Series

If the packet is untagged, it will be assigned a PCP value of zero. Tagged packets will be prioritized based on the original assigned 802.1p tag (for firmware versions prior to v3.10 build 21092813).

If the packet is untagged, it will be prioritized according to the port priority. Tagged packets will be prioritized based on the original assigned 802.1p tag (for firmware versions after v3.10 build 21092813).

TN-5508A, TN-5510A Series

Depending on whether the TOS/COS Inspect function is enabled or disabled, packets will behave differently. The Switch will prioritize packets according to the TOS, COS, and port priority settings.

If TOS Inspect is enabled, the packet will be prioritized according to the TOS field value. Refer to the TOS/DiffServ Mapping table for an overview of TOS values. For example, TOS value 0x00, 0x63 will map to low, normal priority queues respectively. These TOS values translate to PCP values 1, 3 respectively

If COS Inspect is enabled and the packet is tagged, the packet will be prioritized based on the original assigned 802.1p tag.

If COS Inspect is enabled but the packet is untagged, the packet will be prioritized according to the port priority.

If both TOS/COS Inspect are disabled, the packet will be prioritized according to the port priority.

TN- 5516A, TN-5518A Series

If the packet is untagged, it will be assigned a PCP value of zero. Tagged packets will be prioritized based on the original assigned 802.1p tag.

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 two 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.

Configuring Traffic Prioritization

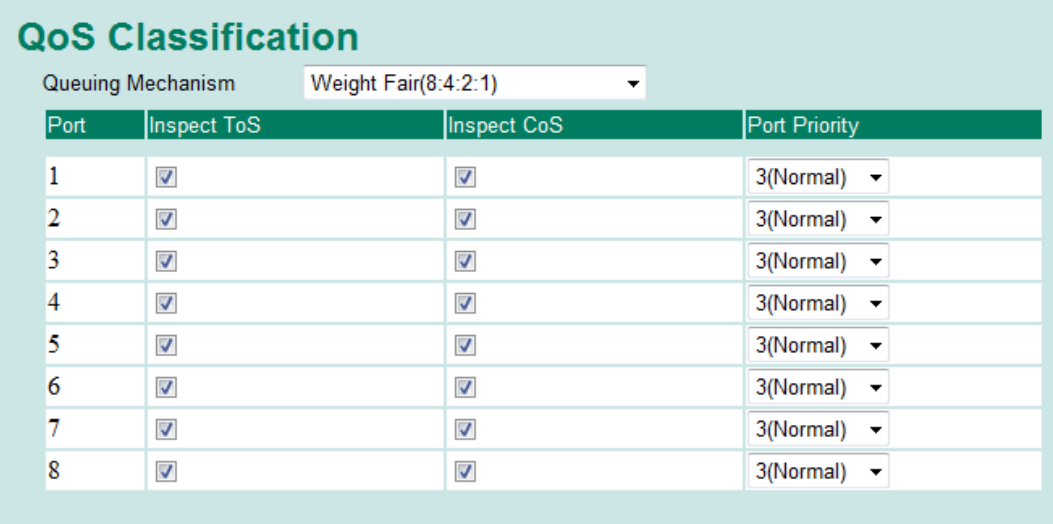
Quality of Service (QoS) provides a traffic prioritization capability to ensure that important data is delivered consistently and predictably. The Moxa switch can inspect IEEE 802.1p/1Q layer 2 CoS tags, and even layer 3 TOS information, to provide a consistent classification of the entire network. The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

QoS Classification

There are two QoS classification settings depending on the specific model of the switch.

Type	Models Supported
Type 1	TN-5508A Series, TN-5510A Series, TN-4516A Series, TN-4524A Series, TN-4528A Series
Type 2	TN-5516A Series, TN-5518A Series, TN-5800A Series

Type1



The Moxa switch supports inspection of layer 3 TOS and/or layer 2 CoS tag information to determine how to classify traffic packets.

Queuing Mechanism

Setting	Description	Factory Default
Weight Fair	The Moxa switch has 4 priority queues. In the weight fair scheme, an 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 queue is empty, and then the next lower priority queue's frames egress. This approach can cause the lower priorities to be starved of opportunity for transmitting any frames but ensures that all high priority frames will egress the switch as soon as possible.	

Inspect TOS

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

Inspect COS

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.	Enabled

Inspect Port Priority

Setting	Description	Factory Default
Port priority	The port priority has 4 priority queues. Low, normal, medium, high priority queue option is applied to each port.	3(Normal)

NOTE

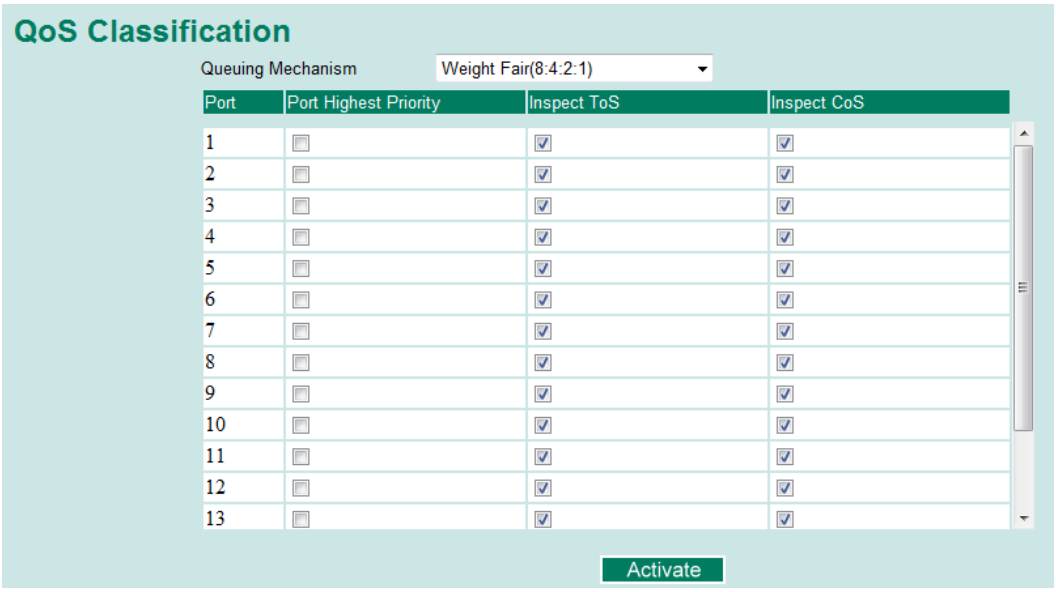
The priority of an ingress frame is determined in the following order:

1. Inspect TOS
2. Inspect CoS
3. Port 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, **Inspect TOS** and **Inspect CoS** 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.

Type 2



Queuing Mechanism

Setting	Description	Factory Default
Weight Fair	The Moxa switch has 4 priority queues. In the weight fair scheme, an 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 queue is empty, and then the next lower priority queue's frames egress. This approach can cause the lower priorities to be starved of opportunity for transmitting any frames but ensures that all high priority frames will egress the switch as soon as possible.	

Inspect Port Highest Priority

Setting	Description	Factory Default
Enable/Disable	Enables or disables the priority inspection of each port	Disabled

Inspect TOS

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

Inspect COS

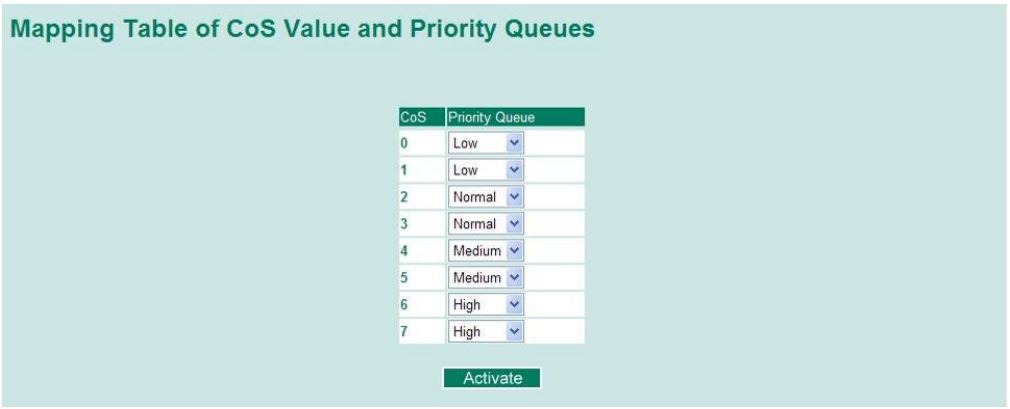
Setting	Description	Factory Default
Enable/Disable	Enables or disables the Moxa switch for inspecting 802.1p COS tags in the MAC frame to determine the priority of each frame.	Enabled

NOTE

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

1. Port Highest Priority
2. Inspect TOS
3. Inspect CoS

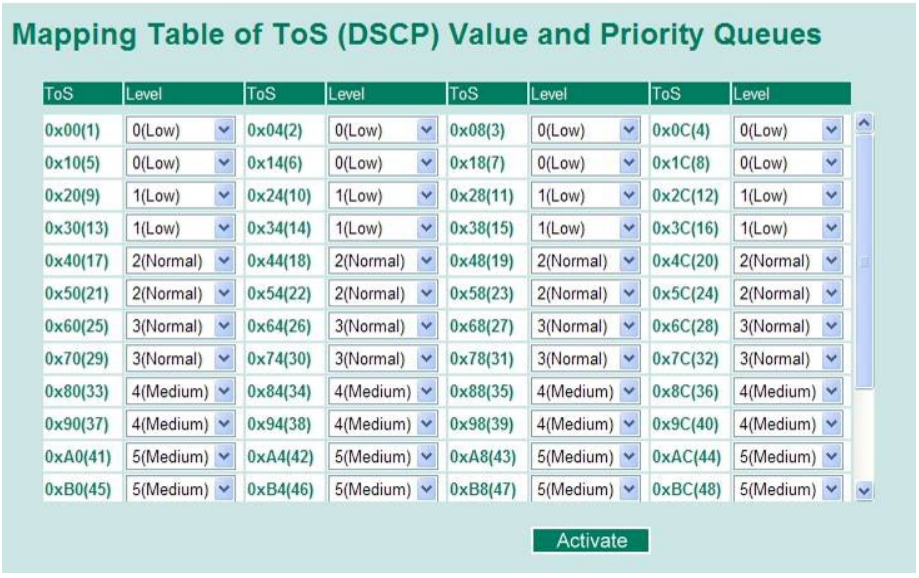
CoS Mapping



CoS Value and Priority Queues

Setting	Description	Factory Default
Low/Normal/ Medium/High	Maps different CoS values to 4 different egress queues.	0: Low 1: Low 2: Normal 3: Normal 4: Medium 5: Medium 6: High 7: High

TOS/DiffServ Mapping



ToS (DSCP) Value and Priority Queues

Setting	Description	Factory Default
Low/Normal/ Medium/High	Maps different TOS values to 4 different egress queues.	1 to 16: Low 17 to 32: Normal 33 to 48: Medium 49 to 64: High

Using Virtual LAN

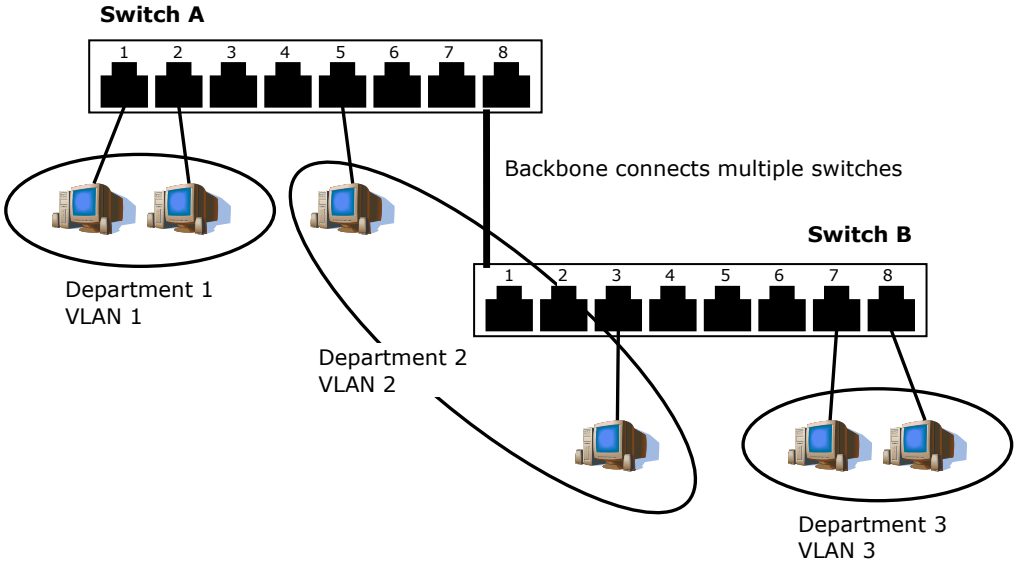
Setting up Virtual LANs (VLANs) on your Moxa switch increases the efficiency of your network by dividing the LAN into logical segments, as opposed to physical segments. In general, VLANs are easier to manage.

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 according 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 VLAN Marketing, for example, 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 VLAN Marketing. 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 VLAN Marketing needs to communicate with devices on VLAN Finance, 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.

Communication Between VLANs

If devices connected to a VLAN need to communicate to 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 and 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, tagged membership must be defined.

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

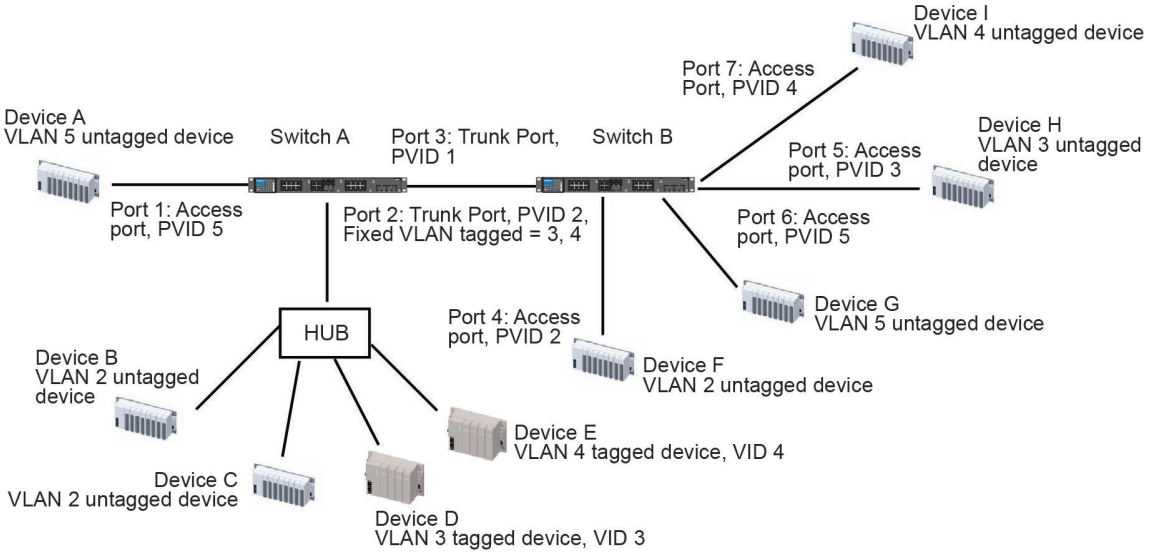
To carry multiple VLANs across a single physical link (backbone, trunk), each packet must be tagged with a VLAN identifier so that the switches can identify which packets belong in which VLAN. To communicate between VLANs, a router must be used.

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 port default 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 **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 **Trunk Port** with PVID 2 for untagged device and Fixed VLAN (Tagged) with 3 and 4 for tagged device. 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 **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 **Access Port** with PVID 2.
- Port 5 connects a single untagged device and assigns it to VLAN 3; it should be configured as **Access Port** with PVID 3.
- Port 6 connect a single untagged device and assigns it to VLAN 5; it should be configured as **Access Port** with PVID 5.
- Port 7 connects a single untagged device and assigns it to VLAN 4; it should be configured as **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 **Trunk Port 3** 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 Virtual LAN

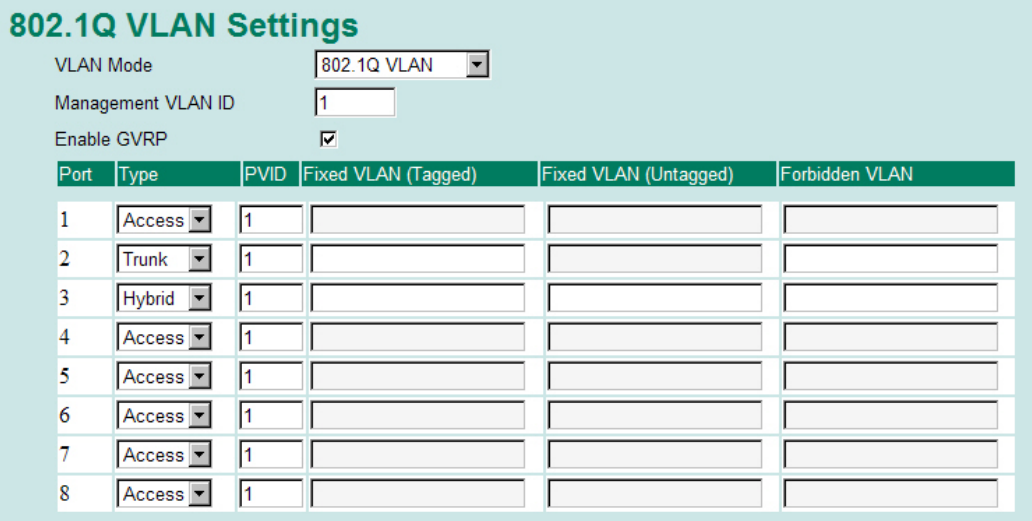
VLAN Settings

To configure 802.1Q VLAN and port-based VLANs on the Moxa switch, use the **VLAN Settings** page to configure the ports.

VLAN Mode

Setting	Description	Factory Default
802.1Q VLAN	Set VLAN mode to 802.1Q VLAN	802.1Q VLAN
Port-based VLAN	Set VLAN mode to Port-based VLAN	

802.1Q VLAN Settings



Management VLAN ID

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

Port Type

Setting	Description	Factory Default
Access	Port type is used to connect single devices without tags.	Access
Trunk	Select Trunk port type to connect another 802.1Q VLAN aware switch	
Hybrid	Select Hybrid port to connect another Access 802.1Q VLAN aware switch or another LAN that combines tagged and/or untagged devices and/or other switches/hubs.	

ATTENTION

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

Port PVID

Setting	Description	Factory Default
VID ranges from 1 to 4094	Sets the default VLAN ID for untagged devices that connect to the port.	1

Fixed VLAN List (Tagged)

Setting	Description	Factory Default
VID ranges from 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

Fixed VLAN List (Untagged)

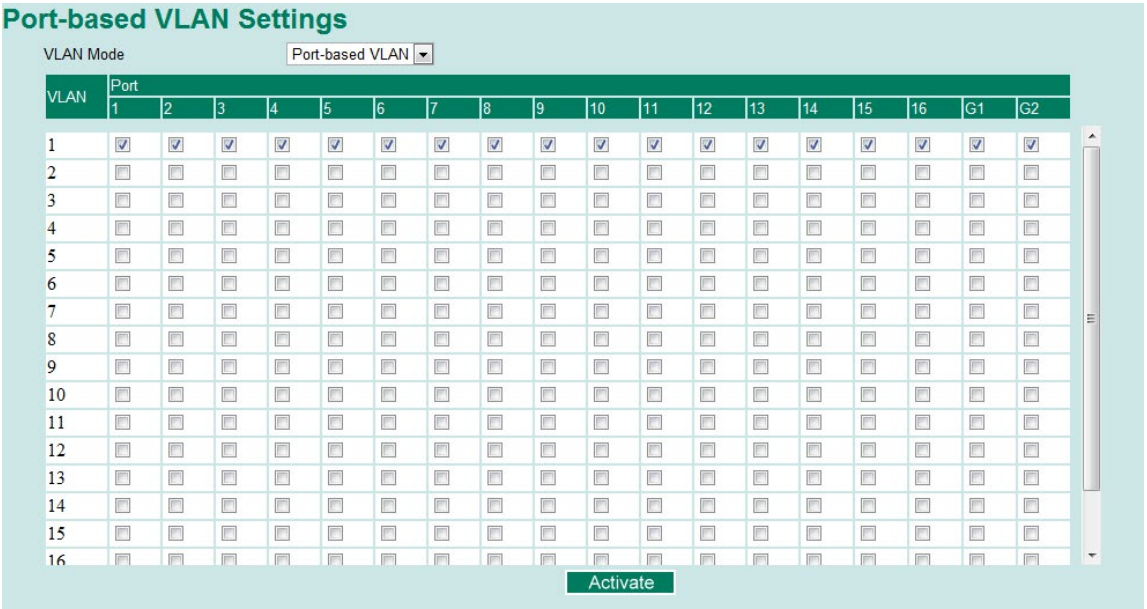
Setting	Description	Factory Default
VID range from 1 to 4094	This field will be active only when selecting the Hybrid port type. Set the other VLAN ID for tagged devices that connect to the port and tags that need to be removed in egress packets. Use commas to separate different VIDs.	None

Forbidden VLAN List

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

Port-Based VLAN Settings

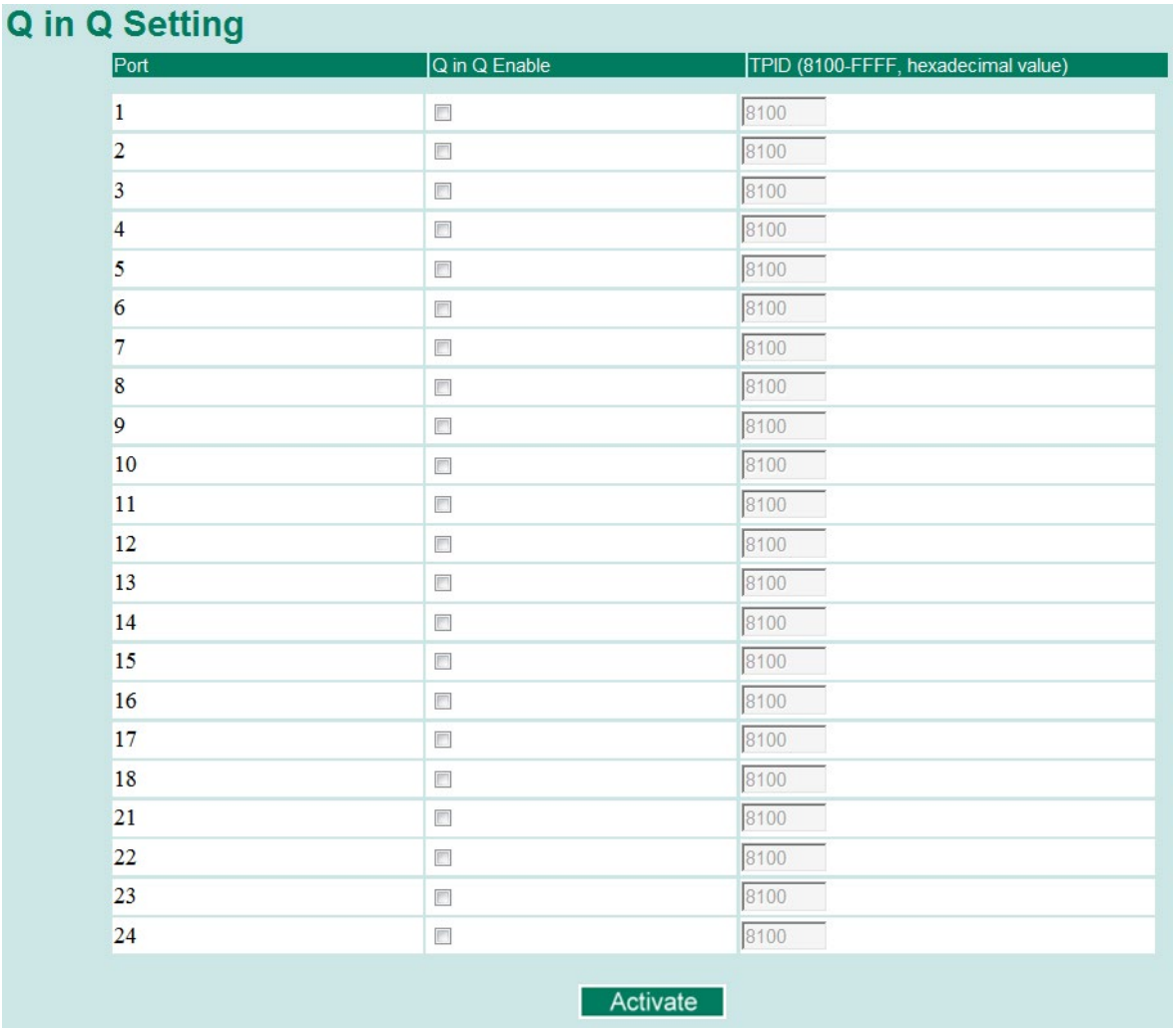
Check each specific port to assign its VLAN ID in the table. The maximum VLAN ID is the same as your number of switch ports.



Q in Q Setting

NOTE

Moxa layer 3 switches provide the IEEE 802.1ad QinQ function. This function allows users to tag double VLAN headers into one single Ethernet frame.



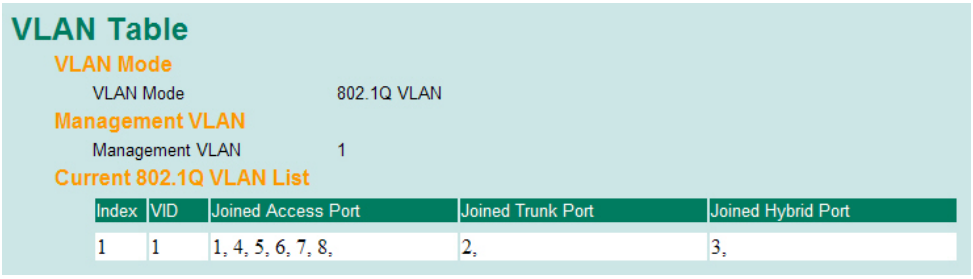
Q in Q Enable

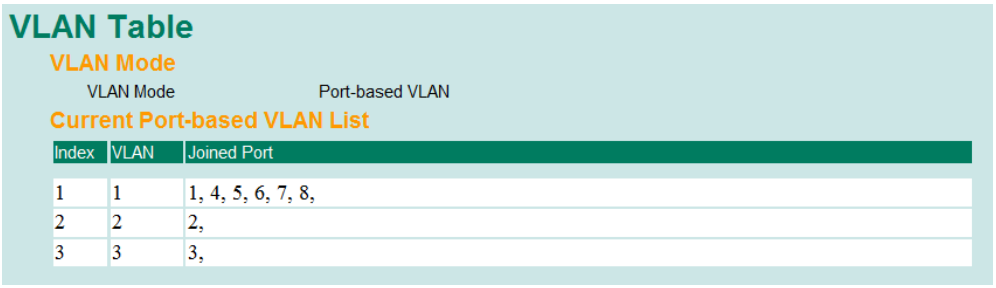
Setting	Description	Factory Default
Enable/Disable	Enable VLAN QinQ function	Disable

TPID

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

VLAN Table





Use the **802.1Q VLAN table** to review the VLAN groups that were created, **Joined Access Ports**, **Trunk Ports**, and **Hybrid Ports**, and use the **Port-based VLAN table** to review the VLAN group and **Joined Ports**.

NOTE

Most Moxa managed switches have a maximum of 64 VLAN settings.

Using Multicast Filtering

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:

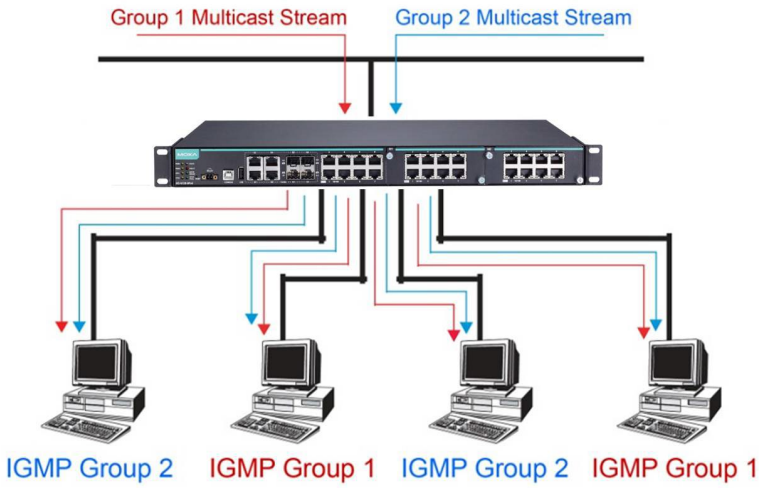
- It uses the most efficient, sensible method to deliver the same information to many receivers with only one transmission.
- It reduces the load on the source (for example, a server) since it will not need to produce several copies of the same data.
- It makes efficient use of network bandwidth and 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 video-conferencing, 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

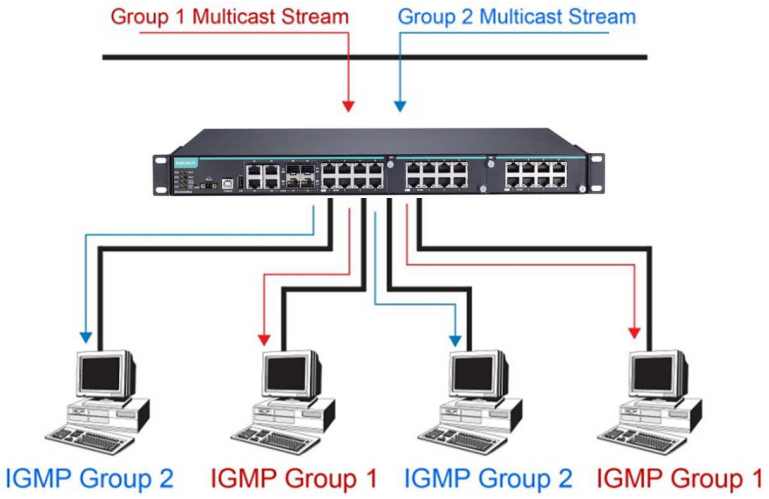
Multicast filtering ensures that only end-stations that have joined certain groups receive multicast traffic. With multicast filtering, network devices only forward multicast traffic to the ports that are connected to registered end-stations. The following two figures illustrate how a network behaves 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

The Moxa switch has three ways to achieve multicast filtering: 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 proceeding query election. 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	a. Periodic query	RFC-1112
V2	Compatible with V1 and adds: a. Group-specific query b. Leave group messages c. Resends specific queries to verify leave message was the last one in the group d. Querier election	RFC-2236
V3	Compatible with V1, V2 and adds: a. 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.

Configuring IGMP Snooping

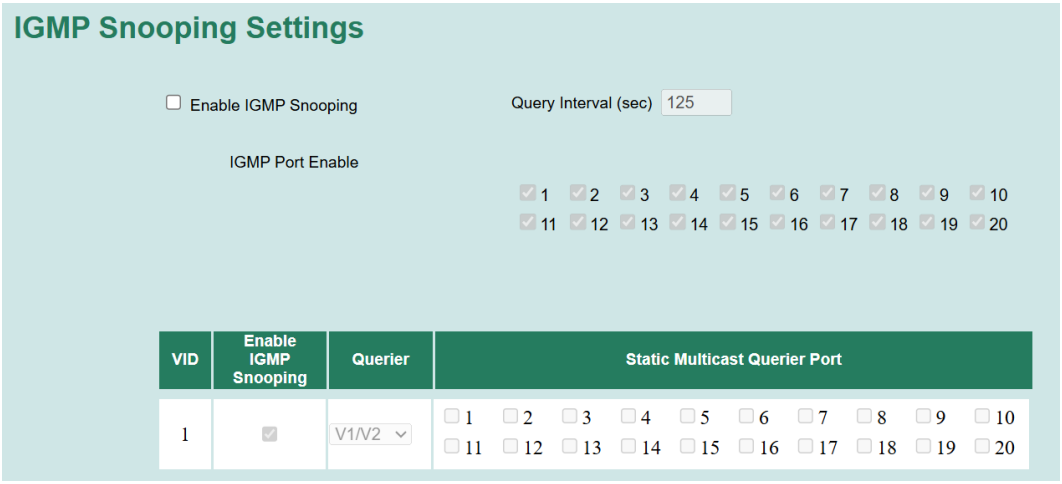
IGMP Snooping limits multicast traffic to destinations that require the traffic, reducing LAN traffic load. For security purposes, it is recommended to limit or disable any ports that could potentially be exploited to intercept and sniff sensitive or critical data streams.

IGMP Snooping can be enabled globally, or on individual ports.

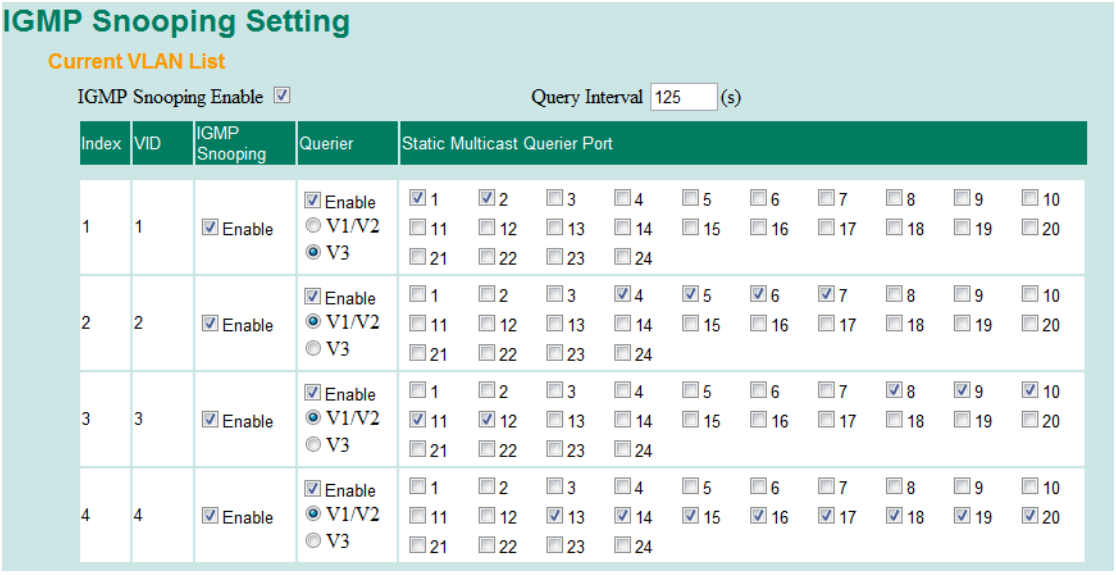
Note that all incoming IGMP control packets will be filtered out on ports that have port-based IGMP disabled. These control packets include:

- IGMP Membership Query
- IGMPv1 Membership Report
- IGMPv2 Membership Report
- IGMPv2 Leave Group
- IGMPv3 Membership Report
- Other protocol control packets with IP protocol number 2

Layer 2 switch setting page



Layer 3 switch setting page



Enable IGMP Snooping

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

NOTE

You should enable IGMP Snooping if the network also uses non-Moxa 3rd party switches.

Query Interval

Setting	Description	Factory Default
20 to 600	Sets the query interval (in seconds) of the Querier function globally.	125 seconds

IGMP Port Enable

Setting	Description	Factory Default
Enable/Disable	Enable or disable IGMP Snooping for the respective port.	Enabled

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
Enable/Disable	Enables or disables the Moxa switch's querier function.	Enabled (if IGMP Snooping is enabled globally)
V1/V2 and V3 checkbox	V1/V2: Enables switch to send IGMP snooping version 1 and 2 queries V3: Enables switch to send IGMP snooping version 3 queries	V1/V2

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

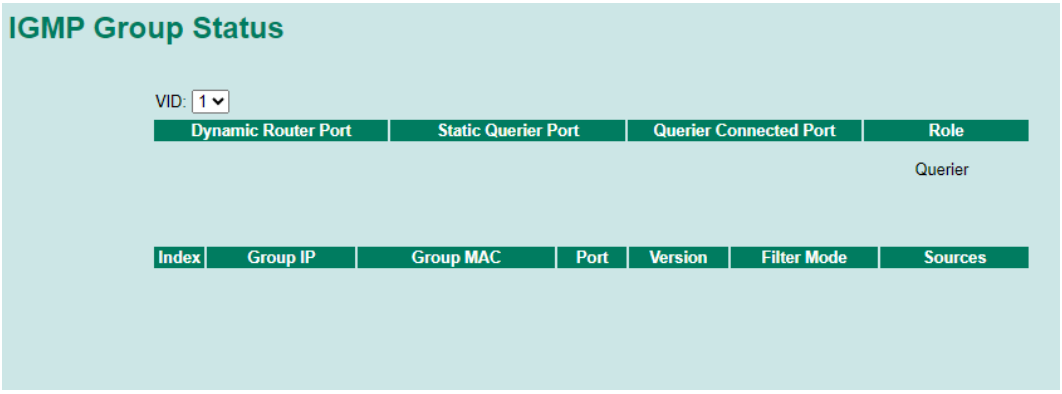
If a router or layer 3 switch is connected to the network, it will act as the Querier, and consequently this Querier option will be disabled on all Moxa layer 2 switches.

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

IGMP Table

The Moxa switch displays the current active IGMP groups that were detected. View IGMP group setting per VLAN ID on this page.

Layer 2 switch page



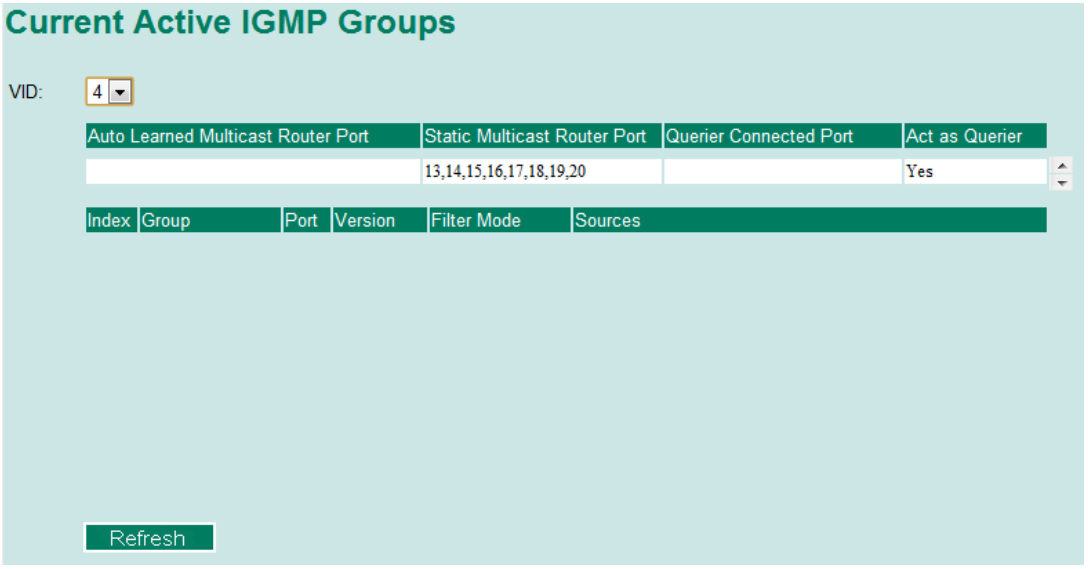
NOTE

Starting from firmware v3.12, static multicast and IGMP now share a common MAC table to give users more flexibility and a higher capacity for their applications.

The TN-4500A Series has a total of 512 MAC entries shared between static multicast and IGMP.

The TN-5500A Series has a total of 256 MAC entries shared between static multicast and IGMP.

Layer 3 switch page

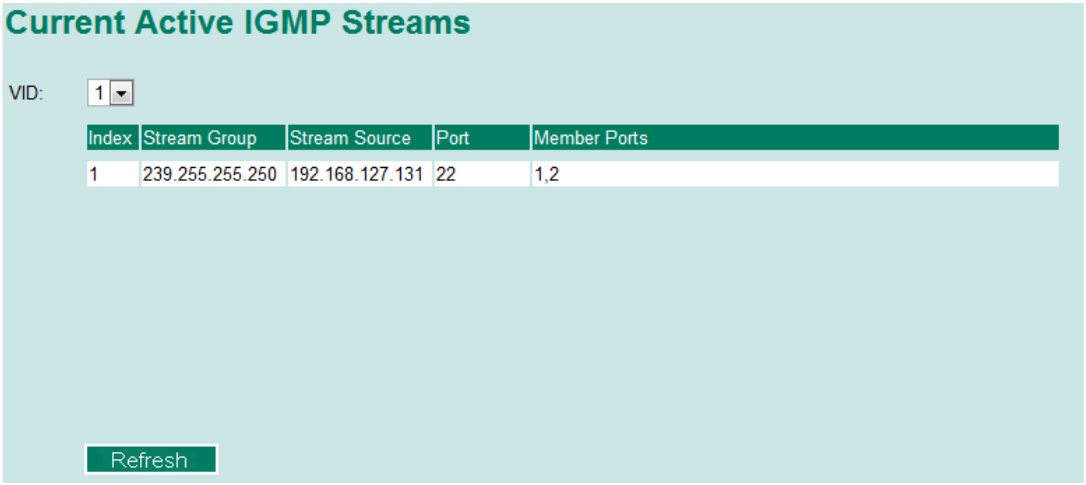


The information shown in the table includes:

- Auto-learned Multicast Router Port: This indicates that a multicast router connects to/sends packets from these port(s)
- Static Multicast Router Port: Displays the static multicast querier port(s)
- Querier Connected Port: Displays the port which is connected to the querier.
- Act as a Querier: Displays whether or not this VLAN is a querier (winner of a election).

Current Active IGMP Streams

This page displays the multicast stream forwarding status. It allows you to view the status per VLAN ID.



Stream Group: Multicast group IP address

Stream Source: Multicast source IP address

Port: Which port receives the multicast stream

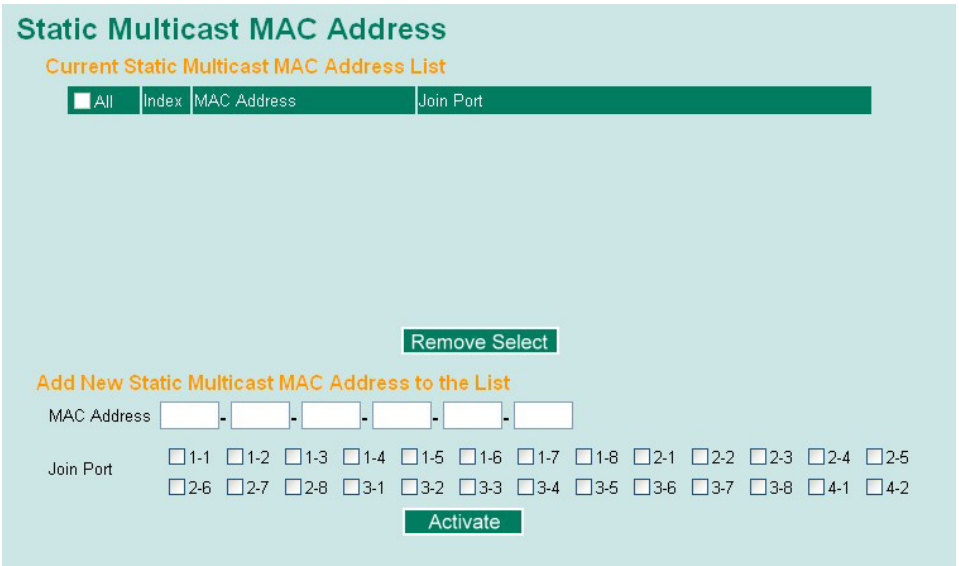
Member ports: Ports the multicast stream is forwarded to.

NOTE

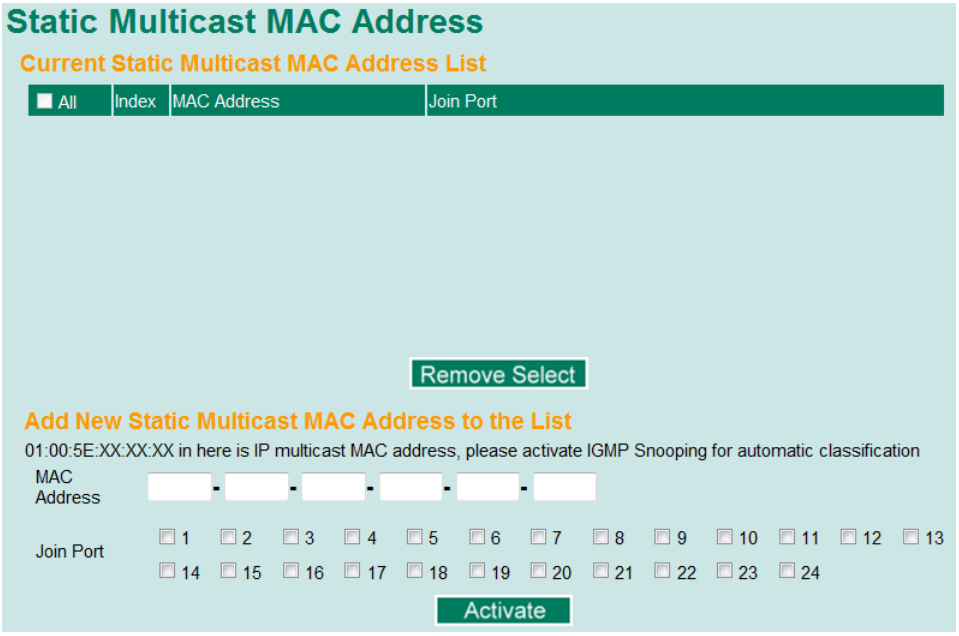
The IGMP stream table is supported only in Layer 3 switches.

Static Multicast MAC Addresses

Layer 2 switch page



Layer 3 switch page



NOTE

01:00:5E:XX:XX:XX on this page is the IP multicast MAC address. Please activate IGMP Snooping for automatic classification.

NOTE

Starting from firmware v3.12, static multicast and IGMP now share a common MAC table to give users more flexibility and a higher capacity for their applications.

The TN-4500A Series has a total of 512 MAC entries shared between static multicast and IGMP.

The TN-5500A Series has a total of 256 MAC entries shared between static multicast and IGMP.

Add New Static Multicast Address to the List

Setting	Description	Factory Default
MAC Address	Input the multicast MAC address of this host.	None

MAC Address

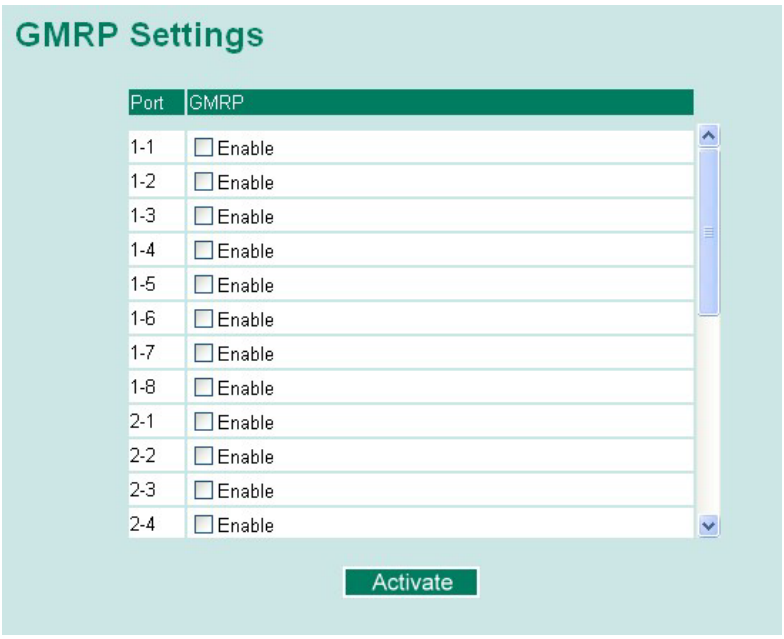
Setting	Description	Factory Default
Integer	Input the number of the VLAN that the host with this MAC address belongs to.	None

Join Port

Setting	Description	Factory Default
Select/Deselect	Checkmark the appropriate check boxes to select the join ports for this multicast group.	None

Configuring 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.

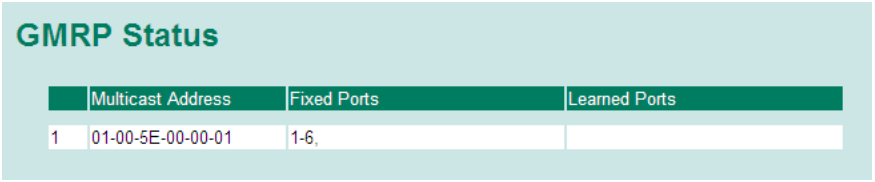


GMRP enable

Setting	Description	Factory Default
Enable/Disable	Enables or disables the GMRP function for the port listed in the Port column	Disable

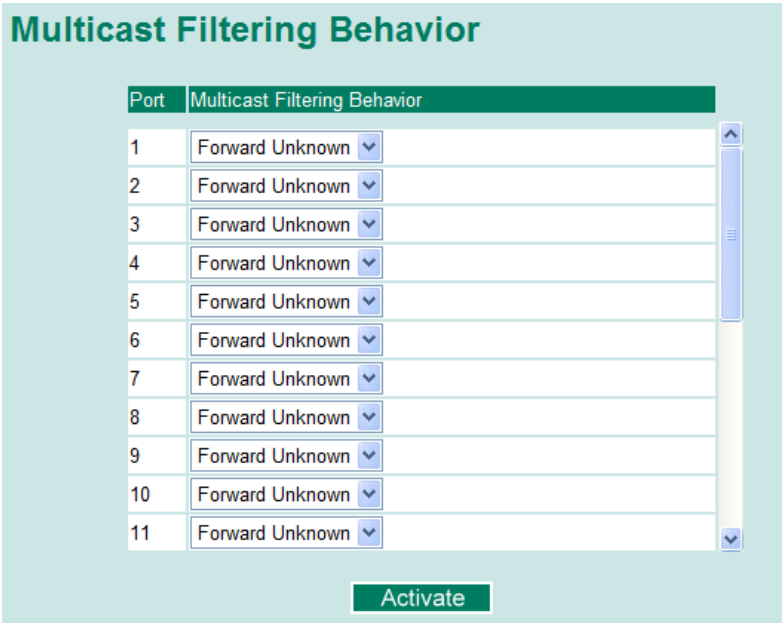
GMRP Table

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



Setting	Description
Fixed Ports	This multicast address is defined by static multicast.
Learned Ports	This multicast address is learned by GMRP.

Multicast Filtering Behavior



Setting	Description	Factory Default
Multicast Filtering Behavior	Define the multicast filtering behavior by three options: Forward All: flood all multicast packets to the VLAN of the network. Forward Unknown: flood unknown multicast packets to the VLAN while known multicast packets are sent to the indicated groups. Filter Unknown: drop unknown multicast packets and only send known multicast packets to indicated groups.	Forward Unknown

Using Bandwidth Management

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 prevents 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.

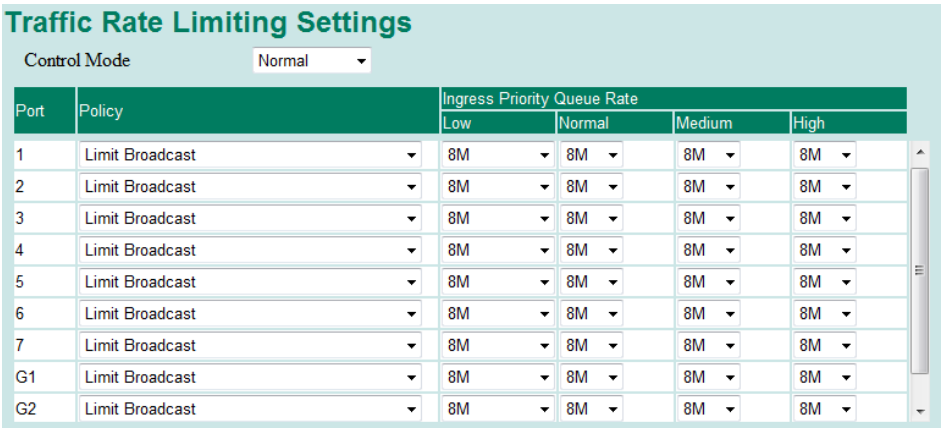
Configuring Bandwidth Management

Please note that two types of bandwidth management settings are available, depending on the specific model of switch.

Type	Models Supported
Type 1	TN-5508A Series, TN-5510A Series
Type 2	TN-5516A Series, TN-5518A Series, TN-5800A Series, TN-4516A Series, TN-4524A Series, TN-4528A Series, TN-5524 Series

Type 1

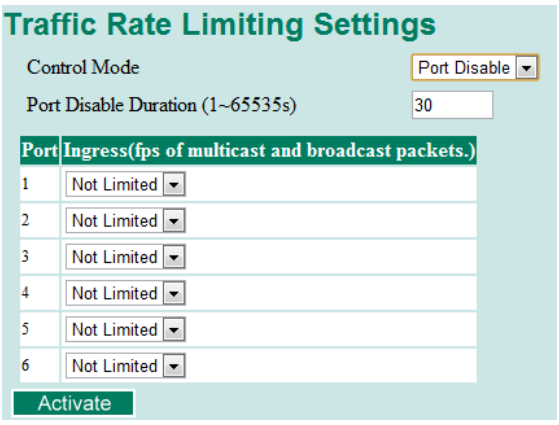
Traffic Rate Limiting Settings



Control Mode	Description	Factory Default
Normal	Set the max. ingress rate limit for different packet types	Normal
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.	

Ingress Rate Limit - Normal

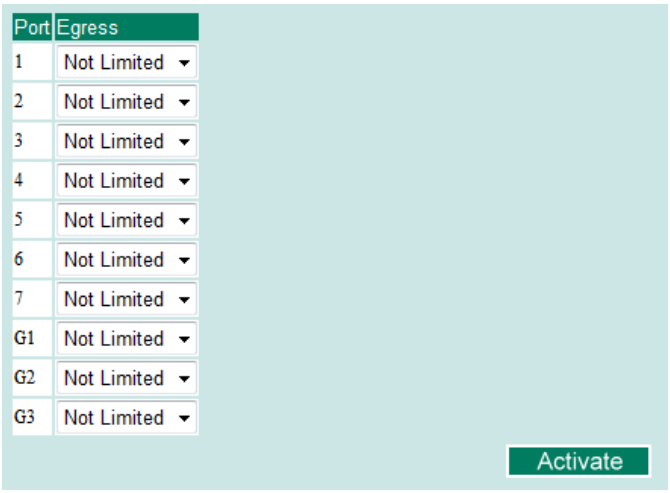
Policy	Description	Factory Default
Limit All	Select the ingress rate limit for different packet types from the following options: Not Limited, 128K, 256K, 512K, 1M, 2M, 4M, 8M	Limit Broadcast 8M
Limit Broadcast, Multicast, Flooded Unicast		
Limit Broadcast, Multicast		
Limit Broadcast		



Ingress Rate Limit – Port Disable

Setting	Description	Factory Default
Port disable duration (1~65535 seconds)	When the ingress multicast and broadcast packets exceed the ingress rate limit, the port will be disabled for this period of time. During this time, all packets from this port will be discarded.	30 second
Ingress (fps)	Select the ingress rate (fps) limit for all packets from the following options: Not Limited, 4464, 7441, 14881, 22322, 37203, 52084, 74405	Not Limited

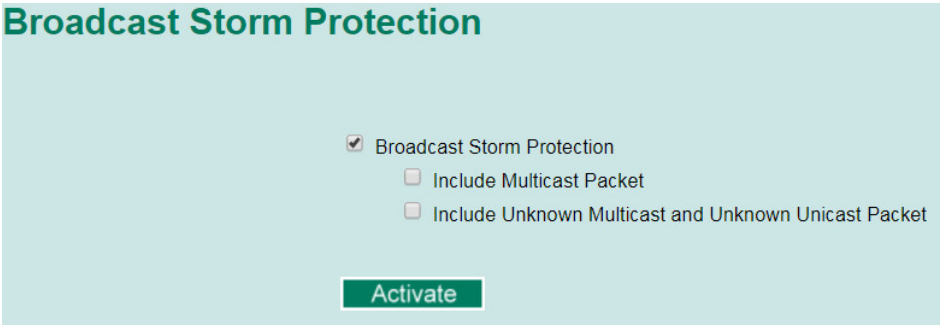
Egress Rate Limit



Setting	Description	Factory Default
Egress rate	Select the ingress rate limit (% of max. throughput) for all packets from the following options: Not Limited, 3%, 5%, 10%, 15%, 25%, 35%, 50%, 65%, 85%	Not Limited

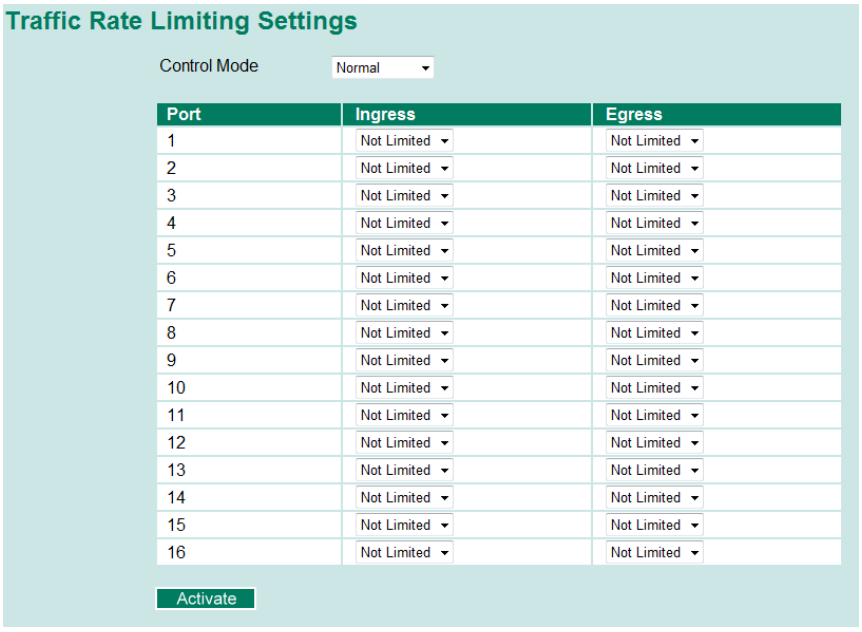
Type 2

Broadcast Storm Protection



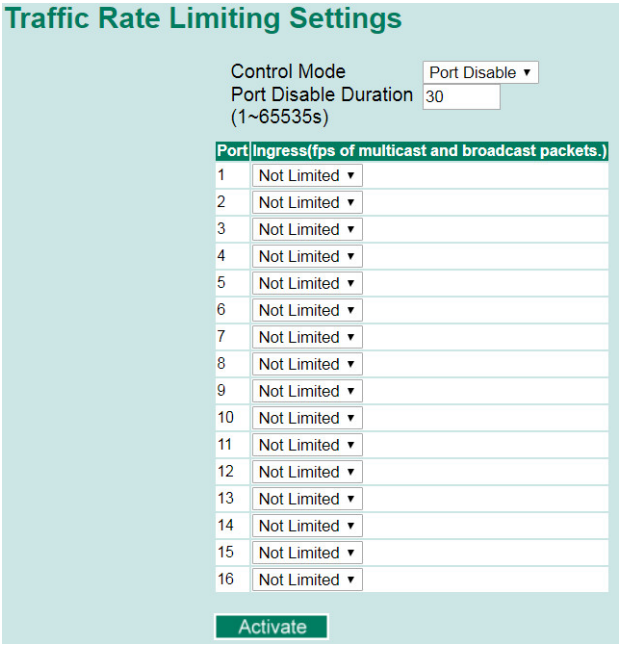
Setting	Description	Factory Default
Enable/Disable	This enables or disables Broadcast Storm Protection for unknown broadcast packet globally	Enable
	This enables or disables Broadcast Storm Protection for unknown multicast packets and unicast packets globally	Disable

Traffic Rate Limiting Settings



Ingress and Egress Rate Limit - Normal

Setting	Description	Factory Default
Ingress rate	Select the ingress/egress rate limit (% of max. throughput) for all packets from the following options: Not Limited, 3%, 5%, 10%, 15%, 25%, 35%, 50%, 65%, 85%	Not Limited
Egress rate		



Ingress Rate Limit – Port Disable

Setting	Description	Factory Default
Period (1~65535 seconds)	When the ingress packets exceed the ingress rate limit, the port will be disabled for a certain period.	30 seconds
Ingress (frame per second)	Select the ingress rate (fps) limit for all packets from the following options: Not Limited, 4464, 7441, 14881, 22322, 37203, 52084, 74405	Not Limited

Unicast Filter Behavior

> **NOTE**
>
> These functions are supported in the TN-4500A series switches.

When a switch receives an unknown unicast packet, it will flood it to all ports in the LAN. The **Unicast Filter Behavior** function provides a mechanism to prevent switch flooding of these unknown unicast packets. Select this check box to activate this filter behavior.

Setting	Description	Factory Default
Enable Filter unknown Unicast	Enable this function to prevent unknown unicast packets from flooding to all ports in the VLAN	Disable

Using Auto Warning

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 and relay output. It also supports two digital inputs to integrate sensors into your system to automate alarms by email and relay output.

Configuring Email Warning

The Auto Email Warning function uses e-mail to alert the user when certain user-configured events take place. Three basic steps are required to set up the Auto Warning function:

Configure Email Event Types

Select the desired **Event types** from the Console or Web Browser Event type page (a description of each event type is given later in the *Email Alarm Events setting* subsection).

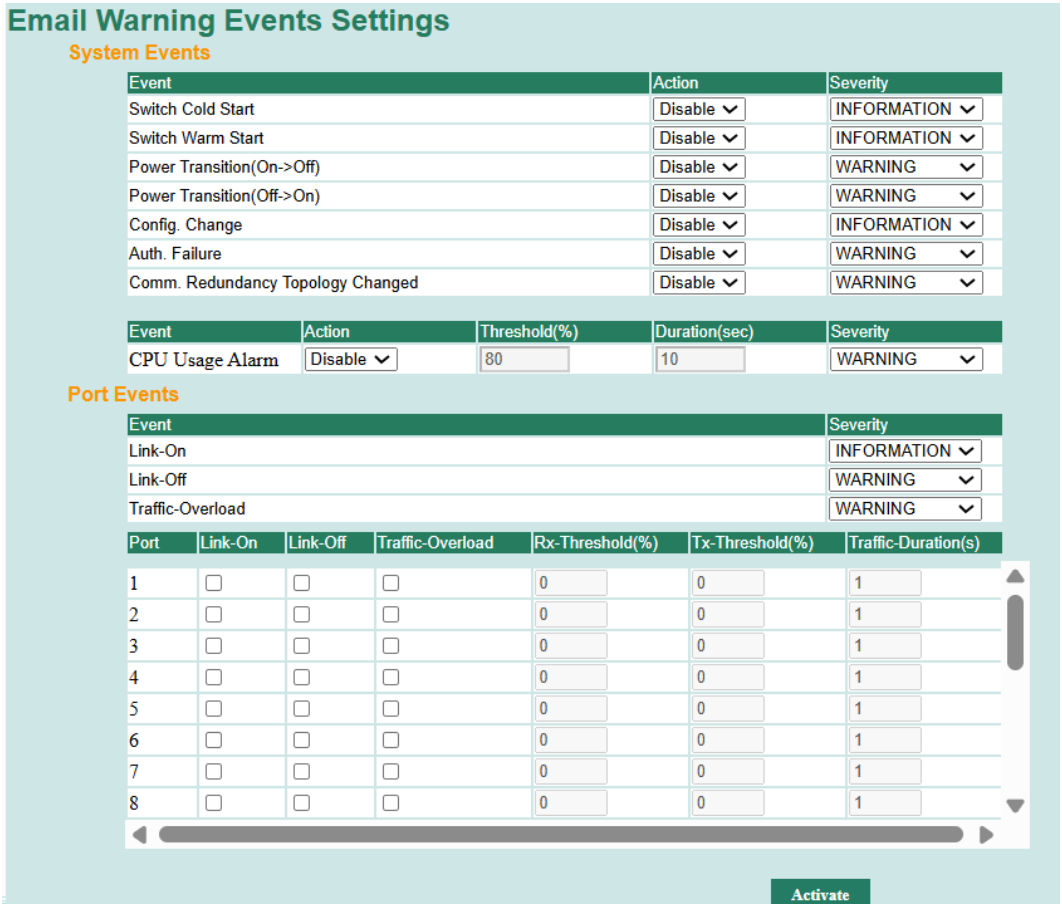
Configure Email Settings

To configure a Moxa switch's email setup from the serial, Telnet, or web console, enter your Mail Server IP/Name (IP address or name), Account Name, Account Password, Retype New Password, and the email address to which warning messages will be sent.

Activate your settings and if necessary, test the email

After configuring and activating your Moxa switch's Event Types and Email Setup, you can use the **Test Email** function to see if your e-mail addresses and mail server address have been properly configured.

Configuring Event Types



Event Types can be divided into two basic groups: **System Events** and **Port Events**. System Events are related to the overall function of the switch, whereas Port Events are related to the activity of a specific port.

System Events	Warning e-mail is sent when...
Switch Cold Start	Power is cut off and then reconnected.
Switch Warm Start	Moxa switch is rebooted, such as when network parameters are changed (IP address, subnet mask, etc.).
Power Transition (On→Off)	Moxa switch is powered down.
Power Transition (Off→On)	Moxa switch is powered up.
Configuration Change Activated	Any configuration item has been changed.
Authentication Failure	An incorrect password was entered.
Comm. Redundancy Topology Changed	If any Spanning Tree Protocol switches have changed their position (applies only to the root of the tree). If the Master of the Turbo Ring has changed or the backup path is activated.
CPU Usage Alarm	If enabled, you can specify the CPU usage threshold (in %), duration (in sec), and severity of this event log. When the CPU usage exceeds the threshold for the specified duration, the switch will send out a warning email.

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).
RX-Threshold (%)	If the Traffic-Overload option is enabled for the port, specify the RX threshold (in %).

Port Events	Warning e-mail is sent when…
TX-Threshold (%)	If the Traffic-Overload option is enabled for the port, specify the TX threshold (in %).
Traffic-Duration (sec.)	A Traffic-Overload warning is sent if the Traffic-Threshold is exceeded for the specified duration (in seconds).

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.

NOTE

To prevent excessive log recording, once a traffic overload event is triggered, the system will wait for 60 seconds before resuming to check the port's traffic load.

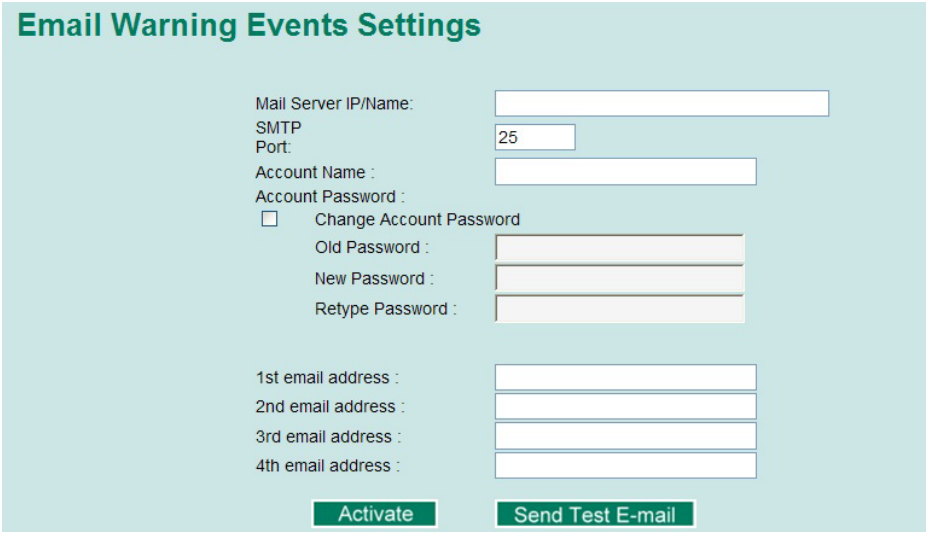
NOTE

The sender of warning e-mail messages will have the following format:

Managed-Redundant-Switch-00000@Switch_Location

Managed-Redundant-Switch-00000 is the default Switch Name, *00000* is the Moxa switch's serial number, and *Switch Location* is the default Server Location. Refer to the **System Identification** section for information on how to modify the switch name and location.

Configuring Email Settings



Mail Server IP/Name

Setting	Description	Factory Default
IP address	The IP Address of your email server.	None

SMTP Port

Setting	Description	Factory Default
SMTP port	Display the SMTP port number	25

Account Name

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

Password Setting

Setting	Description	Factory Default
Disable/Enable to change password	To reset the password from the Web Browser interface, click the Change password check-box, type the Old password, type the New password, retype the New password, and then click Activate (Max. of 45 characters).	Disable
Old password	Type the current password when changing the password	None
New password	Type new password when enabled to change password; Max. 45 characters.	None
Retype password	If you type a new password in the Password field, you will be required to retype the password in the Retype new password field before updating the new 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

Send Test Email

After you complete the email settings, you should first click **Activate** to activate those settings, and then press the **Send Test Email** 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.

Configuring Relay Warning

The Auto Relay Warning function uses relay output to alert the user when certain user-configured events take place. There are two basic steps required to set up the Relay Warning function:

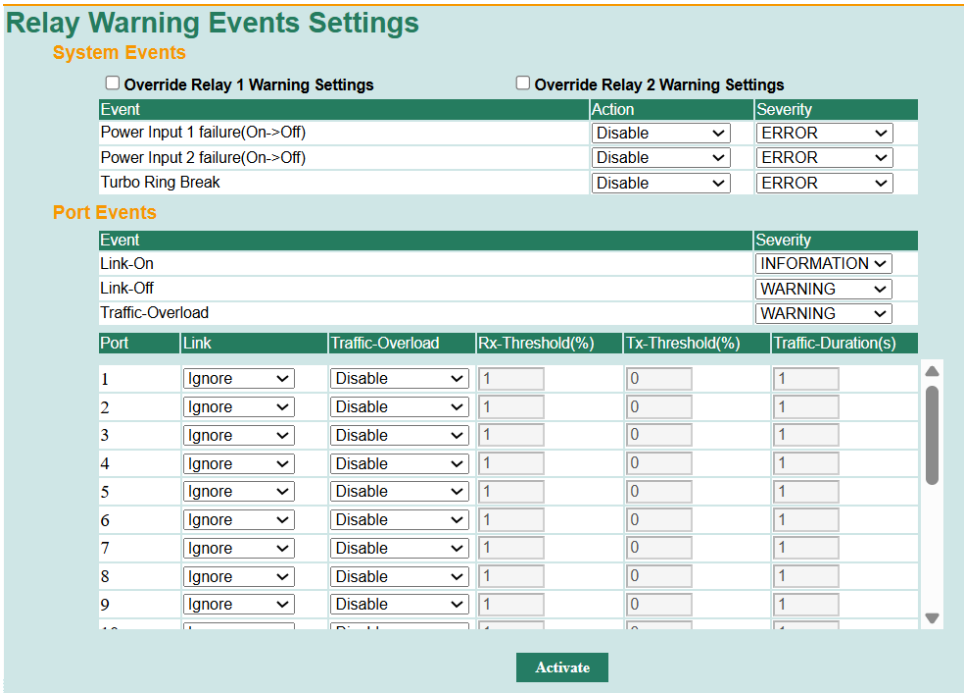
Configure Relay Event Types

Select the desired **Event types** from the Console or Web Browser Event type page (a description of each event type is given later in the *Relay Alarm Events setting* subsection).

Activate your settings

After completing the configuration procedure, you will need to activate your Moxa switch's Relay Event Types.

Configuring Event Types



Event Types can be divided into two basic groups: **System Events** and **Port Events**. System Events are related to the overall function of the switch, whereas Port Events are related to the activity of a specific port.

The Moxa switch supports two relay outputs. You can configure which relay output is related to which events, which helps administrators identify the importance of the different events.

System Events	Warning Relay output is triggered when…
Power Transition (On -> Off)	Moxa switch is powered down
Power Transition (Off -> On)	Moxa switch is powered up
Turbo Ring Break	The Turbo Ring is broken. Only the MASTER switch of Turbo Ring will output warning relay.

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).
RX-Threshold (%)	If the Traffic-Overload option is enabled for the port, specify the RX threshold (in %).
TX-Threshold (%)	If the Traffic-Overload option is enabled for the port, specify the TX threshold (in %).
Traffic-Duration (sec.)	A Traffic-Overload warning is sent if the Traffic-Threshold is exceeded for the specified duration (in seconds).

Override relay alarm settings

Check the checkbox to override the relay warning setting temporarily. Releasing the relay output will allow administrators to fix any problems with the warning condition.

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.

NOTE

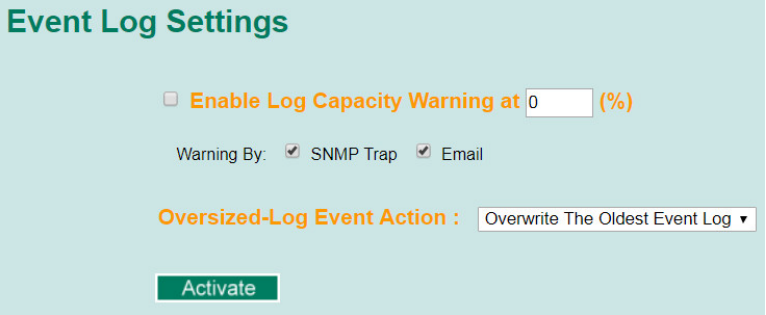
To prevent excessive log recording, once a traffic overload event is triggered, the system will wait for 10 seconds before resuming to check the port's traffic load.

Warning List

Use this table to see if any relay alarms have been issued.

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.



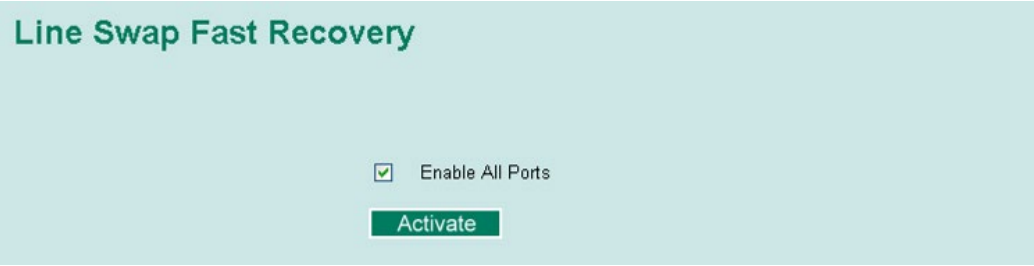
Oversized-Log Event Action

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.	

Using Line-Swap-Fast-Recovery

The Line-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 on 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 Line-Swap Fast Recovery function, or to re-enable the function after it has already been disabled, access either the Console utility's **Line-Swap recovery** page, or the Web Browser interface's **Line-Swap fast recovery** page, as shown below.

Configuring Line-Swap Fast Recovery



Enable Line-Swap-Fast-Recovery

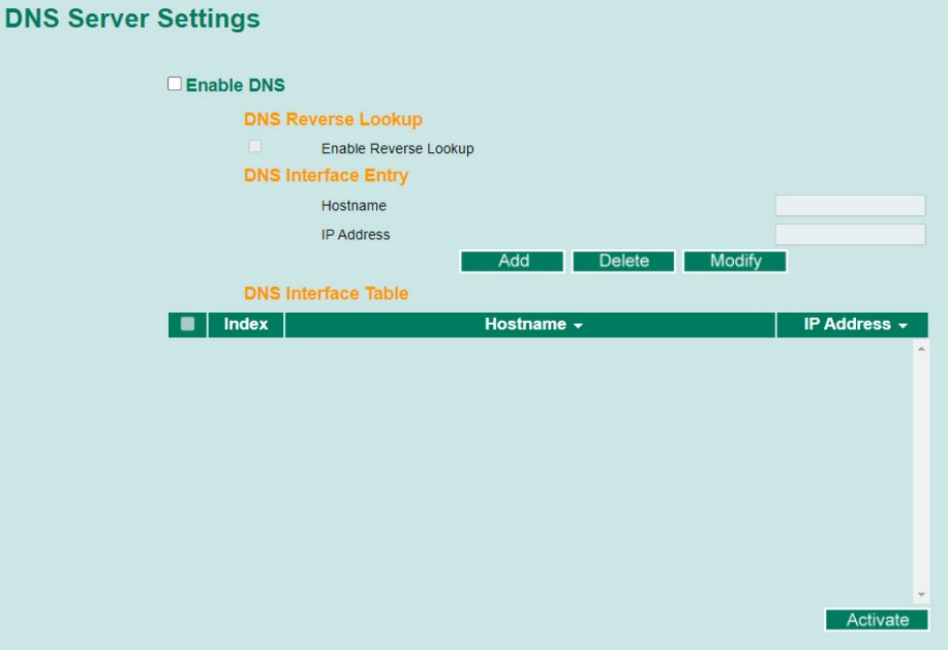
Setting	Description	Factory Default
Enable/Disable	Checkmark the checkbox to enable the Line-Swap-Fast-Recovery function	Enable

DNS Server

Domain Name System (DNS) Server contains a database of IP addresses and their associated hostnames, and it can translate the hostname that DNS client request to an IP address that the host device really is. With DNS server, it is easier to manage IP addresses with easy-to-recognized hostnames.

NOTE

This function is supported in the TN-4500A and TN-5516A/18A Series switches.



Enable DNS

Setting	Description	Factory Default
Enable/Disable	Enable or disable DNS server functionality.	Disable

DNS Reverse Lookup

Enable Reverse Lookup

Setting	Description	Factory Default
Enable/Disable	Enable or disable the DNS Reverse Lookup function.	None

DNS Interface Entry

Hostname

Setting	Description	Factory Default
Max. 63 characters	Enter the hostname of the DNS server. NOTE: Only "a-z", "A-Z", "0-9", "-", "." are allowed.	None

IP Address

Setting	Description	Factory Default
Max. 15 characters	Enter the IP address of the DNS server.	None

NOTE

The maximum number of DNS Interface Entries in the TN-4500A Series is 1024, and in TN-5516A/18A Series is 512.

Using Set Device IP

There are two Set Device IP settings depending on the specific model of the switch.

Type	Models Supported
Type 1	TN-5524 Series
Type 2	TN-5508A Series, TN-5510A Series, TN-5516A Series, TN-5518A Series, TN-5800A Series, TN-4516A Series, TN-4524A Series, TN-4528A Series, TN-5524 Series

To reduce the effort required to set up IP addresses, the Moxa switch comes equipped with DHCP/BootP server and RARP protocol to set up IP addresses of Ethernet-enabled devices automatically.

When enabled, the **Set device IP** function allows the Moxa switch to assign specific IP addresses automatically to connected devices that are equipped with *DHCP Client* or *RARP* protocol. In effect, the Moxa switch acts as a DHCP server by assigning a connected device with a specific IP address stored in its internal memory. Each time the connected device is switched on or rebooted, the Moxa switch sends the device the desired IP address.

Take the following steps to use the **Set device IP** function:

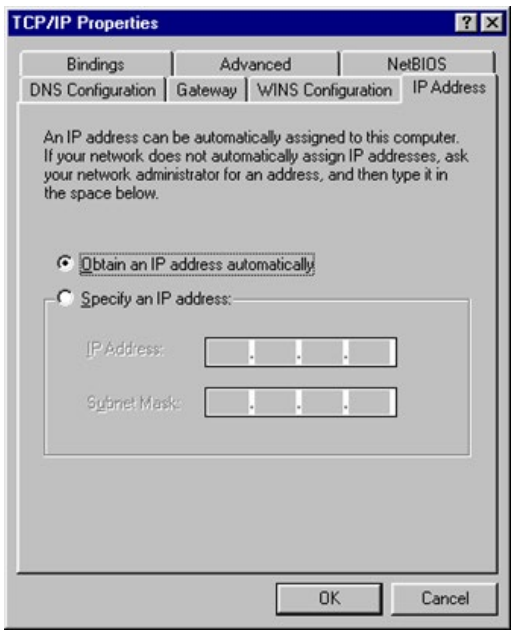
Step 1: *Set up the connected devices*

Set up those Ethernet-enabled devices connected to the Moxa switch for which you would like IP addresses to be assigned automatically. The devices must be configured to obtain their IP address automatically.

The devices' configuration utility should include a setup page that allows you to choose an option similar to the Obtain an IP address automatically option.

For example, Windows' TCP/IP Properties window is shown at the right. Although your device's configuration utility may look quite a bit different, this figure should give you some idea of what to look for.

You also need to decide which of the Moxa switch's ports your Ethernet-enabled devices will be connected to. You will need to set up each of these ports separately, as described in the following step.



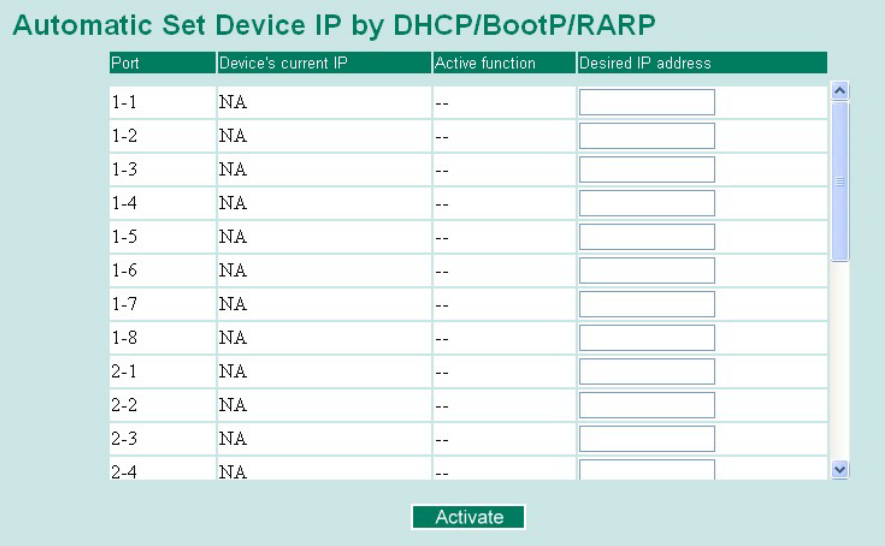
Step 2: Configure the Moxa switch's **Set device IP** function, either from the Console utility or from the Web Browser interface. In either case, you simply need to enter the **Desired IP** for each port that needs to be configured.

Step 3: Be sure to activate your settings before exiting.

- When using the Web Browser interface, activate by clicking on the Activate button.
- When using the Console utility, activate by first highlighting the **Activate** menu option, and then press **Enter**. You should receive the **Set device IP settings are now active! (Press any key to continue)** message.

Configuring Set Device IP (Type 1)

Automatic "Set Device IP" by DHCP/BootP/RARP



Desired IP Address

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

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:

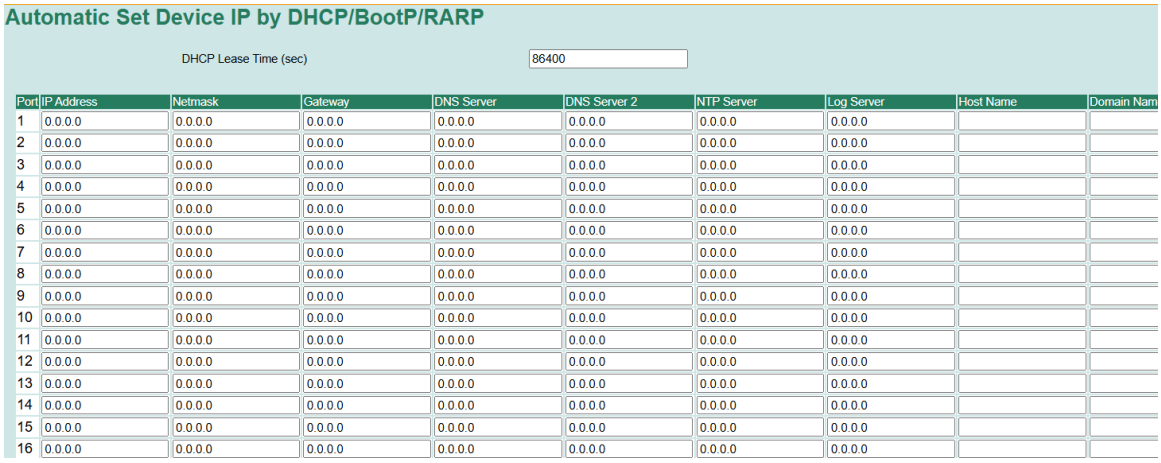
01–00–0F–03 is the "Circuit ID" of port number 3 with port VLAN ID 15.

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.

Configuring Set Device IP (Type2)

Automatic "Set Device IP" by DHCP/BootP/RARP



IP Address

Setting	Description	Factory Default
IP Address	Set the desired IP address on designated ports of connected devices.	0.0.0.0

Netmask

Setting	Description	Factory Default
Netmask	Set the netmask to divide an IP address into subnets.	0.0.0.0

Gateway

Setting	Description	Factory Default
Gateway	A router interface connected to the local network that sends packets out of the local network.	0.0.0.0

DNS Server

Setting	Description	Factory Default
DNS Server	Set the IP address of the DNS server used by your network. After specifying the DNS server's IP address, you can use the domain name to open the web console instead of entering the IP address.	0.0.0.0

DNS Server 2

Setting	Description	Factory Default
DNS Server	Set the IP address of the secondary DNS server used by your network. After specifying the DNS server's IP address, you can use the domain name to open the web console instead of entering the IP address.	0.0.0.0

NTP Server

Setting	Description	Factory Default
NTP Server	Set the IP address of the NTP server and it will be used to synchronize the clocks of devices.	0.0.0.0

Log Server

Setting	Description	Factory Default
Log Server	Configure the IP address of the log server used by your network. The DHCP client will obtain the log server's IP address based on DHCP Option 7.	0.0.0.0

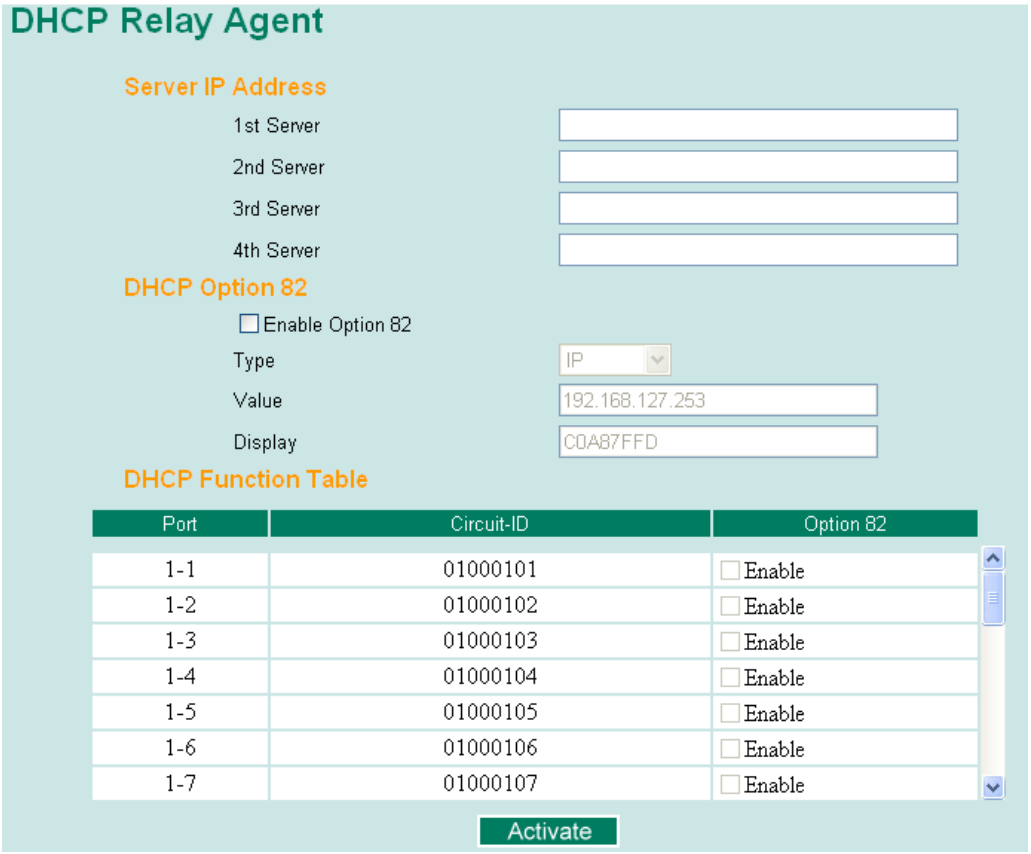
Host Name

Setting	Description	Factory Default
Host Name	The host name is used by client for easy distinguish compare to IP address	None

Domain Name

Setting	Description	Factory Default
Domain Name	The domain name is used for DHCP client when resolving host name with DNS	None

Configuring DHCP Relay Agent



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

Type

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. 12 characters	Displays the value that was set. Complete this field if type is set to Other.	Switch IP address

Display

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.	COA87FFD

DHCP Function Table

Enable

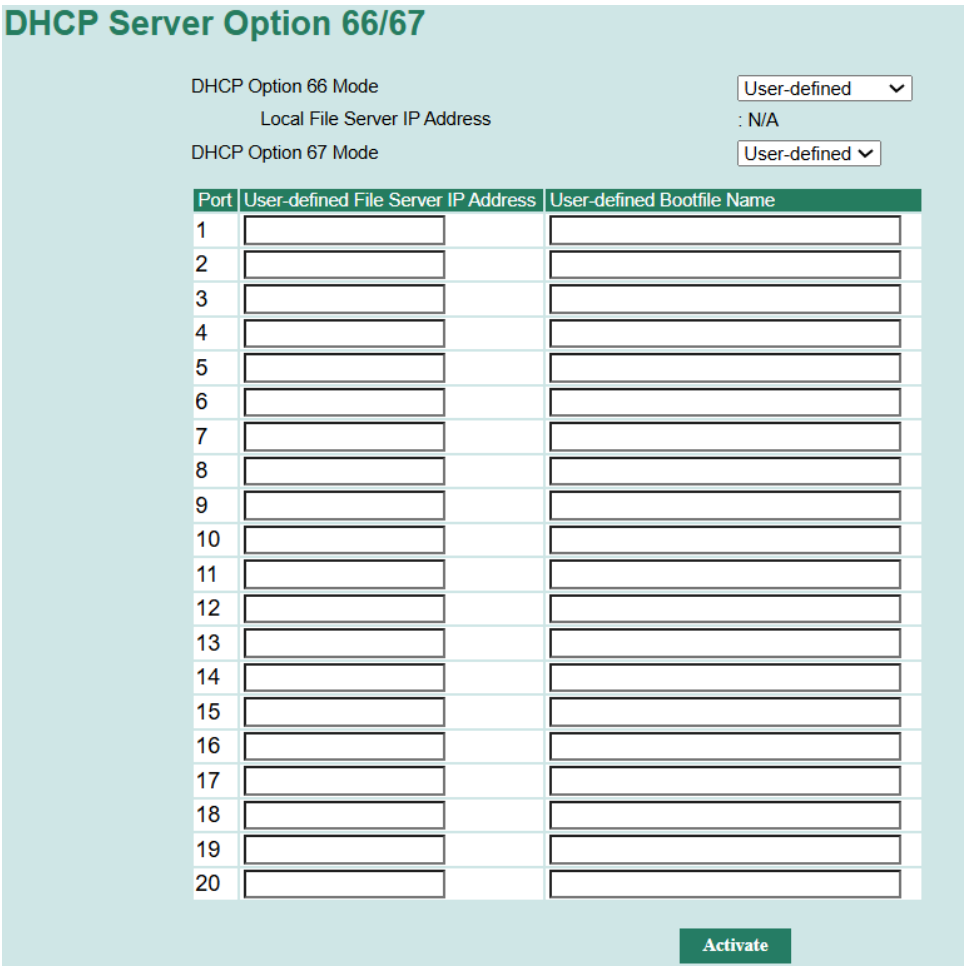
Setting	Description	Factory Default
Enable or Disable	Enable or disable the DHCP Option 82 function for this port.	Disable

Configuring DHCP Server Option 66/67

The **DHCP Server Option 66/67** feature allows users to specify the TFTP server and boot file information for DHCP clients, as defined in RFC 2132. This feature simplifies deployment by streamlining configuration file management for end devices connected to the switch.

- **Option 66**: Specifies the IP address of the TFTP server from which the client should request files.
- **Option 67**: Specifies the name of the boot file that the client should download.

When the device operates as a DHCP client and receives a DHCP reply containing Options 66 and 67, it will contact the file server specified in Option 66 to request the designated configuration file or boot file specified in Option 67. If the file is successfully downloaded, the device will import the configuration file accordingly. Additionally, the device will store and share the Option 66/67 values with other DHCP clients if needed.



When the device operates as a DHCP server, Option 66 and 67 allow users to specify the target configuration file and file server address for DHCP clients. The behavior of these functions depends on the selected mode.

DHCP Option 66 Mode

Setting	Description	Factory Default
Issued by DHCP	The device forwards the DHCP Option 66 value received from its upstream DHCP server to the configured DHCP clients through designated ports. In this mode, the **User-defined File Server IP Address** field will be automatically populated and cannot be modified,	User-defined
User-defined	Users can manually specify the file server IP address in the **User-defined File Server IP Address** field for specific ports. The device will then transmit this value as DHCP Option 66 to associated DHCP clients.	

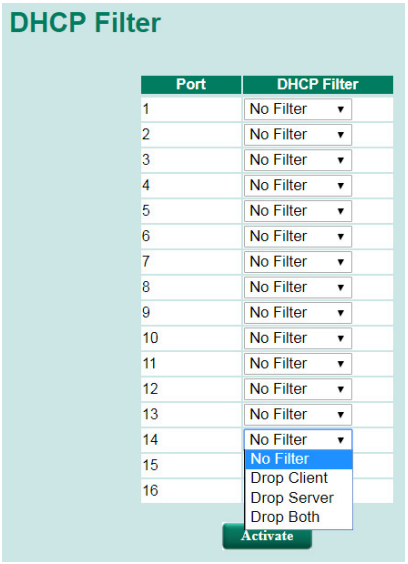
DHCP Option 67 Mode

Setting	Description	Factory Default
User-defined	Users can manually specify the boot file name in the **User-defined Bootfile Name** field for specific ports. The device will transmit this value as DHCP Option 67 to associated DHCP clients.	User-defined
IP Address	The device will use the IP address assigned to the DHCP client as the DHCP Option 67 value. In this mode, the **User-defined Bootfile Name** field will be automatically populated and cannot be modified,	

Configuring DHCP Filter

In some applications, users do not want DHCP packets to interfere with specific devices or networks, therefore, the DHCP Filter function can help filter the packets from DHCP clients, servers, or both.

> **NOTE**
>
> This function is only supported by the TN-4500A Series.



DHCP Filter

Setting	Description	Factory Default
No Filter	No filter on packets	No Filter
Drop Client	Drop packets from DHCP Clients	
Drop Server	Drop packets from DHCP Servers	
Drop Both	Drop packets from both DHCP Clients and Servers	

Using Diagnosis

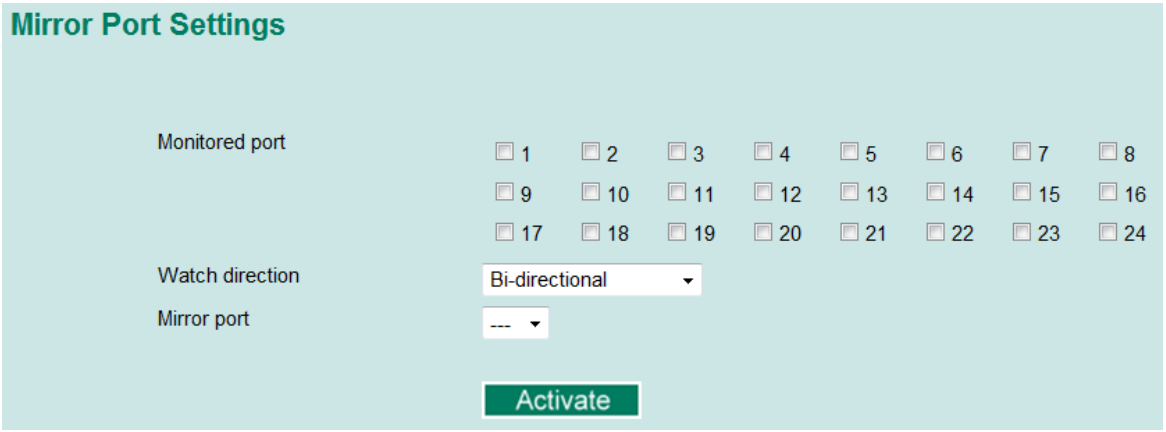
The Moxa switch provides three important tools for administrators to diagnose network systems.

Mirror Port

The **Mirror Port** 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.

Please note that two types of mirror port behavior are available, depending on the specific model of switch. In Type 1, the mirror port can only receive the same data being transmitted to and from an observation port, but does not allow access to the switch via this port. In Type 2, the mirror port can receive the same data being transmitted to and from an observation port, and also allows the switch to access this port.

Type	Models Supported
Type 1	TN-4516A Series, TN-4524A Series, TN-4528A Series
Type 2	TN-5508A/5510A Series TN-5516A/5518A Series, TN-5916A Series, TN-5800A Series



Mirror Port Settings

Setting	Description
Monitored Port	Select the number of the ports whose network activity will be monitored.
Watch Direction	Select one of the following two watch direction options: • Input data stream: Select this option to monitor only those data packets coming into the Moxa switch's port. • Output data stream: Select this option to monitor only those data packets being sent out through the Moxa switch's port. • Bi-directional: 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.

RSPAN

What Is RSPAN?

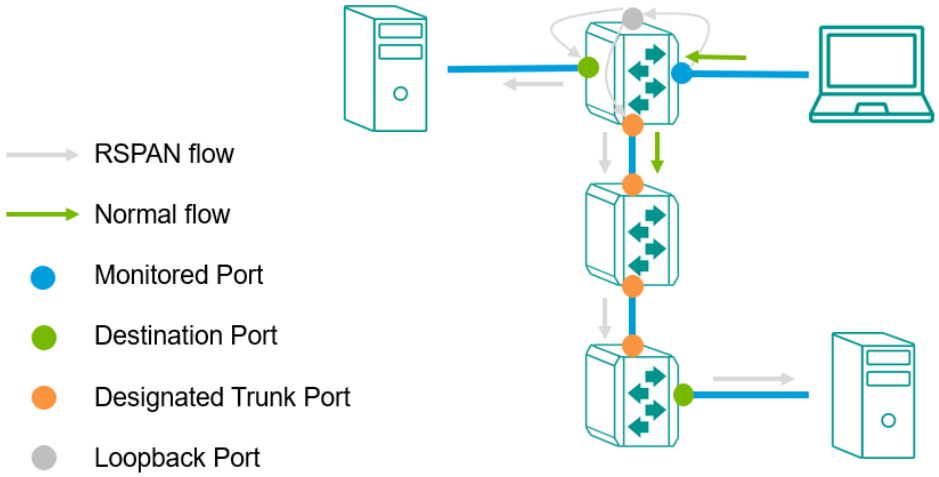
Remote Switched Port Analyzer (RSPAN) is a network monitoring feature that allows traffic from one switch to be mirrored and sent across a Layer 2 network to a remote switch for analysis. Its primary purpose is to give network administrators visibility into traffic flows without requiring monitoring tools to be physically connected to the source switch. By using a dedicated RSPAN VLAN to transport mirrored packets, RSPAN enables centralized monitoring, simplifies troubleshooting across distributed switches, and supports security tools like IDS/IPS by delivering traffic to them wherever they are located.

Each RSPAN setup is a set of configurations affecting a group of switches. Each configuration group consists of multiple components. Refer to the following overview of RSPAN terms, concepts, and definitions:

- **Monitored Ports**: These are the source ports being monitored on a single switch. A RSPAN Group can mirror traffic from multiple monitored ports.
- **Destination Ports**: These are the ports where mirrored traffic is sent. Since only one destination port is available on a single switch, multiple switches within the same RSPAN group are required to support scenarios with multiple destination ports, such as IDS redundancy. Mirror traffic can be forwarded to multiple destination ports across different switches. Each switch can only have one designated destination port.
- **RSPAN VLAN**: A dedicated VLAN for transmitting mirrored RSPAN traffic to the destination port. Each RSPAN group can only have one RSPAN VLAN.
- **Trunk Ports**: These are the VLAN trunk ports that carry RSPAN traffic across switches.
- **Loopback Port**: This port is used to copy mirrored traffic into the RSPAN VLAN. This setting is required whenever you specify at least one monitored port.
- **Watch direction**: RSPAN allows monitoring traffic in the following directions:
  (1) Input data stream: The traffic received on the monitored port(s).
  (2) Output data stream: The traffic transmitted from the monitored port(s).
  (3) Bi-directional: The traffic received and transmitted on the monitored port(s).

Example RSPAN Setup

Consider the following reference diagram illustrating how RSPAN works. Packets transmitted through the monitored port are copied (mirrored) to a loopback port and passed on to both a local destination port on the same switch, and to a destination port on a remote switch via designated trunk ports. Analyzer tools on each destination port analyze the mirrored traffic.



Limitations

- GVRP (GARP VLAN Registration Protocol): GVRP must be disabled when RSPAN is enabled to prevent RSPAN VLAN packets from being forwarded improperly.
- RSPAN VLAN MAC learning: MAC learning must be disabled for the designated RSPAN VLAN. This ensures that RSPAN packets are mirrored correctly and prevents multiple learning instances of the source address within the RSPAN VLAN.
- IGMP Snooping: When IGMP snooping and RSPAN are both enabled, the RSPAN Designated Trunk Port and Destination Port must be added as static querier ports for the IGMP Snooping RSPAN VLAN. This ensures that unknown multicast traffic is mirrored properly.
- Port Mirroring: RSPAN must be disabled before using the Port Mirror function. These two features are mutually exclusive and cannot operate simultaneously.
- Redundant protocols: The RSPAN Monitored port and Loopback port cannot be configured as redundant ports. Ring ports and coupling ports should be configured as designated trunk ports.
- Bandwidth limitation on VLAN trunk ports: Mirrored traffic affects the total bandwidth available on the VLAN trunk ports as the mirrored traffic is effectively duplicated. Traffic should be shaped according to the bandwidth requirements of your network.
- Loopback port: If the loopback port is Fast Ethernet, the total traffic monitored on a single switch cannot exceed 10% of the total port capacity.
- Access control list: RSPAN does not capture management traffic or packets that match ACL rules. Some mirrored packets may be dropped due to ACL rules applied on the Loopback Port, Designated Trunk Port, or Destination Port, resulting in incomplete or unsuccessful monitoring.

Recommendations

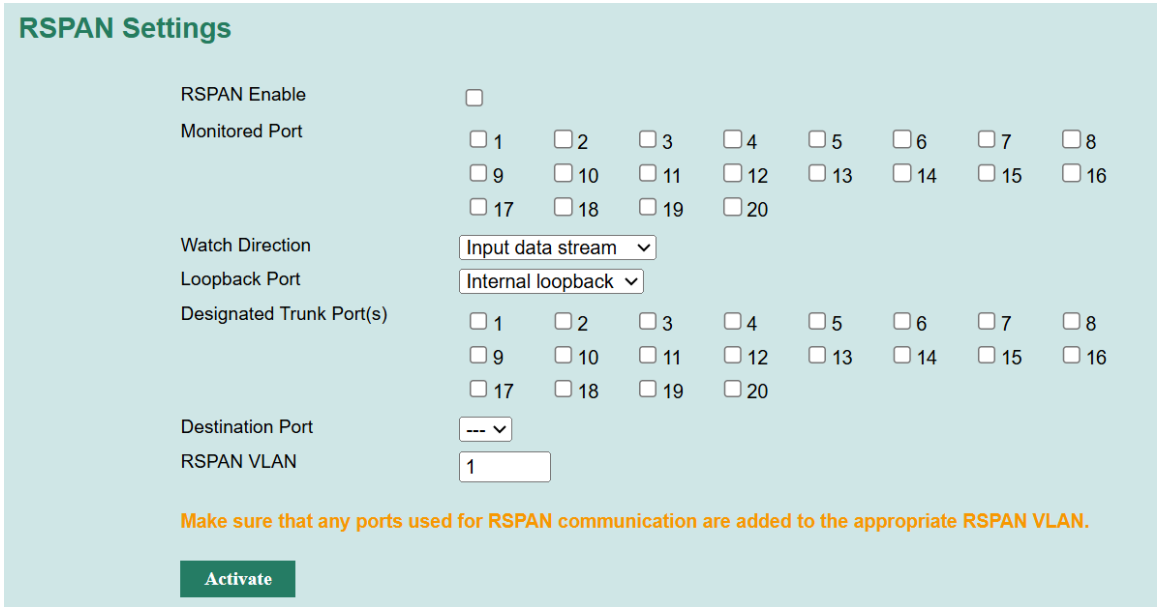
Enabling RSPAN may lead to traffic congestion, potentially resulting in packet loss. To mitigate this risk, we strongly recommend conducting a thorough analysis and testing of the configuration before deploying RSPAN in a live environment. For instance, if video stream ports are mistakenly configured for monitoring, it could significantly impact system performance and lead to noticeable traffic congestion.

If the monitored traffic on a single switch is expected to exceed 10% of the loopback port's capacity, it is recommended to use a physical port with a loopback cable attached. The loopback port mode should also be set to **External loopback** in this case. This limitation only applies if the loopback port is Fast Ethernet.

RSPAN Settings

NOTE

RSPAN is only available on the TN-4500A Series.



RSPAN Enable

Setting	Description	Factory Default
Enable or Disable	Enable or disable the RSPAN feature.	Disabled

Monitored Port

Setting	Description	Factory Default
Enable or Disable	Select the port(s) that will be used to capture traffic for monitoring purposes. Both regular and trunk ports can be designated as monitored ports.	Disabled

Watch Direction

Setting	Description	Factory Default
Input data stream	Only mirror traffic received on the monitored port(s).	Input data stream
Output data stream	Only mirror traffic transmitted from the monitored port(s).	
Bi-directional	Monitor both incoming and outgoing traffic on the monitored port(s).	

Loopback Port

Setting	Description	Factory Default
Internal loopback	The switch will use an available internal Fast Ethernet port as the loopback port for RSPAN.	Internal loopback
External loopback	Designate a physical port as the loopback port. To use this function, a physical loopback cable must be connected to the selected port.	

NOTE

Trunk ports cannot be designated as the loopback port.

NOTE

For TN-4528A models, you must select the loopback port, regardless of whether you choose **Internal loopback** or **External loopback**.

Designated Trunk Port(s)

Setting	Description	Factory Default
Enable or Disable	Select the ports to act as VLAN trunk ports that carry RSPAN traffic across switches. Both regular and trunk ports can be designated as monitored ports.	Disabled

Destination Port

Setting	Description	Factory Default
Port	Select the port to act as the destination ports that the mirrored traffic will be sent to.	None

NOTE

Trunk ports cannot be designated as destination ports.

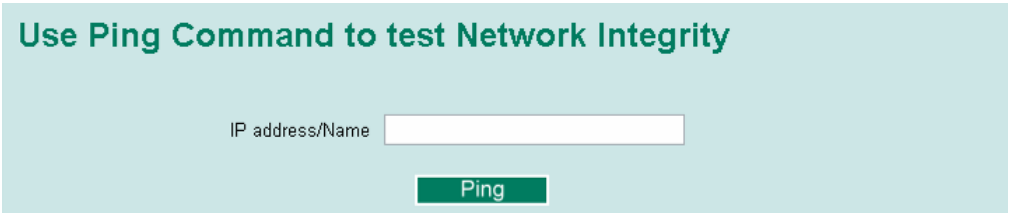
RSPAN VLAN

Setting	Description	Factory Default
1 to 4094	Specify the RSPAN VLAN ID. The RSPAN VLAN cannot be the same as the Management VLAN.	1

NOTE

As RSPAN affects VLAN settings, review VLAN settings after configuring RSPAN to ensure everything is set up and working correctly.

Ping



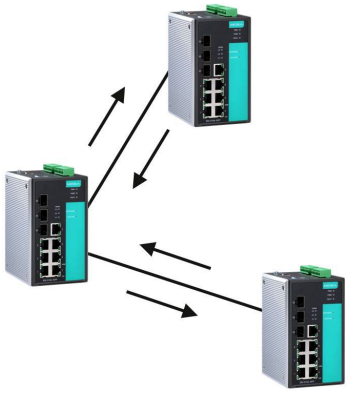
The **Ping** function uses the *ping* command to give users a simple but powerful tool for troubleshooting network problems. The function's most unique feature is that even though the ping command is entered from the user's PC keyboard, the actual ping command originates from the Moxa switch itself. 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.

LLDP Function

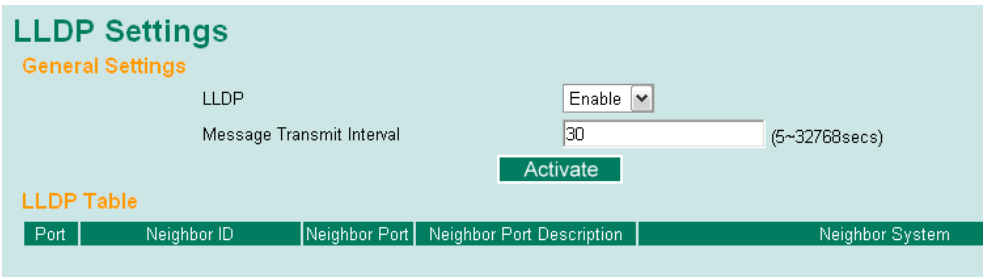
Overview

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.	30 (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.

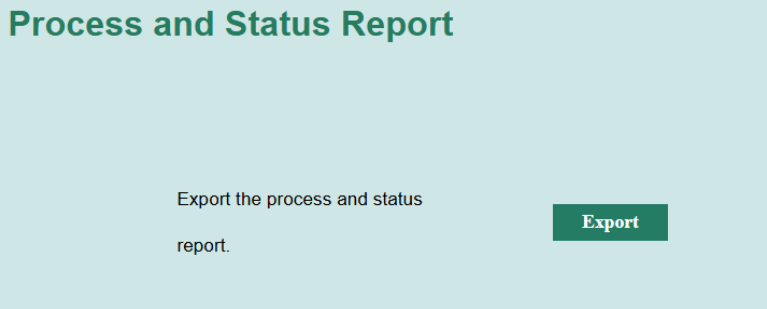
Process and Status Report

This function lets you export specific device information as a report that is used by Moxa Technical Support for analysis and troubleshooting purposes. The contents of the report will be encrypted and can only be decrypted by Moxa Technical Support.

The report includes the following information:

- Information about all running threads
- Dynamic memory information and CPU loading
- System memory status
- Debug logs

Click **Export** to generate and download the report.



Duplicate IP Detection

Duplicate IP Detection detects and records IP conflicts occurring on the management VLAN, using one of the three methods:

- **Passive Detection**: The device will check each incoming ARP packet to see if the sender IP address is the same as the device IP address. However, passive detection cannot detect the conflict if the conflicting device does not actively send ARP packet to the switch. This is the default mode.
- **Active Detection**: When active detection is enabled, the switch will periodically broadcast an ARP Probe to each forwarding port at the specified interval. This can prompt other devices to reply with ARP packets to the switch, so that conflicts can be detected through passive detection. This mode provides a more proactive way to detect conflicts, in case there are other devices that do not actively send out ARP packets.
- **Manual Detection**: An immediate detection scan performed by the user at any given time. This detection is independent from the active detection.

The **Duplicate IP Detection** feature is designed according to the IPv4 Address Conflict Detection function defined in RFC-5227 (https://www.rfc-editor.org/rfc/rfc5227.html).

The detection behavior as defined in RFC-5227 covers the following:

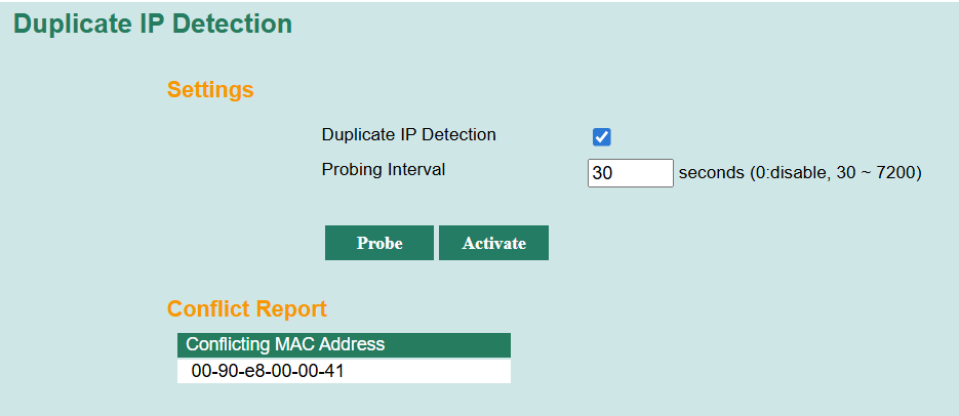
- **Passive Detection**: Checks if the sender's IP address matches the local IP address.
- **Active Detection (ARP Probe)**: Checks if the IP is in use by other devices before using the IP. This behavior will not update this IP in the ARP table of other devices.
- **ARP Announcement**: Announces that the device is using this IP. This behavior will update the hardware address of this IP in other devices' ARP table if this IP already exists in their ARP tables. Moxa's implementation of IPv4 conflict detection does not include the ARP Announcement behavior.

NOTE

While the Moxa switch does not support ARP Announcements for duplicate IP detection, the switch does send ARP Announcements to all forwarding ports under the following conditions:

- When the device changes its IP address.
- When a device obtains an IP address from the DHCP server.

Whenever an IP conflict is detected, the MAC address of the conflicting device will be shown in the **Conflict Report** section and in the **System Log**.



Settings

Duplicate IP Detection

Setting	Description	Factory Default
Enable or Disable	Enable or disable Duplicate IP Detection. If enabled, the switch will perform passive IP conflict detection.	Enabled

Probing Interval

Setting	Description	Factory Default
30 to 7200	Specify the probing interval (in seconds). If set, the switch will perform active IP conflict detection by periodically sending out ARP Probes at the specified interval. If set to 0, active detection will be disabled.	30

Conflict Report

This section shows the MAC addresses of the devices with an IP conflict. The report table will show a total of 16 records; any subsequently detected conflicts will not be recorded.

NOTE

IP conflict records in the **Conflict Report** section will be cleared under the following situations:

- If no ARP packet has been received from the corresponding MAC address after three consecutive ARP Probes at the specified interval.
- When the device is rebooted.
- When the Duplicate IP Detection function is disabled.
- When the IP of the device is changed.
- When a manual detection scan is performed by pressing **Probe**.

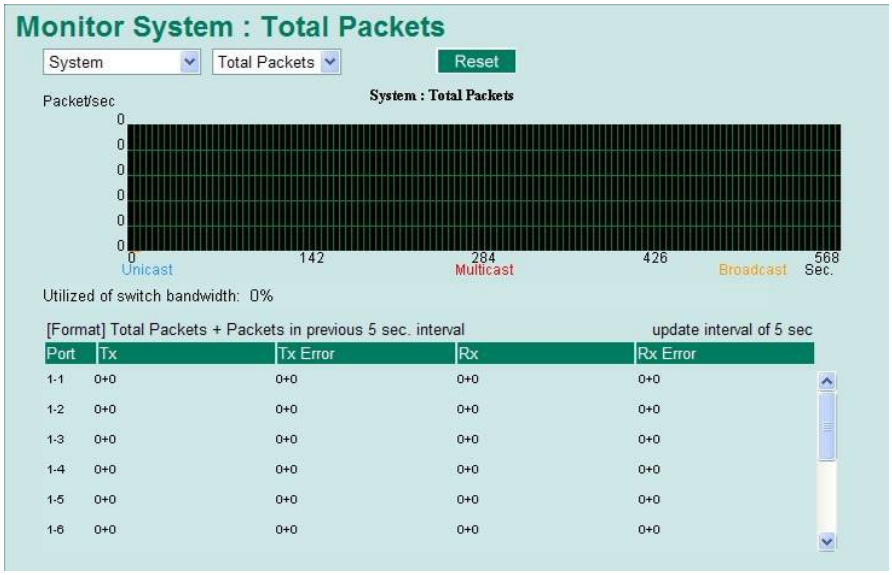
Using Monitor

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

Monitor by Switch

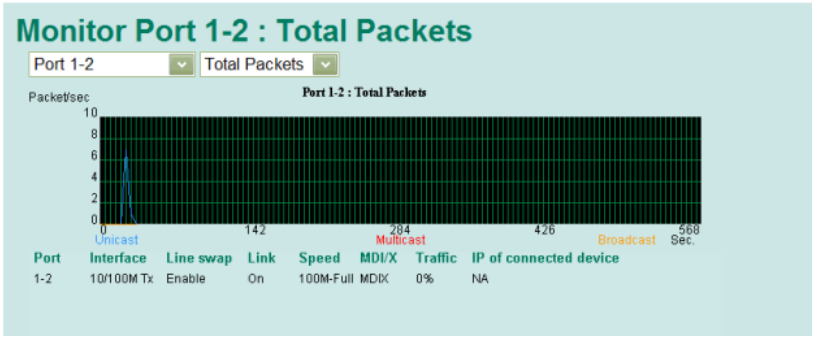
Access the Monitor by selecting **System** from the left selection bar. Monitor by System allows the user to view a graph that shows the combined data transmission activity of all of the Moxa switch's 18 ports. Click one of the four options—**Total Packets**, **TX Packets**, **RX Packets**, or **Error 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 Packets 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.



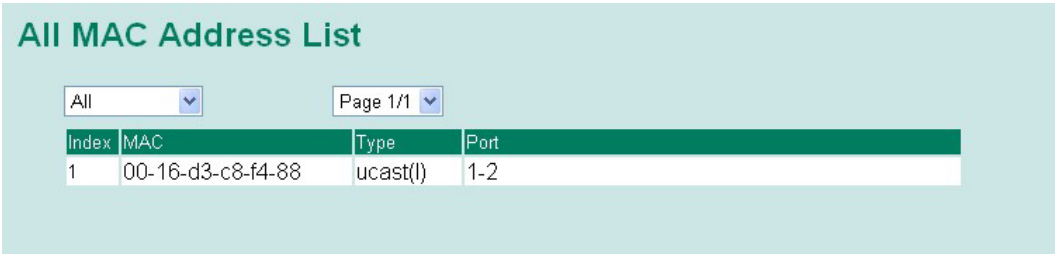
Monitor by Port

Access the Monitor by Port function by selecting **ALL 10/100M or 1G 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.



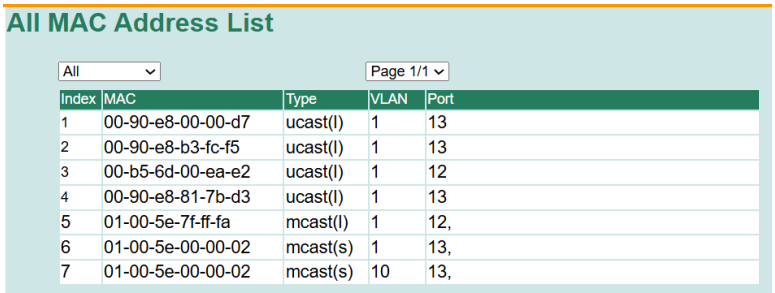
Using the MAC Address Table

This section explains the information provided by the Moxa switch's MAC address table.



NOTE

The VLAN learning method for the TN-4500A was modified from Single VLAN Learning (SVL) to Independent VLAN Learning (IVL) as of firmware version 4.0 to support the RSPAN feature. As a result, an additional VLAN column is shown for TN-4500A Series devices.



NOTE

- The TN-4500A Series supports a total of 2048 entries.

- The TN-5500A Series supports a total of 256 entries.

The MAC Address table can be configured to display the following Moxa switch MAC address groups, which are selected from the 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 Lock	Select this item to show all of the Moxa switch's Static Lock MAC addresses.
ALL Static	Select this item to show all of the Moxa switch's Static, Static Lock, and Static Multicast MAC addresses.
ALL Static 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 addresses 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.
VLAN	This field displays the VLAN ID where the MAC address was learned and associated with a specific port (For the TN-4500A Series only).
Port	This field shows the port that this MAC address belongs to.

Using Access Control List

NOTE

Access Control Lists are available in TN-4500A Series and TN-5800A Series.

Access control lists (ACL) increase the flexibility and security of networking management.

ACL provides traffic filter capabilities for ingress or egress packets. Moxa access control list helps manage filter criteria for diverse protocols and allows users to configure customized filter criteria. For example, users can deny access to specific source or destination IP/MAC addresses.

The Moxa access control list configuration interface is easy-to-use. Users can quickly establish filtering rules, manage rule priorities, and view overall settings in the display page.

The ACL Concept

What is ACL?

Access control list is a basic traffic filter for ingress and egress packets. It can examine each Ethernet packet's information and take necessary action. Moxa Layer 3 switches provide complete filtering capability. 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

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

- **Manage authority of hosts:** 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. ACL can restrict packets from or to specific subnets.
- **Network security:** The demand for networking security is growing. ACL can provide basic protection which works similarly to an Ethernet firewall device.
- **Control traffic flow by filtering specific protocols:** ACL can filter specific IP protocols such as TCP or UDP packets.

How ACL works

ACL working structure is based on access lists. Each access list is a filter. When a packet enters into or exits from a switch, ACL will compare the packet to the rules in the access lists, starting from the first rule. If a packet is rejected or accepted by the first rule, the switch will drop or pass this packet directly without checking the rest of the lower-priority rules. In the other words, Access Control List has "Priority Index" as its attribute to define the priority in the web configuration console.

There are two types of settings for an ACL: the *list* settings, and the *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. 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. In this function, there are two types of packet filtering available:

- IP based
- MAC Based

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

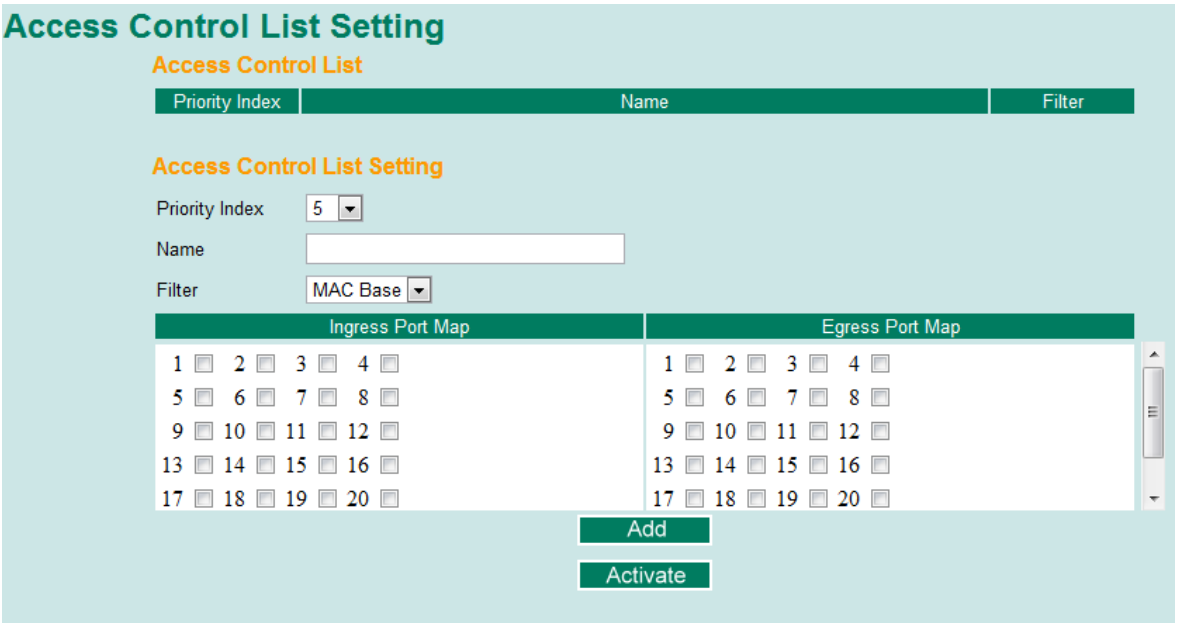
After adding a new access control list, you can also create new rules for the access control list. Each ACL group accepts 10 rules. Rules can filter packets by source and destination IP/MAC address, IP protocol, TCP/UDP Port, Ethernet Type, and VLAN ID.

After all rules are set, 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 List Settings

Creating an access control list starts at the Access Control List Setting page.



In this page, you can mainly configure two settings:

Add/Modify Access Control List

This function lets you **Add** a new access control list or **Modify** an existing access control list. The operation depends on the **Priority Index** you select. If the selected priority index is still empty, you can start by creating a new access control list. Parameters for editing are:

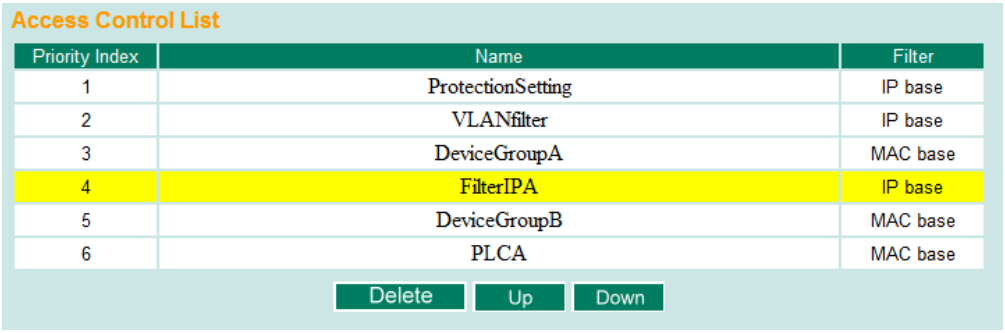
- **Priority Index:** ACL checking sequence is based on this index. Smaller index numbers have higher priority for packet filtering. If a packet is filtered by an access list with higher priority, those access lists with lower priority will not being executed.

  Note that Priority Index is not a one-to-one index for each list name. It changes when swapping the priority of different access control lists.

  The maximum Priority Index number is 16.
- **Name:** You can name the access control list in this field. This is the access list's unique name.
- **Filter:** Select filtering by either IP or MAC address. Detailed settings can be configured in the **Access Control Rule Settings** page.
- **Ingress Port Map/Egress Port Map:** You can choose which ports to apply the rules to. The Ingress and Egress condition uses **OR** logic. This means a packet only needs to match one ingress or egress port rule to be examined.

If a selected priority index is already in the access control list, then you can modify these parameters listed above. After configuration, click **Activate** to confirm the settings. Then you will see a new list appear in the **Access Control List** table.

Adjust ACL Priority Index



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

Step 1: Select the list

Step 2: Click the **Up/Down** button to adjust the sequence. The Priority Index will change with the list's position.

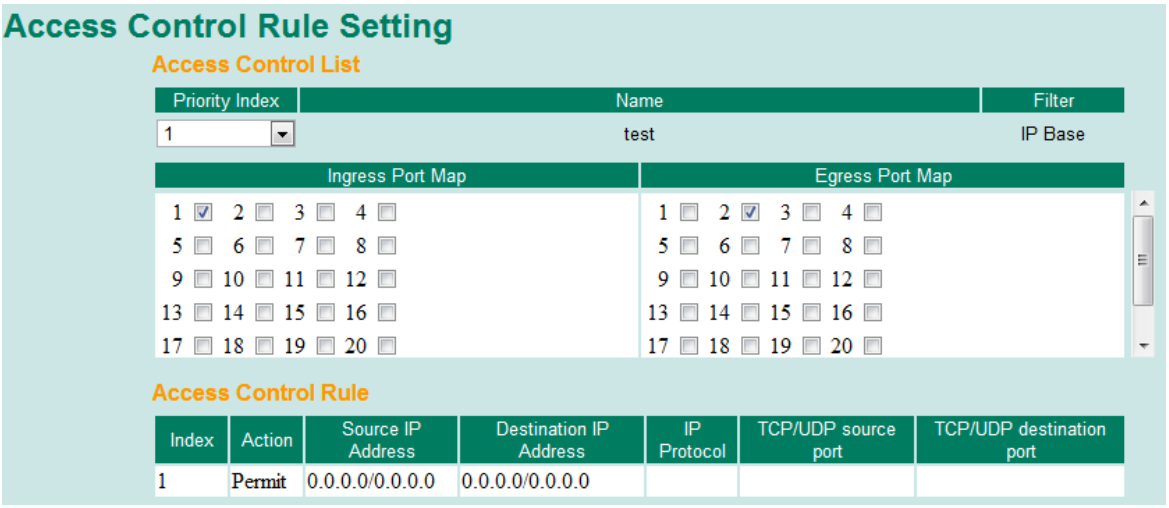
Step 3: Click the **Activate** button to confirm the settings.

NOTE

TN-4500A Series switch only supports Ingress Port Map, and the TN-5800A Series switch supports both Ingress and Egress Port Map.

Access Control Rule Settings

You can edit an access control list's rules on this page. Each ACL can include up to 10 rules.



First, select the access control list you would like to edit based on the Priority Index. The Ingress/Egress Port map will display the port settings.

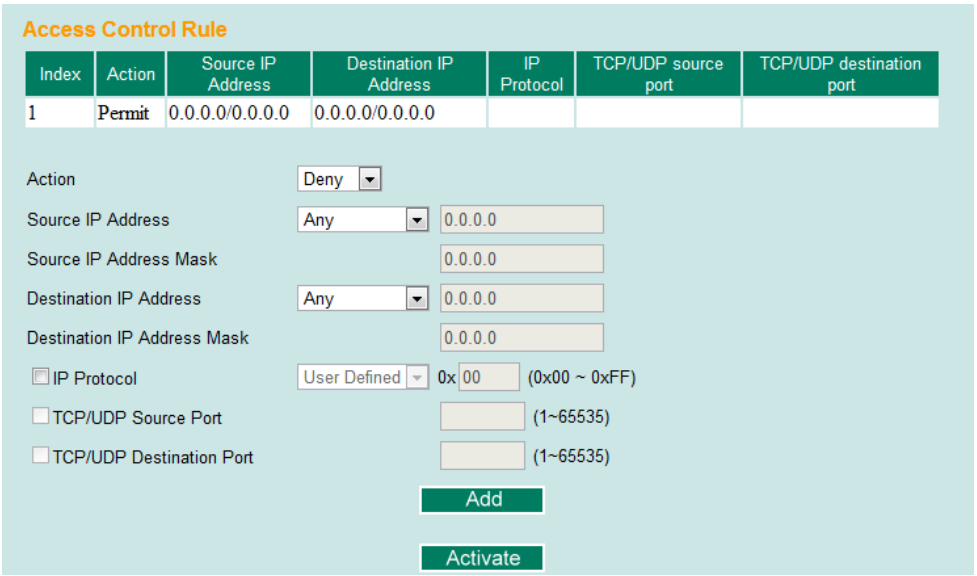
NOTE

The port map here is also editable. Any change here will change the access control list settings.

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

IP-Based

After configuring, click Add button to add the rule to the list. Then, click Activate to activate the settings.

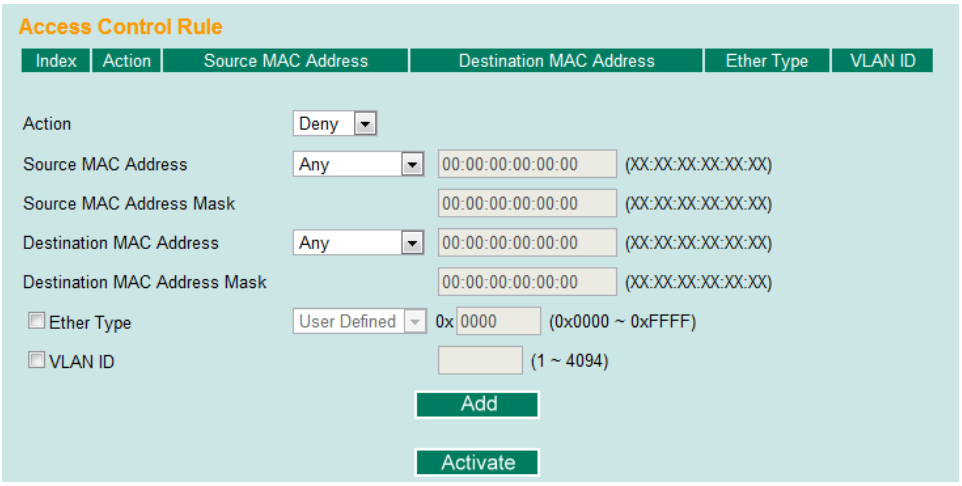


- **Action:** Select the action if the rule criterion is met.
  - **Deny**: Drop packets when the ACL rule is met.
  - **Permit to Low Priority Queue**: Forward packets with low priority when the ACL rule is met.
  - **Permit to Normal Priority Queue**: Forward packets with normal priority when the ACL rule is met.
  - **Permit to Medium Priority Queue**: Forward packets with medium priority when the ACL rule is met.
  - **Permit to High Priority Queue**: Forward packets with high priority when the ACL rule is met.

- **Source IP Address/Source 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 Port, TCP/UDP Destination Port:** If TCP or UDP are selected as the filtering protocol, these fields will allow you to enter port numbers for filtering.

Once ready, click the **Add** button to add the rule to the list. Then, click **Activate** to activate the settings.

MAC-Based

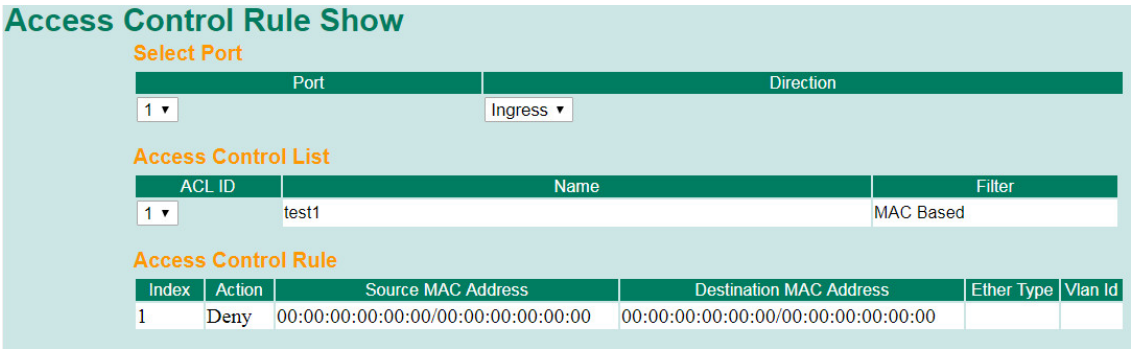


- **Action:** Select the action if the rule criterion is met.
  - **Deny**: Drop packets when the ACL rule is met.
  - **Permit to Low Priority Queue**: Forward packets with low priority when the ACL rule is met.
  - **Permit to Normal Priority Queue**: Forward packets with normal priority when the ACL rule is met.
  - **Permit to Medium Priority Queue**: Forward packets with medium priority when the ACL rule is met.
  - **Permit to High Priority Queue**: Forward packets with high priority when the ACL rule is met.
- **Source MAC Address/Source 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 criteria.
- **Ethernet Type:** Select the type of Ethernet protocol to filter. Options here are **IPv4, ARP, RARP, IEEE802.1Q, IPv6, IEE802.3, PROFIENT,** and **LLDP**
- **VLAN ID:** Enter a VLAN ID you would like to filter by.

Once ready, click the **Add** button to add the rule to the list. Then, click **Activate** to activate the settings.

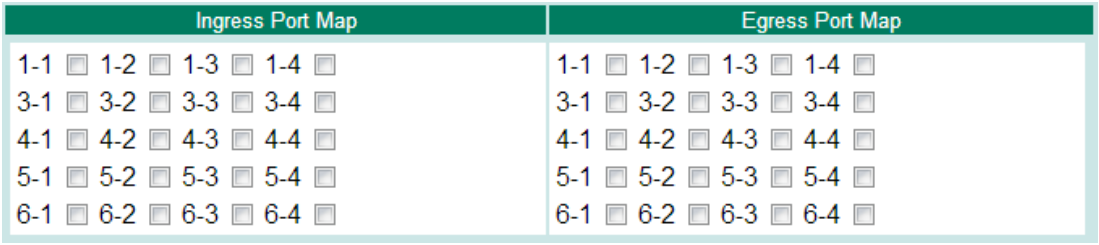
Access Control Rule Show

The Access Control Rule Show page provides a complete view of all ACL settings. In this page, you can view the rules by **Ingress** port, **Egress** port, or **Priority Index**. Click the drop-down menu to select the Port or Priority Index, and all the rules will be displayed in the table.



NOTE

For TN-5800A series, there are two limitations on ACL settings. Based on the ingress port type of ACL rules, there are two types for the limitation of numbers.



Limitation Type 1:

When rules contain Ingress Fast Ethernet (FE) ports, the **Number should NOT be greater than 160**.

Limitation Type 2:

When rules contain Ingress Gigabit Ethernet (GE) ports or no Ingress ports, the **Number should NOT be greater than 40**.

Example 1 for Limitation 1

Rule A contains 3 ingress FE ports and 4 egress FE ports, and it results in the number of 3 x 4 = 12.

Rule B contains 5 ingress FE ports and 6 egress GE ports, and it results in the number of 5 x 6 = 30.

Rule C contains 7 ingress FE ports and no egress port, and it results in the number of 7.

Make sure the amount of those numbers "12+30+7" is not greater than 160.

Example 2 for Limitation 2

Rule D contains 1 ingress GE port and 2 egress FE ports, and it results in the number of 1 x 2 = 2.

Rule E contains 3 ingress GE ports and 4 egress GE ports, and it results in the number of 3 x 4 = 12.

Rule F contains 5 ingress GE ports and no egress ports, and it results in the number of 5.

Rule G contains no ingress ports and 6 FE egress ports, and it results in the number of 6.

Rule H contains no ingress ports and 7 GE egress ports, and it results in the number of 7.

Make sure the amount of those numbers "2+12+5+6+7" is not greater than 40.

Example 3 for Limitation 1 and 2

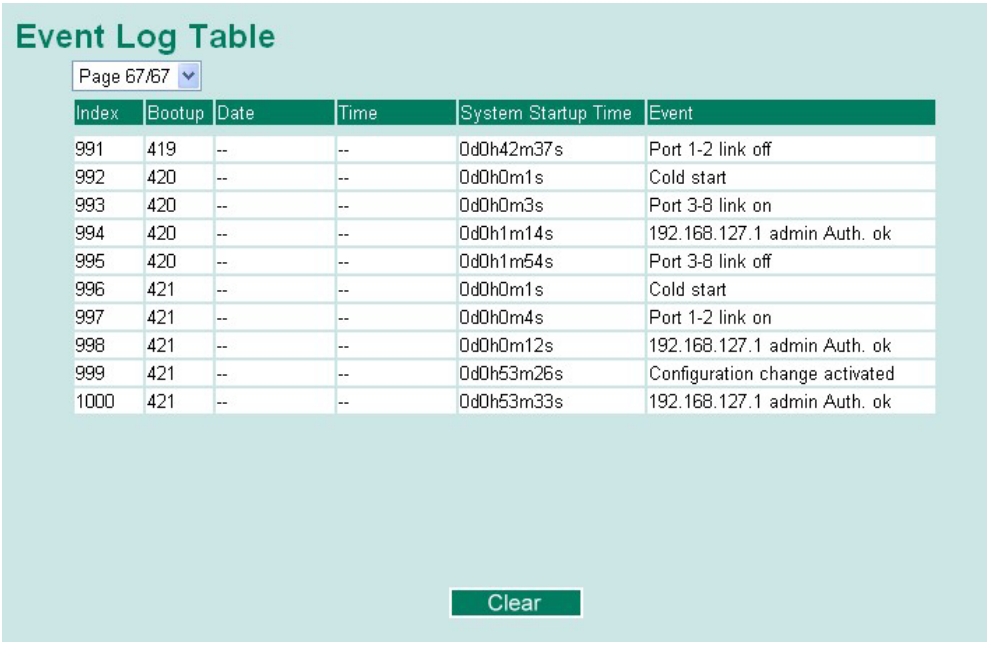
Rule Z contains 3 ingress FE ports, 2 ingress GE ports, and 5 egress GE ports.

It results in the number of 3 x 5 = 15 in Limitation 1, and 2 x 5 = 10 in Limitation 2.

Make sure the amount in limitation 1, "15", is not greater than 160.

Make sure the amount in limitation 2, "10", is not greater than 40.

Using Event Log



The Event Log Table displays the following information:

Bootup	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.
Events	Events that have occurred.

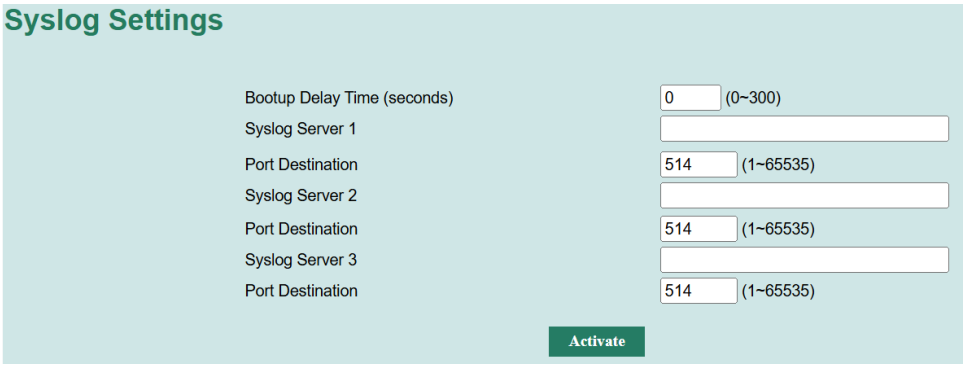
NOTE

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

Using Syslog

The Syslog function provides the event logs for the syslog server. The function supports 3 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.



Bootup Delay Time (seconds)

Setting	Description	Factory Default
0 to 300	Specify the boot-up delay (in seconds). The switch may boot up faster than the syslog server, which may result in some logs being lost. To prevent this, you can specify the duration for the switch to wait for the syslog server to be ready before sending logs.	0

Syslog Server 1/2/3

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 1/2 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

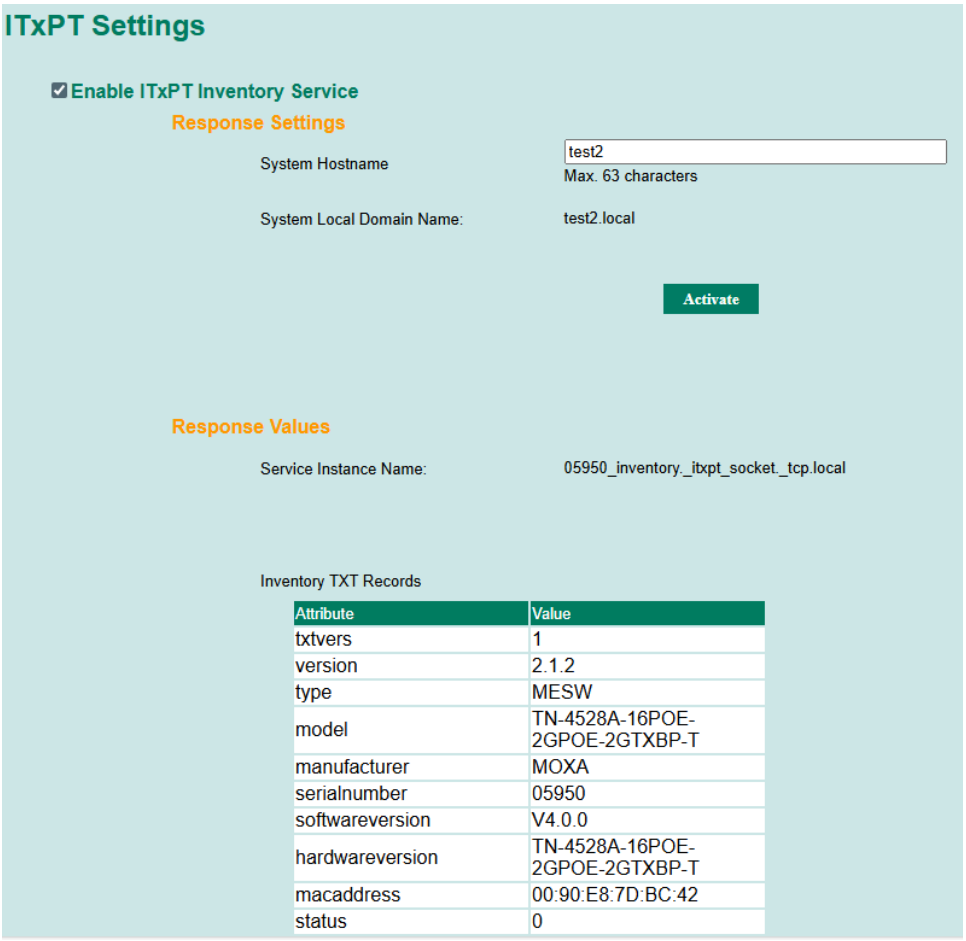
ITxPT Settings

NOTE

This feature is only available on the TN-4500A Series.

This feature allows a device to announce its presence and available services on a local network. To support the Module Inventory Service specification as defined in ITxPT S02P01, the switch can reply to module-inventory queries using the ITxPT-defined headers and content. This allows ITxPT tools to recognize, parse, and retrieve the relevant information. The system uses two protocols to achieve this:

- **Multicast DNS (mDNS)**: This protocol provides a non-centralized DNS query and reply mechanism. Devices using mDNS can perform DNS queries and replies without knowing the location of the DNS Server. mDNS-capable devices can act as client or server at the same time without requiring centralized management of the DNS Server.
- **DNS-Based Service Discovery (DNS-SD)**: This protocol provides a service discovery method by redefining the original DNS format and data. DNS-SD essentially functions the same as DNS and is compatible with mDNS. The only difference lies in its redefinition of the data within the domain name field for service discovery.



Enable ITxPT Inventory Service

Setting	Description	Factory Default
Enable or Disable	Enable or disable the ITxPT Inventory Service feature. When enabled, the device will respond to DNS-SD and Module Inventory Service queries.	Enabled

System Hostname

Setting	Description	Factory Default
1 to 63 characters	Enter the device's system hostname. Only letters (a-z, A-Z), numbers (0-9), and hyphens (-) are supported. The hostname cannot start or end with a hyphen (-). The **System Local Domain Name** is automatically generated by adding the *.local* suffix to the specified system hostname.	None

Inventory TXT Records

This table shows compliant module information.

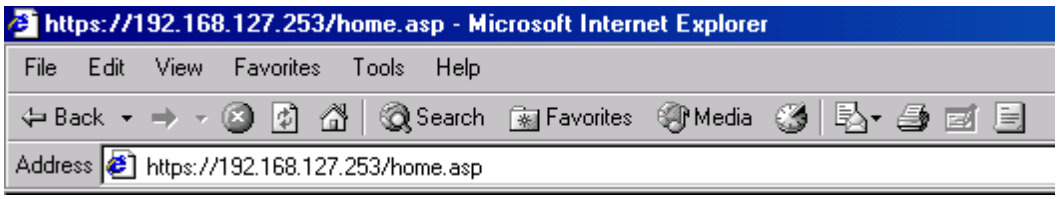
NOTE

All TN-4500A Series switches are categorized as type MESW, as defined by ITxPT.

Using HTTPS/SSL

To secure your HTTP access, the Moxa switch supports HTTPS/SSL to encrypt all HTTP traffic. Perform the following steps to access the Moxa switch's web browser interface via HTTPS/SSL.

1. Open Internet Explorer and type **https://{Moxa switch's IP address}** in the address field. Press Enter to establish the connection.



2. Warning messages will pop up to warn the user that the security certificate was issued by a company they have not chosen to trust.

3. Select **Yes** to enter the Moxa switch's web browser interface and access the web browser interface secured via HTTPS/SSL.

NOTE

Moxa provides a Root CA certificate. After installing this certificate on your PC or notebook, you can access the web browser interface directly and you will no longer see any warning messages. You may download the certificate from the Moxa switch's CD-ROM.

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