

# Moxa Managed Switch MRX (v1.x) Layer 2 User Manual

---

**Version 1.0, April 2024**

[www.moxa.com/products](http://www.moxa.com/products)

**Models covered by this user's manual:**

MRX-G4064-L3-8XGS Series Managed Ethernet Switches

MRX-Q4064-L3-16XGS Series Managed Ethernet Switches



© 2024 Moxa Inc. All rights reserved.

# Moxa Managed Switch MRX (v1.x) Layer 2 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

© 2024 Moxa Inc. All rights reserved.

## Trademarks

The MOXA logo is a registered trademark of Moxa Inc.  
All other trademarks or registered marks in this manual belong to their respective manufacturers.

## 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](http://www.moxa.com/support)

# Table of Contents

<b>1. About This Manual</b> .....	<b>5</b>
Symbols for the Meanings in the Web Interface Configurations .....	6
About Note, Attention, and Warning .....	7
Configuration Reminders .....	8
A: About Mandatory Parameters.....	8
B: Configurations before Enable/Disable.....	8
<b>2. Getting Started</b> .....	<b>9</b>
Log in by Web Interface .....	9
Connecting to the Switch.....	10
Log in by RS-232 Console .....	11
Log in by Telnet.....	14
<b>3. Web Interface Configuration</b> .....	<b>17</b>
Function Introduction .....	17
Device Summary .....	18
Model Information .....	18
Panel Status .....	19
Event Summary (Last 3 Days) .....	20
CPU Utilization History .....	21
System.....	22
System Management .....	22
Account Management.....	34
Out of band management.....	40
Time .....	42
System Time .....	43
NTP Server.....	47
Time Synchronization .....	47
Port .....	51
Port Interface .....	51
Link Aggregation .....	55
Energy Efficiency Ethernet.....	61
Layer 2 Switching .....	63
VLAN .....	63
GARP Overview .....	71
MAC .....	73
QoS.....	75
Multicast .....	90
Network Redundancy .....	98
Layer 2 Redundancy .....	98
Management .....	127
Network Management.....	127
Security.....	131
Device Security .....	131
Management Interface .....	131
Network Security .....	144
IEEE 802.1X .....	144
Loop Protection .....	167
Authentication .....	168
Login Authentication .....	169
Diagnostics .....	174
System Status .....	174
Log & Event Notification .....	183
Diagnosis .....	200
Maintenance and Tools .....	215
Standard/Advanced Mode.....	215
Disable Auto Save .....	216
Reboot.....	218
Reset to Default .....	219
Log Out of the Switch .....	220

<b>A.</b>	<b>Account Privileges List.....</b>	<b>221</b>
	Account Privileges List.....	221
<b>B.</b>	<b>Event Log Description.....</b>	<b>223</b>
	Event Log Description .....	223
<b>C.</b>	<b>SNMP MIB File .....</b>	<b>226</b>
	Standard MIB Installation Order .....	226
	MIB Tree .....	226
<b>D.</b>	<b>Security Guidelines.....</b>	<b>228</b>
	Installation .....	228
	Physical Installation.....	228
	Account Management.....	228
	Vulnerable Network Ports .....	229
	Operation .....	229
	Maintenance .....	231
	Decommission.....	231



# 1. About This Manual

---

Thank you for purchasing Moxa's managed switch. Read this user's manual to learn how to connect your Moxa switch with various interfaces and how to configure all settings and parameters via the user-friendly web interface.

Three methods can be used to connect to the Moxa's switch, which all will be described in the next two chapters. See the following descriptions for each chapter's main functions.

## Chapter 2: Getting Started

In this chapter, we explain the instruction on how to initialize the configuration on Moxa's switch. We provide three interfaces to access the configuration settings: RS-232 console interface, telnet interface, and web interface.

## Chapter 3: Web Interface Configuration

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

## Appendix A: Account Privileges List

This appendix describes the read/write access privileges for different accounts on Moxa's Managed Ethernet Series switch.

## Appendix B: Event Log Description




























In this appendix, users can check the event log name and its event log description. When any event occurs, this appendix helps users quickly check the detailed definition for each event.

## Appendix C: SNMP MIB File

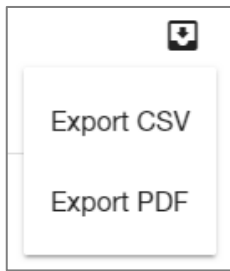
This appendix contains the SNMP MIB files so that users can manage the entities in a network with Moxa's switch.

# Symbols for the Meanings in the Web Interface Configurations

The Web Interface Configuration includes various symbols. For your convenience, refer to the following table for the meanings of the symbols.

Symbols	Meanings
	Add
	Read detailed information
	Clear all
	Column selection
	Refresh
	Enable/Disable Auto Save When Auto Save is disabled, users need to click this icon to save the configurations.
	Export*
	Edit
	Re-authentication
	Delete
	Panel View
	Expand
	Collapse
	Hint Information
	Settings
	Data Comparison
	Menu icon
	Change mode
	Locator
	Reboot
	Reset to default
	Logout
	Increase
	Decrease
	Equal
	Menu
	Search

\*The **Export** function helps users save the current configurations or information for the specific functions. It is located on the upper part of the configuration area. There are two formats available: **CSV**, or **PDF**. Select the format and save in your local computer.



## About Note, Attention, and Warning

Throughout the whole manual, users will see some notes, attentions, and warnings. Here are the explanations for each definition.

**Note:** It indicates the additional explanations for the situation that users might encounter. Here is the example:



### 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.

**Attention:** It indicates the situations where users might take some extra care or it might bring some problems. Here is the example:



### ATTENTION

When a different type of module has been inserted into the switch, we suggest you configure the settings, or use reset-to-default.

**Warning:** It indicates the situations where users need to pay particular attention to, or it might bring serious damage to the system or the switch. Here is an example:



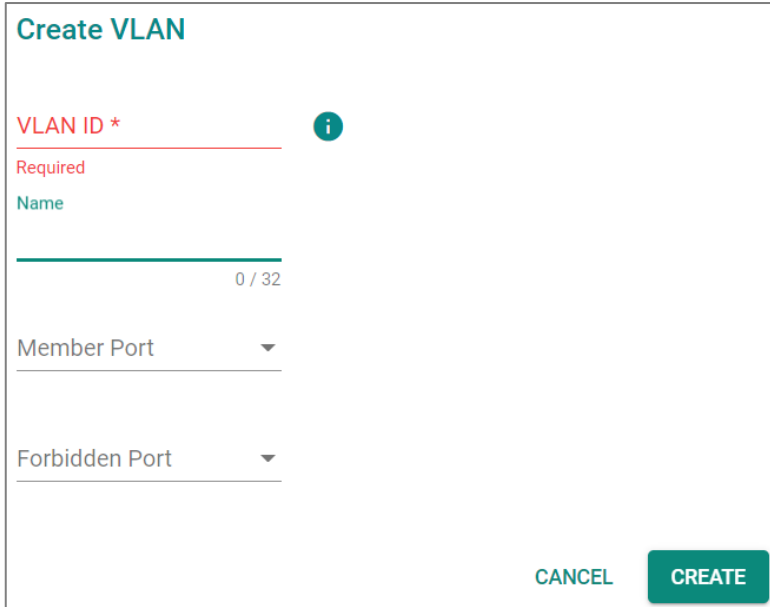
### WARNING

There is a risk of explosion if the battery is replaced by an incorrect type.

# Configuration Reminders

In this section, several examples will be used to remind users when configuring the settings for Moxa's switch.

## A: About Mandatory Parameters

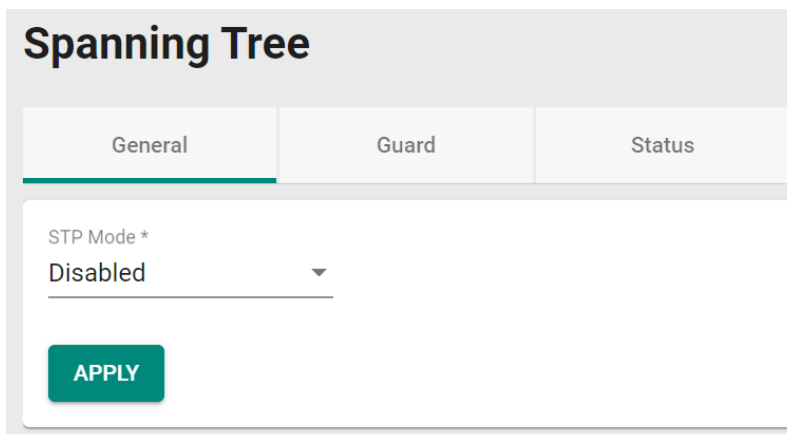


1. The items with asterisks mean they are mandatory parameters that must be provided. In the figure above, the parameters for VLAN, Version, and Query Interval all need to be provided, or it will not be created or applied.
2. If the item is marked with red it means this item has been skipped. You need to fill in the parameters or you cannot apply or create the function.

In addition, some parameter values will be limited to a specific range. If the values exceed the range, it cannot be applied or created.

## B: Configurations before Enable/Disable

In another situation, some settings can be configured first, but remain disabled. Users can decide to enable them when necessary without configuring the same settings again. This is particularly convenient and user-friendly when configuring various settings. For example, in Spanning Tree configuration page, users can configure the Guard settings first, but later select to disable the Guard settings in the General tab. When users decide to enable the Guard settings, they only need to select Enable in General settings, so that the Guard setting can be enabled at the same time.



## 2. Getting Started

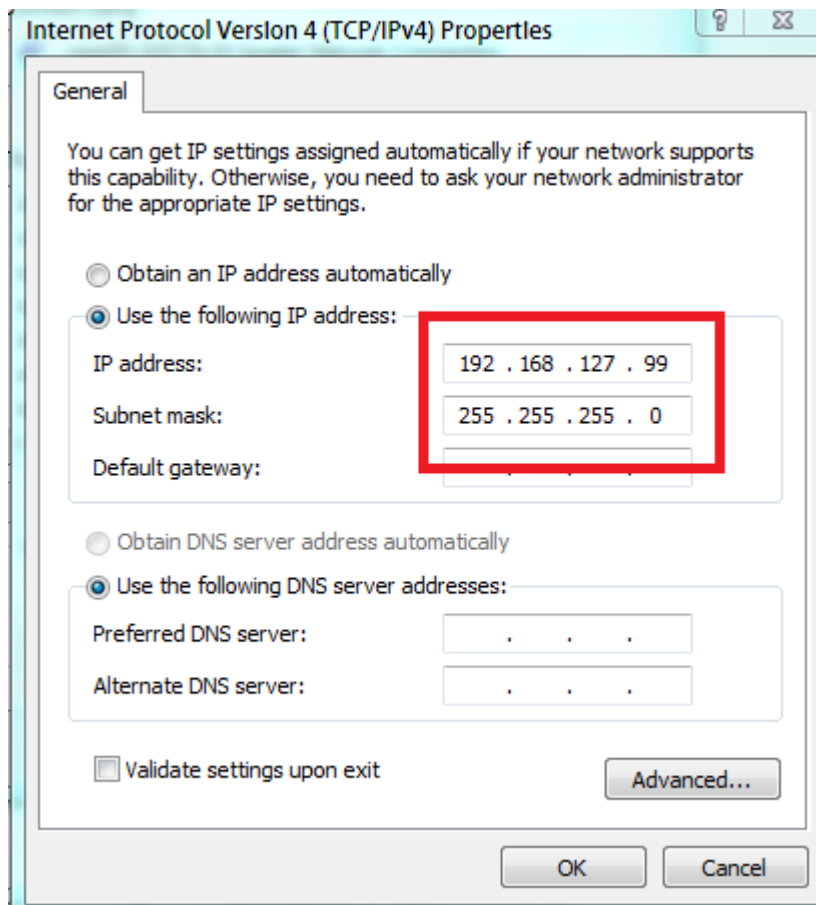
In this chapter, we explain how to log in a Moxa's switch for the first time. There are three ways to access the Moxa switch's configuration settings: RS-232 console, or web-based interface.

### Log in by Web Interface

You can directly connect a Moxa switch to your computer with a standard network cable or install your computer on the same intranet as your switch. You will then need to configure your computer's network settings. The default IP address for a Moxa switch is:

**192.168.127.253**

For example, you can configure the computer's IP setting as **192.168.127.99**, and the subnet mask as 255.255.255.0.



Click **OK** when finished.



#### NOTE

The default IP address for OOBM is:

**192.168.126.253** with default subnet mask is 255.255.255.0.

## Connecting to the Switch

Open a browser, such as Google Chrome, Internet Explorer 11, or Firefox, and connect to the following IP address:

**https://192.168.127.253**



### NOTE

The default IP address for OOBM is:

**192.168.126.253** with default subnet mask is 255.255.255.0.



### NOTE

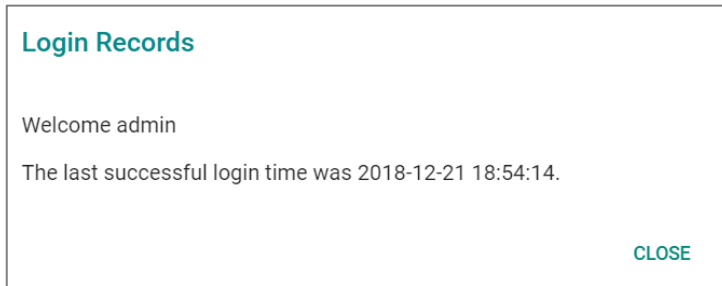
To enhance network security, all HTTP connections will be automatically redirected to HTTPS connections. In addition, when a web browser displays a warning message because a certificate has not been signed by a certification authority, you may add an exception rule for that certificate in the web browser or use a custom certificate to continue. Please go to the following: Security > Device Security > SSH & SSL > SSL

The default username and password are:

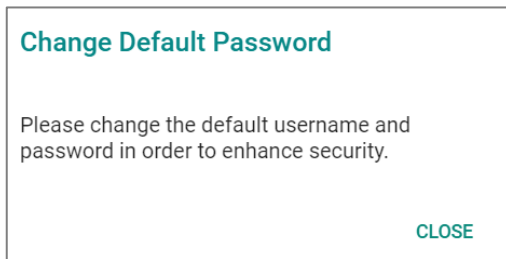
Username: **admin**

Password: **moxa**

Click **LOG IN** to continue. If you have logged in before, you will see a screen indicating the previous login information. Click **CLOSE**.



Another system message will appear, reminding you to change the default password. We recommend that you change your password, or a message will appear whenever you log in telling you to change your password. You can change the password in the **Account Management** section. Click **CLOSE** to continue.



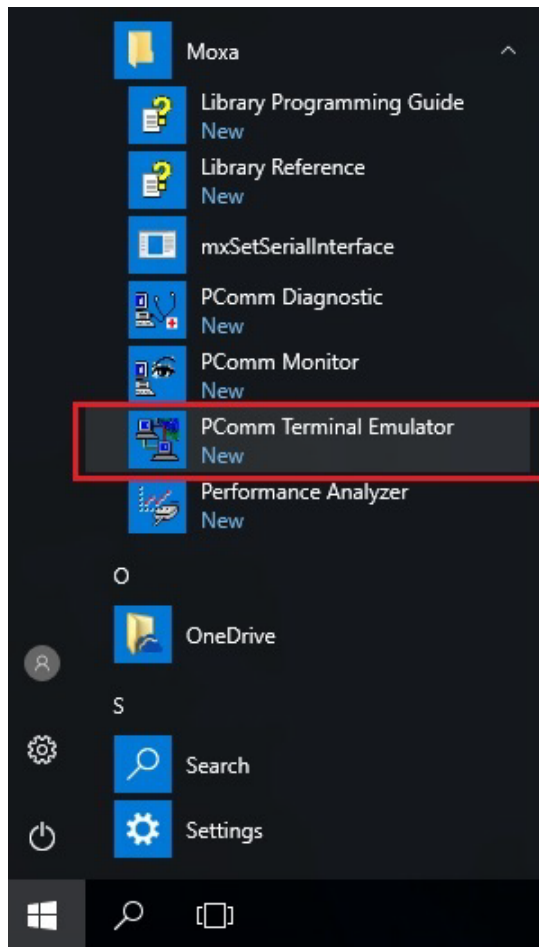
## Log in by RS-232 Console

The Moxa's managed switch offers a serial console port, allowing users to connect to the switch and configure the settings. Do the following steps for the serial connection and configuration.

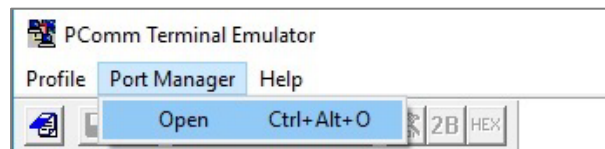
1. Prepare an RS-232 serial cable with an RJ45 interface.
2. Connect the RJ45 interface end to the console port on the switch, and the other end to the computer.
3. We recommend you use **PComm Terminal Emulator** for serial communication. The software can be downloaded free of charge from Moxa's website.

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

4. From the Windows desktop, click **Start → Moxa → PComm Terminal Emulator**.

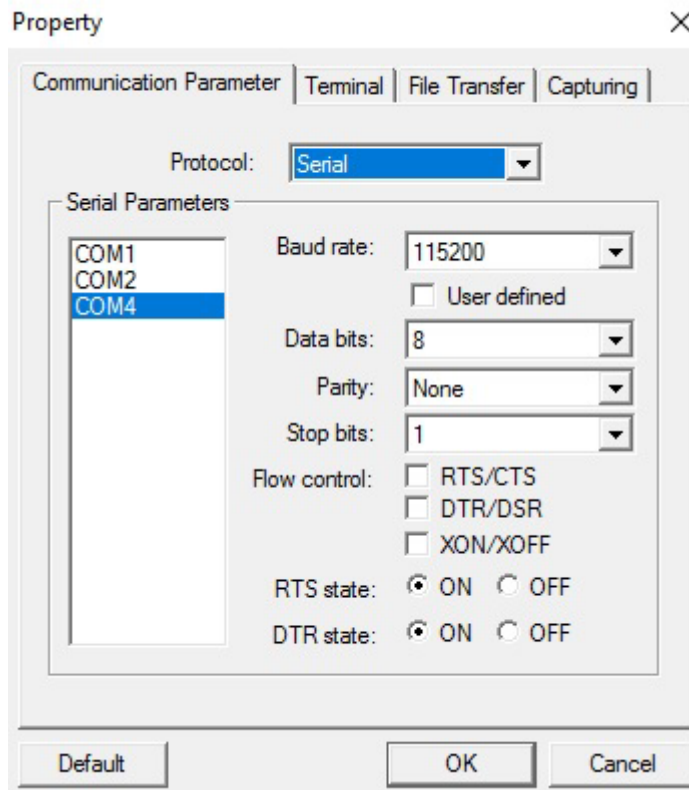


5. Select **Open** under the **Port Manager** menu to open a new connection.

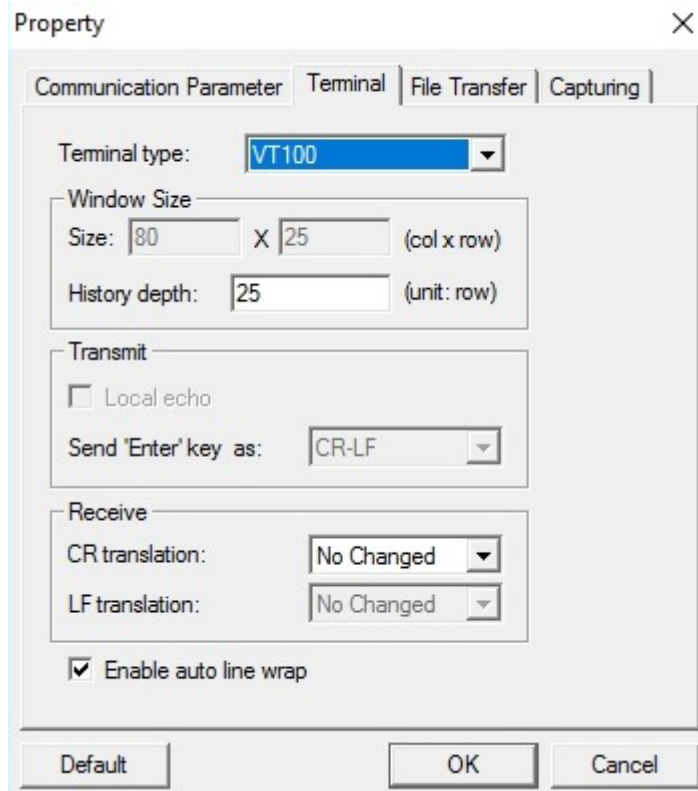




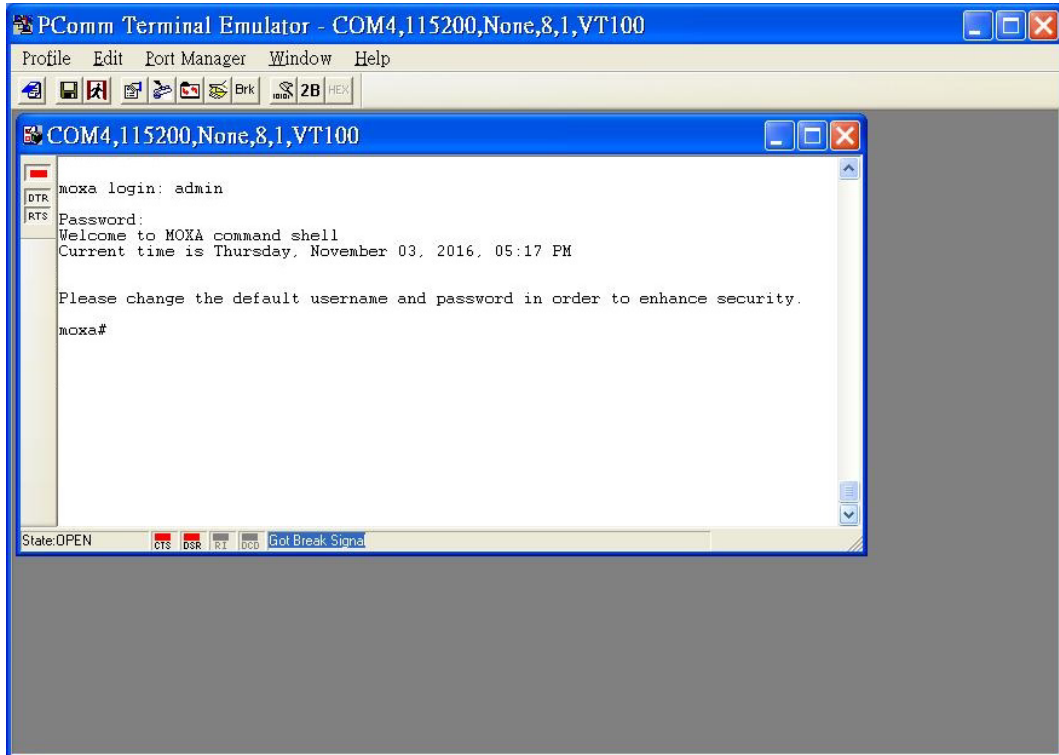
- The **Property** window should open. On the **Communication Parameter** tab for **Ports**, select the COM port that is being used for the console connection. Set the other fields as follows: **115200** for **Baud Rate**, **8** for **Data Bits**, **None** for **Parity**, and **1** for **Stop Bits**.



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



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



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



## 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.

## Log in by Telnet

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 might 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. Your PC's IP address must be set to 192.168.xxx.xxx if the subnet mask is 255.255.0.0, or to 192.168.127.xxx if the subnet mask is 255.255.255.0.



## NOTE

When connecting to the 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 can use either a straight-through or cross-over Ethernet cable.

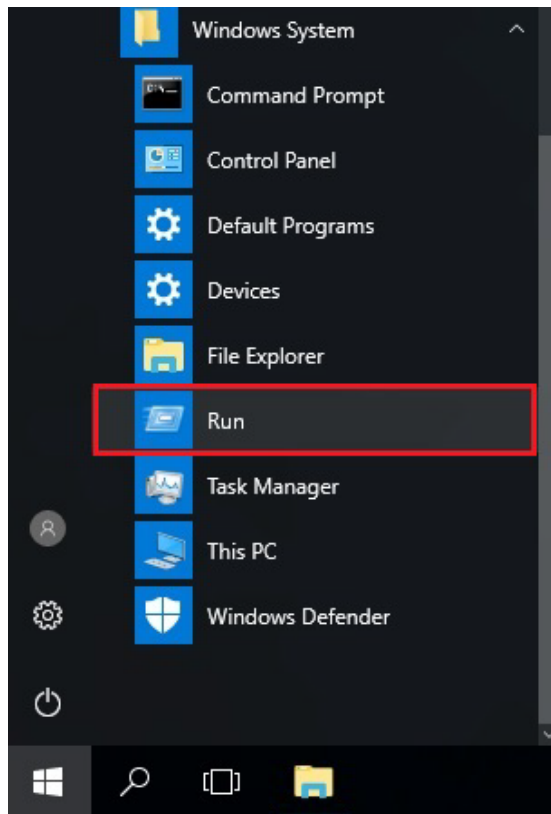


## NOTE

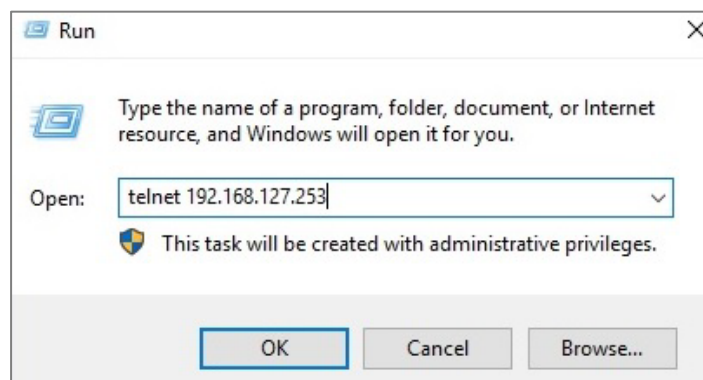
The default IP address for out-of-band management is **192.168.126.253** with default subnet mask of 255.255.255.0.

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:

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



11. Next, use Telnet to connect the Moxa switch's IP address (192.168.127.253) from the Windows **Run** window. You can also issue the Telnet command from a DOS prompt.



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

```
Telnet 192.168.127.253

moxa login: admin
Password:
Welcome to MOXA command shell
Current time is Sunday, April 28, 2019, 05:40 PM

Please change the default username and password in order to enhance security.

moxa#
```

- After successfully connecting to the switch by Telnet, users can start configuring the switch parameters by using command line instructions. Refer to the **Moxa Command Line Interface Manual**.



## NOTE

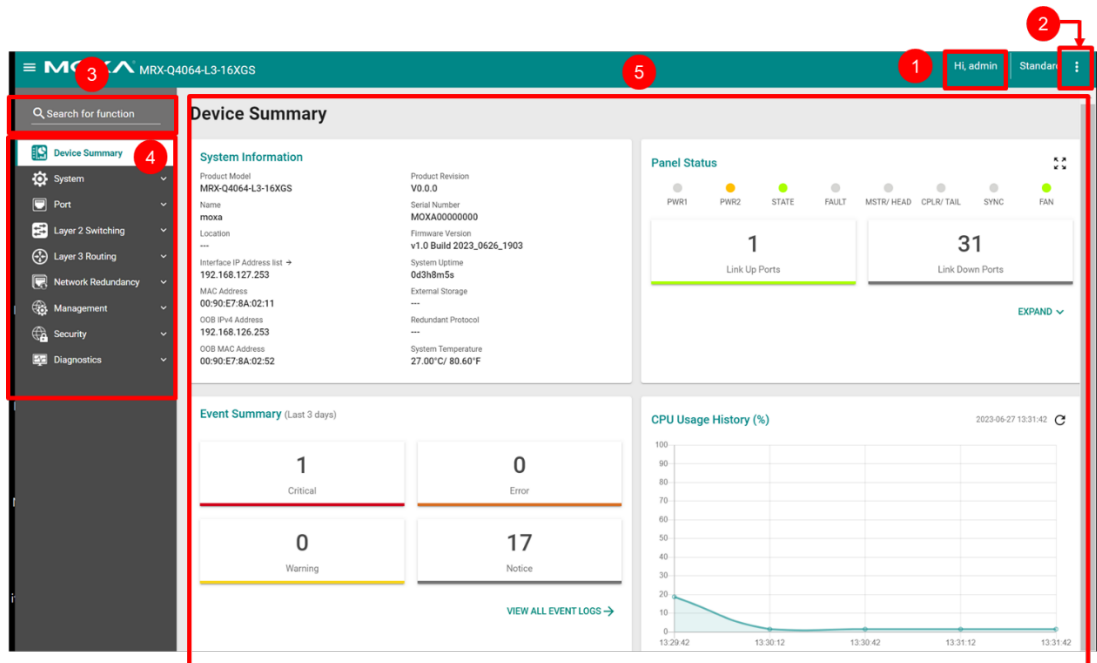
By default, the password assigned to the Moxa switch is moxa. Be sure to change the default password after you first log in to help keep your system secure.

# 3. Web Interface Configuration

Moxa’s managed switch offers a user-friendly web interface for easy configurations. Users find it simple to configure various settings over the web interface. All configurations for the Moxa’s managed switch can be easily set up and done via this web interface, essentially reducing system maintenance and configuration effort.

## Function Introduction

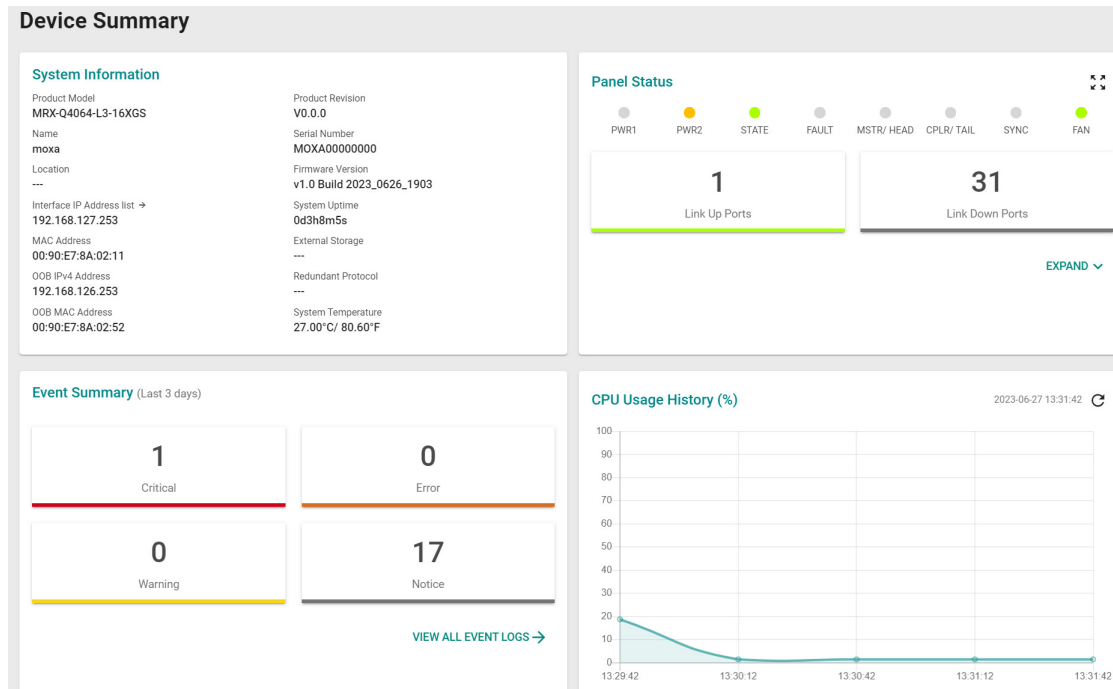
This section describes the web interface design, providing a basic visual concept for users to understand the main information or configuration menu for the web interface pages.



1. **Login Name:** It shows the role of the login name.
2. **Configuration Mode:** Two modes can be shown: **Standard Mode** and **Advanced Mode**.
  - **Standard Mode:** Some of the features and parameters will be hidden to make the configurations simpler (default).
  - **Advanced Mode:** More features and parameters will be shown for users to configure detailed settings.
3. **Search Bar:** Type the items you want to search of the function menu tree.
4. **Function Menu:** All functions of the switch are shown here. Click the function you want to view or configure.
5. **Device Summary:** All important device information of the functions will be shown here.

# Device Summary

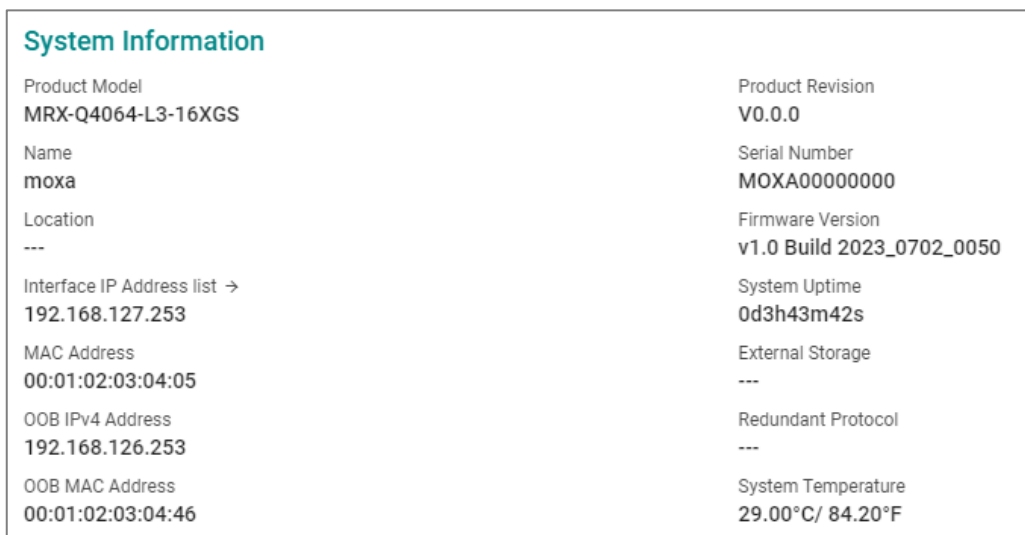
After successfully connecting to the switch, the **Device Summary** will automatically appear. You can view the whole web interface on the screen. If you are in the middle of performing configurations, simply click **Device Summary** on the Function Menu and you can view the detailed information of the switch.



See the following sections for detailed descriptions for the specific items.

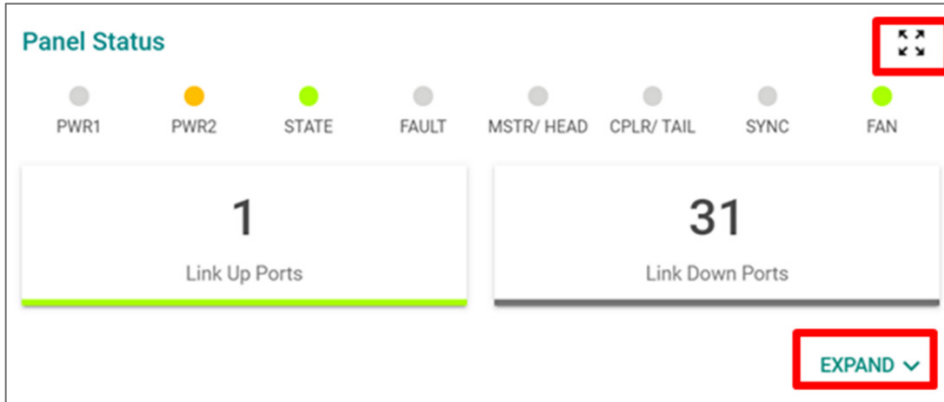
## Model Information

This shows the model information, including product model name, serial number, firmware version, system uptime, etc.

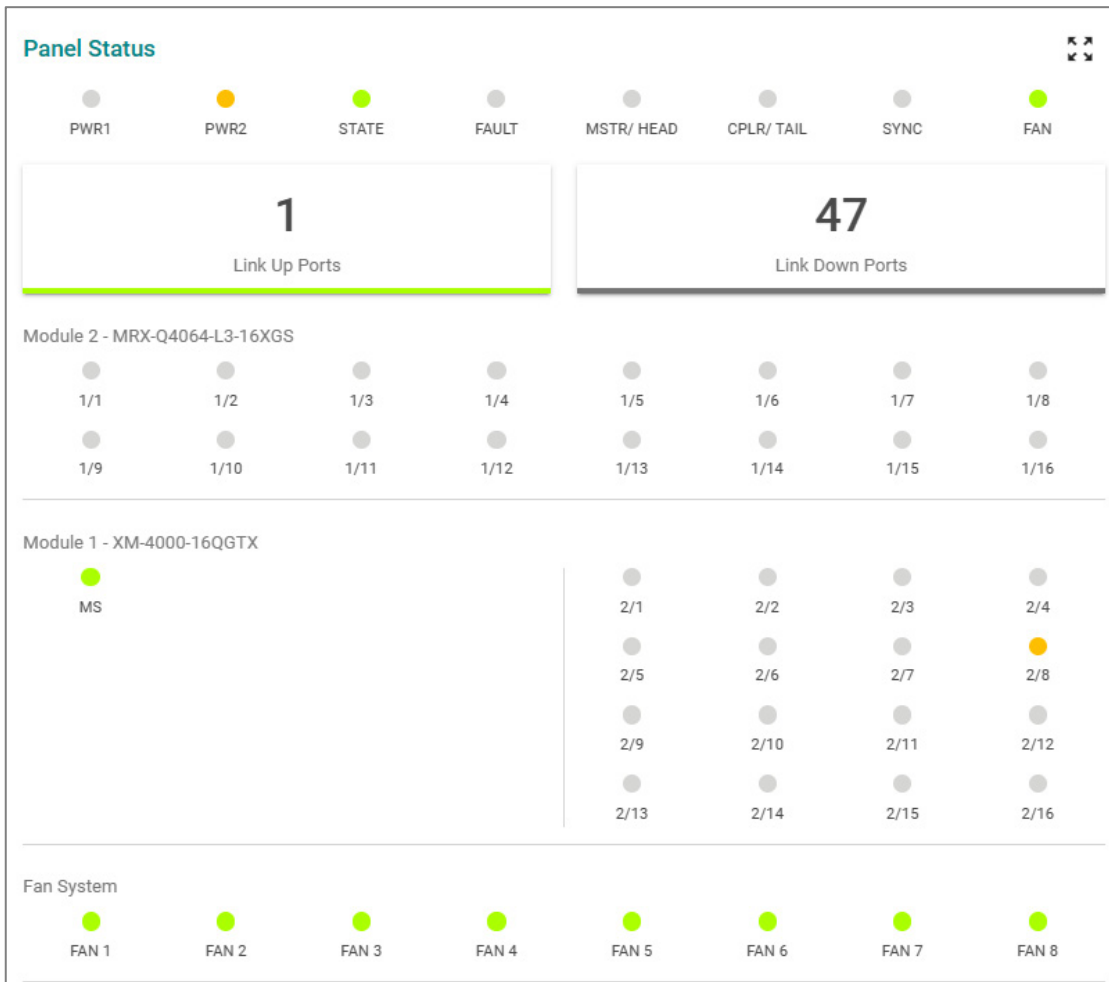


# Panel Status



This section illustrates the panel status. For example, the connecting ports will be shown in green, while the disconnected ports will be shown in gray. Click **Expand** to view more detailed information on the panel status and click **Collapse** to return.



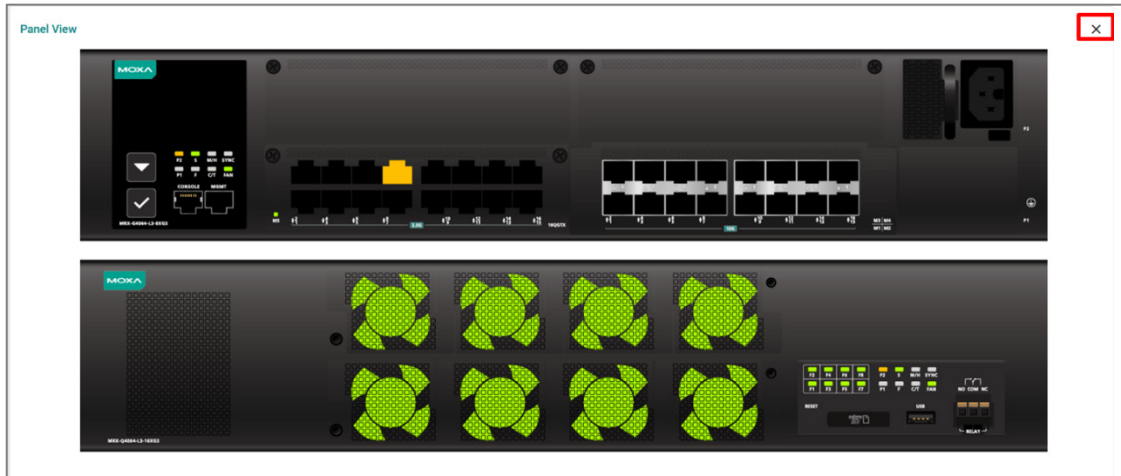
Click **Expand** to view more detailed information on the panel status and click **Collapse** to return.



## Panel View

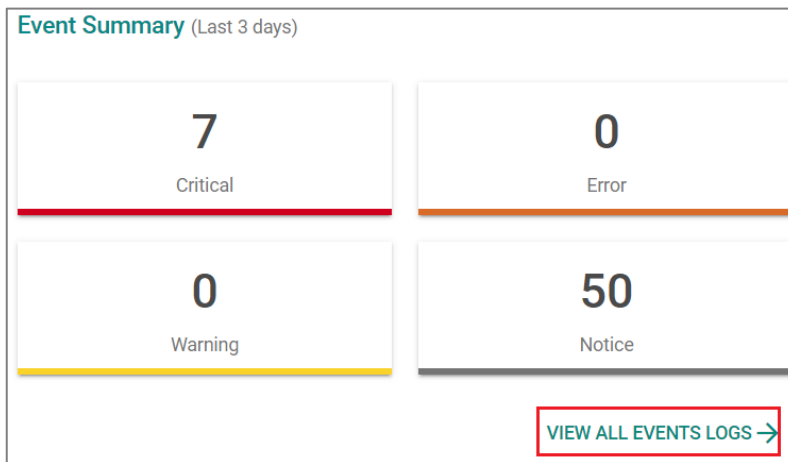
By clicking this icon, , users can view the device port status by a graphic figure. Click the  icon on the upper right corner to return to the main page.

This panel view figure might vary, depending on the different modules that you purchase.



## Event Summary (Last 3 Days)

This section shows the event summary for the past three days.





Click **VIEW ALL EVENT LOGS** to go to the Event Log page, where you can view all event logs.

### Event Log

Event Log    Oversize-Action    Backup

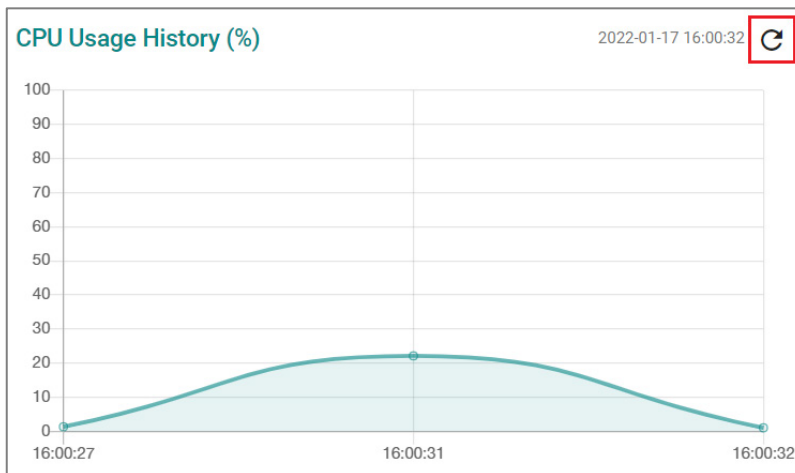
🔄 🗑️ 📄 🔍 Search

Index	Bootup Number	Severity	Timestamp	Uptime	Message
1	12	Notice	2018-12-21 19:15:18	0d0h21m52s	[Account:admin] successfully logged in via local.
2	12	Notice	2018-12-21 18:59:25	0d0h5m59s	[Account:admin] logged out.
3	12	Notice	2018-12-21 18:59:06	0d0h5m40s	[Account:system] logged out.
4	12	Critical	2018-12-21 18:54:16	0d0h0m50s	System has performed a cold start.
5	12	Notice	2018-12-21 18:54:14	0d0h0m48s	[Account:admin] successfully logged in via local.
6	12	Notice	2018-12-21 18:53:59	0d0h0m33s	Interface vlan1 up.
7	12	Notice	2018-12-21 18:53:59	0d0h0m33s	Port 2/1 link up.
8	11	Notice	2018-12-21 19:18:52	0d0h25m27s	[Account:admin] logged out.

For Event Log settings, refer to **Event Log** under the **Diagnosis** section.

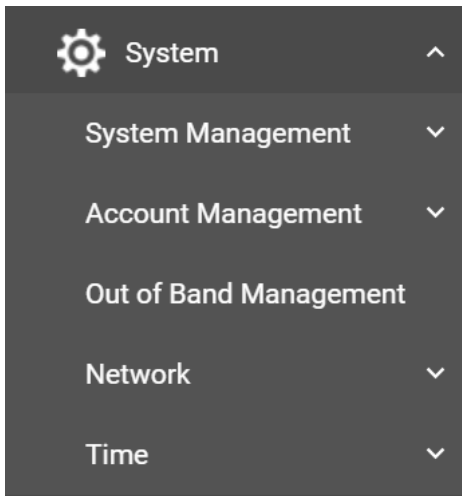
## CPU Utilization History

This section shows the CPU usage. The data will be shown as a percentage over time. Click the 🔄 icon on the page to show the latest information.



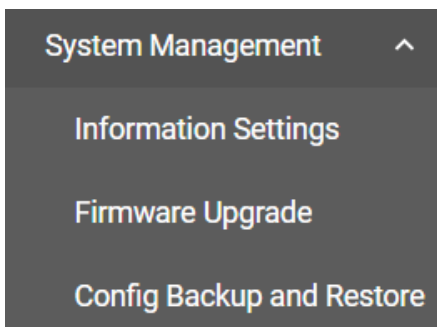
# System

Click **System** on the function menu to manage with **System Management, Account Management, Network, Out of Band Management,** and **Time** controls.



## System Management

Click **System Management**, four functions can be configured under this section: **Information Setting, Firmware Upgrade,** and **Configure Backup and Restore.**



## Information Setting

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

### Information Settings

Device Name \*

moxa

---

4 / 64

Location

---

0 / 255

Description

---

0 / 255

Contact Information

---

0 / 255

**APPLY**

### Device Name

Setting	Description	Factory Default
1 to 64 characters	This option is useful for differentiating between the roles or applications of different units. Note that the device name cannot be empty.	moxa



### NOTE

The Device Name field follows the PROFINET I/O naming rule. The name can only include the following characters, **a-z/0-9/-**. The prefix cannot start from port-x where x=0~9.

### Location

Setting	Description	Factory Default
Max. 255 characters	This option is for differentiating between the locations of different switches. Example: production line 1.	None

### Description

Setting	Description	Factory Default
Max. 255 characters	This option is for recording a more detailed description of the unit.	None

### Contact Information

Setting	Description	Factory Default
Max. 255 characters	Users can input contact information such as email address, or telephone number when problems occur.	None

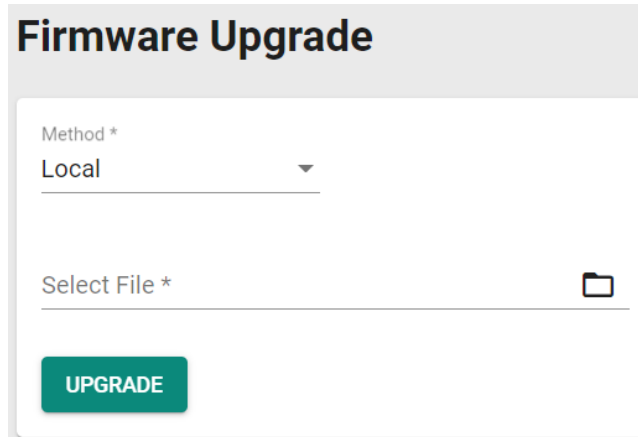
When finished, click **APPLY** to save your changes.

## Firmware Upgrade

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

### Local

Select **Local** from the drop-down list under **Method**.



**Firmware Upgrade**

Method \*  
Local

Select File \*

UPGRADE

#### Select File

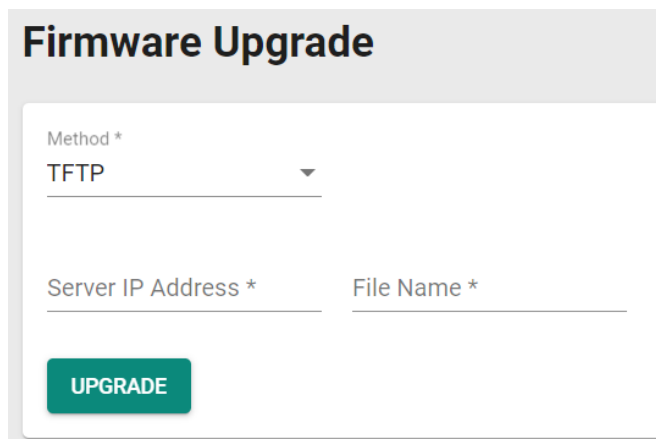
Before performing firmware upgrade, download the updated firmware (\*.rom) file first from Moxa's website ([www.moxa.com](http://www.moxa.com)).

Setting	Description	Factory Default
Select the firmware file	Select the firmware file from the location where the updated firmware is located.	None
Browse for the (*.rom) file	This option allows users to select the updated firmware file and perform the firmware upgrade.	None

When finished, click **UPGRADE** to perform the firmware upgrade.

### TFTP Server

Click **TFTP** from the drop-down list under **Method**.



**Firmware Upgrade**

Method \*  
TFTP

Server IP Address \*      File Name \*

UPGRADE

#### Server IP Address

Setting	Description	Factory Default
Input the IP address of the TFTP server	Input the IP address of the TFTP server where the new firmware file (*.rom) is located.	None

### File Name

Setting	Description	Factory Default
Input the file name of the firmware	Input the file name of the new firmware.	None

When finished, click **UPGRADE** to perform the firmware upgrade.


## SFTP

Select **SFTP** from the drop-down list under **Method**.

### Firmware Upgrade

Method \*  
SFTP

Server IP Address \*      File Name \*

Account \*      Password \* 

**UPGRADE**

### Server IP Address

Setting	Description	Factory Default
Input the IP address of the SFTP server.	Input the server IP address of the computer where the new firmware file (*.rom) is located.	None

### File Name

Setting	Description	Factory Default
Input the file name of the firmware	Input the file name of the new firmware.	None

### Account

Setting	Description	Factory Default
Input the account of the SFTP server	The account must be authorized in order for the SFTP Server to have a secure connection.	None

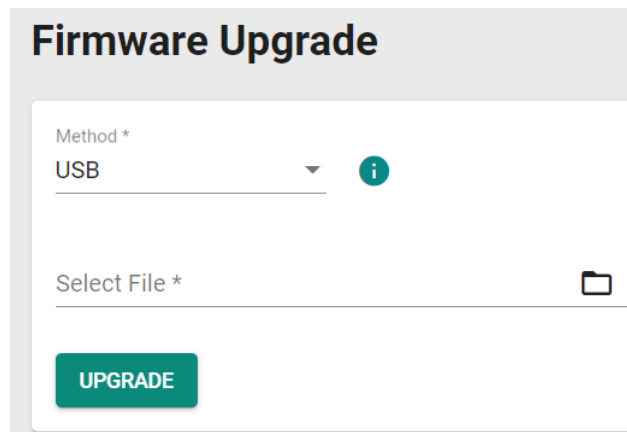
### Password

Setting	Description	Factory Default
Input the password for the SFTP server	The account has to be specified in order to authorize the SFTP Server for secure connection.	None

When finished, click **UPGRADE** to perform the firmware upgrade. The switch will reboot automatically and perform the firmware upgrade.

## USB

You can upgrade the firmware via Moxa's USB-based ABC-02 configuration tool. Connect the ABC-02 to the switch and select **USB** from the drop-down list under **Method**.



**Firmware Upgrade**

Method \*  
USB

Select File \*

**UPGRADE**

### Select File

Before performing the firmware upgrade, download the latest firmware (\*.rom) file first from Moxa's website ([www.moxa.com](http://www.moxa.com)).

Setting	Description	Factory Default
Select the firmware file	Select the firmware file from the location where the updated firmware is located.	None
Browse for the (*.rom) file	This option allows users to select the updated firmware file and perform the firmware upgrade.	None

When finished, click **UPGRADE** to perform the firmware upgrade.



### Note

If you have difficulty using the ABC-02 configuration tool, check if the **USB Function** has been enabled in the **Hardware Interfaces** section.

# Configuration Backup and Restore

## Backup

Click the **Backup** tab first.

**Configuration Backup and Restore**

Backup | Restore | File Encryption | File Signature

Method \*  
Local

Configuration Selection \*  
Running Configuration

Default Configuration \*  
Not Included

**BACKUP**

There are four ways to back up the configurations of your Moxa switch: from a local configuration file, by remote SFTP server, by remote TFTP server, or by a USB tool.

### Local

Select **Local** from the drop-down list under **Method**. Configure the following settings.

#### Configuration Selection

Setting	Description	Factory Default
Running Configuration	Back up the running configuration.	Running
Startup Configuration	Back up the start-up configuration.	Configuration

#### Default Configuration

Setting	Description	Factory Default
Not Included	Back up the configuration without default settings.	Not Included
Included	Back up the configuration with default settings.	

### TFTP Server

Select **TFTP** from the drop-down list under **Method**.

**Configuration Backup and Restore**

Backup | Restore | File Encryption | File Signature

Method  
TFTP

Server IP Address \*    File Name \*

**BACKUP**

#### Server IP Address

Setting	Description	Factory Default
Input the IP address of the TFTP server	Users can input the IP address of the TFTP server.	None

### File Name

Setting	Description	Factory Default
Input the backup file name (supports up to 54 characters, including the .ini file extension).	Users can input the file name to back up the system configuration file.	None

When finished, click **BACKUP** to back up the system configuration file.

### SFTP Server


Select **SFTP** from the drop-down list under **Method**.

### Configuration Backup and Restore

Backup    Restore    File Encryption    File Signature

Method  
SFTP

Server IP Address \*    File Name \*

Account \*    Password \* 

**BACKUP**

### Server IP Address

Setting	Description	Factory Default
Input the IP address of the SFTP server	Input the IP address of the SFTP server where the new firmware file (*.rom) is located.	None

### File Name

Setting	Description	Factory Default
Input the backup file name (support up to 54 characters, including the .ini file extension).	Input the file name of the configuration backup file.	None

### Account

Setting	Description	Factory Default
Input the account of the SFTP server	An account must be provided to authorize the SFTP server for secure connection.	None

### Password

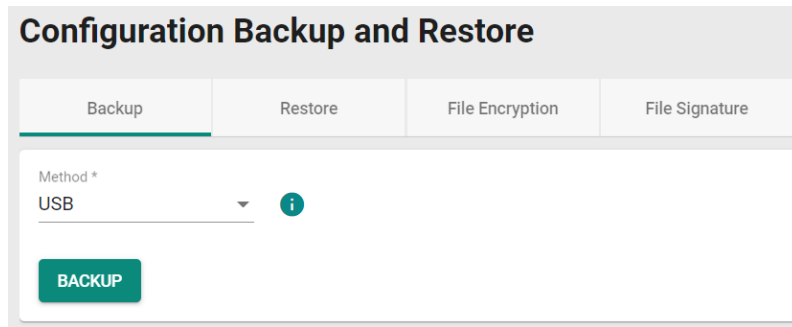
Setting	Description	Factory Default
Input the passwords for the SFTP server	The password has to be specified in order to authorize the SFTP Server for secure connection.	None

When finished, click **BACKUP** to back up the system configuration file.



## USB

Select **USB** from the drop-down list under **Method**.



The screenshot shows the 'Configuration Backup and Restore' interface. At the top, there are four tabs: 'Backup', 'Restore', 'File Encryption', and 'File Signature'. The 'Backup' tab is currently selected. Below the tabs, there is a 'Method \*' dropdown menu with 'USB' selected. To the right of the dropdown is an information icon (i). Below the dropdown is a green 'BACKUP' button.

Insert Moxa's ABC-02 USB-based configuration tool into the USB port of the switch, click **BACKUP** to back up the system configuration file.

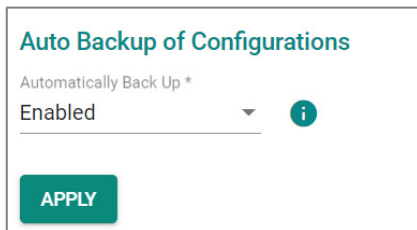


### Note

If you have difficulty using the ABC-02 configuration tool, check if the **USB Function** has been enabled in the **Hardware Interfaces** section.

## Automatic Backup of Configurations

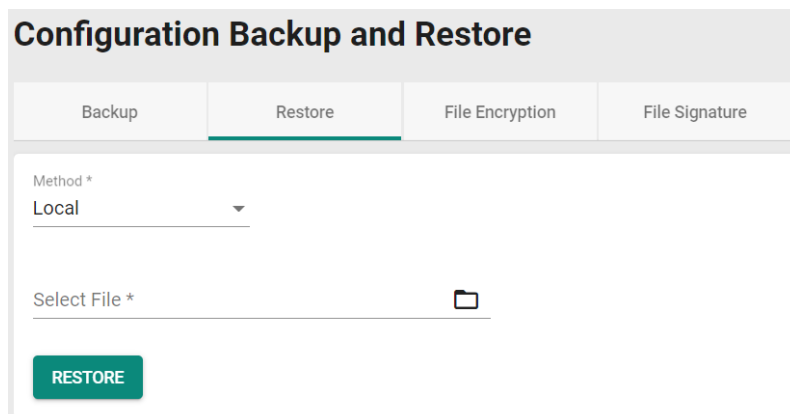
To enable automatic backup, select **Enabled** from the drop-down list. Click **APPLY** to back up the system configuration file automatically.



The screenshot shows the 'Auto Backup of Configurations' interface. It has a title 'Auto Backup of Configurations' and a subtitle 'Automatically Back Up \*'. Below the subtitle is a dropdown menu with 'Enabled' selected. To the right of the dropdown is an information icon (i). Below the dropdown is a green 'APPLY' button.

## Restore

First, click the **Restore** tab.



The screenshot shows the 'Configuration Backup and Restore' interface. At the top, there are four tabs: 'Backup', 'Restore', 'File Encryption', and 'File Signature'. The 'Restore' tab is currently selected. Below the tabs, there is a 'Method \*' dropdown menu with 'Local' selected. Below the dropdown is a 'Select File \*' field with a folder icon. Below the field is a green 'RESTORE' button.

There are four ways to restore the configurations of your Moxa switch: from a local configuration file, by remote SFTP server, by remote TFTP server, or by a USB tool.

## Local

Select **Local** from the drop-down list under **Method**.

### Select File

Setting	Description	Factory Default
Browse for a configuration file on a local disk	Select the configuration file and perform system restoration.	None

When finished, click **RESTORE** to restore the system configuration file.

## TFTP Server

Select **TFTP** from the drop-down list under **Method**.

### Configuration Backup and Restore

Backup   **Restore**   File Encryption   File Signature

Method \*  
TFTP

Server IP Address \*   File Name \*

**RESTORE**

### Server IP Address

Setting	Description	Factory Default
Input the IP address of the TFTP server	Users can input the IP address of the TFTP server.	None

### File Name

Setting	Description	Factory Default
Input the restore file name (supports up to 54 characters, including the .ini file extension).	Users can input the file name to restore the system configuration file.	None

When finished, click **RESTORE** to restore the system configuration file.

## SFTP Server


Select **SFTP** from the drop-down list under **Method**.

### Configuration Backup and Restore

Backup   **Restore**   File Encryption   File Signature

Method  
SFTP

Server IP Address \*   File Name \*

Account \*   Password \* 

**RESTORE**

### Server IP Address

Setting	Description	Factory Default
Input the IP address of the SFTP server	Input the IP address of the SFTP server where the new firmware file (*.rom) is located.	None

### File Name

Setting	Description	Factory Default
Input the restore file name (supports up to 54 characters, including the .ini file extension).	Input the file name of the configuration restoration file.	None

### Account

Setting	Description	Factory Default
Input the account of the SFTP server	An account must be provided to authorize the SFTP server for secure connection.	None

### Password

Setting	Description	Factory Default
Input the passwords for the SFTP server	The password has to be specified in order to authorize the SFTP Server for secure connection.	None

When finished, click **RESTORE** to restore the system configuration file.

## USB

Select **USB** from the drop-down list under **Method**.

The screenshot shows the 'Configuration Backup and Restore' interface. At the top, there are four tabs: 'Backup', 'Restore', 'File Encryption', and 'File Signature'. The 'Restore' tab is currently selected. Below the tabs, there is a 'Method \*' dropdown menu with 'USB' selected. To the right of the dropdown is an information icon. Below the dropdown is a 'Select File \*' field with a folder icon. At the bottom left, there is a green 'RESTORE' button.

Insert Moxa's ABC-02 USB-based configuration tool into the USB port of the switch, click **RESTORE** to restore the system configuration file.

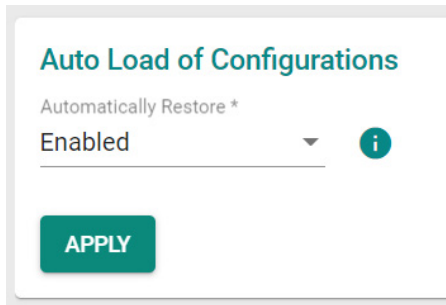


## Note

If you have difficulty using ABC-02 tool, check if **USB Function** has been enabled in **Hardware Interfaces** section.

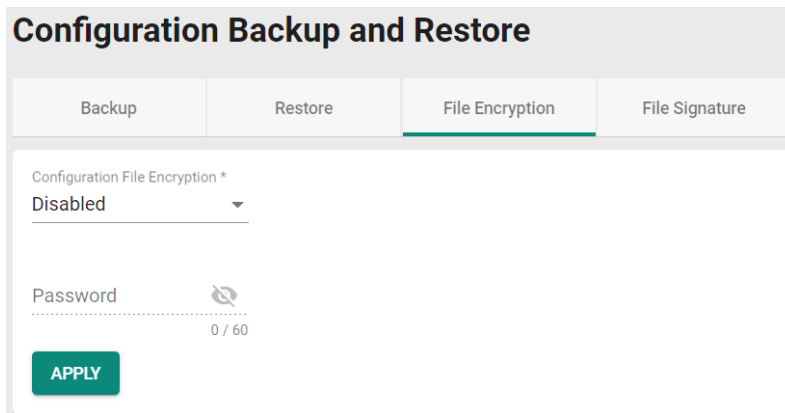
## Auto Load of Configurations

To enable automatic configuration restore, select **Enabled** from the drop-down list. Click **APPLY** to restore the system configuration file automatically.



## File Encryption

To encrypt the configuration file, click the **File Encryption** tab first.



### Configuration File Encryption

Setting	Description	Factory Default
Enabled	Enable the configuration file to be encrypted.	Disabled
Disabled	Disable the feature that allows the configuration file to be encrypted.	

### Password

Setting	Description	Factory Default
4 to 16 characters, numbers only.	Input the password when users encrypt the configuration file.	None

When finished, click **APPLY** to save your changes.

## File Signature

Click **File Signature** tab to see additional configuration options. Enabling the file signature can ensure file integrity and authenticity.

### Configuration Backup and Restore

Backup
Restore
File Encryption
File Signature

Signed config \*  
 Disabled i

APPLY

+

Key	Label	Algorithm	Length

Max. 1

### Enable Signed Configuration

Setting	Description	Factory Default
Enabled	Enable configuration file signature.	Disabled
Disabled	Disable configuration file signature	

Click **APPLY** to save your changes.

Click the + icon to add customer key.

### Add Custom Key

Label \* 0 / 16

Certificate \* 📁

Key \* 📁

CANCEL
CREATE

### Label

Setting	Description	Factory Default
0 to 16 characters	Provide the name for the certificate and the key.	None

### Certificate

Setting	Description	Factory Default
Click the <span style="color: #008080; font-size: 1.2em;">📁</span> icon to select the file from your computer	Import the certificate file.	None

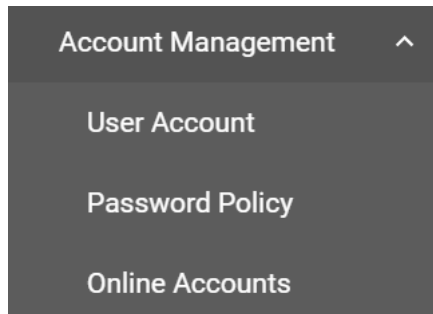
### Key

Setting	Description	Factory Default
Click the  icon to select the file from your computer	Import the key file.	None

When finished, click **CREATE** to save your changes.

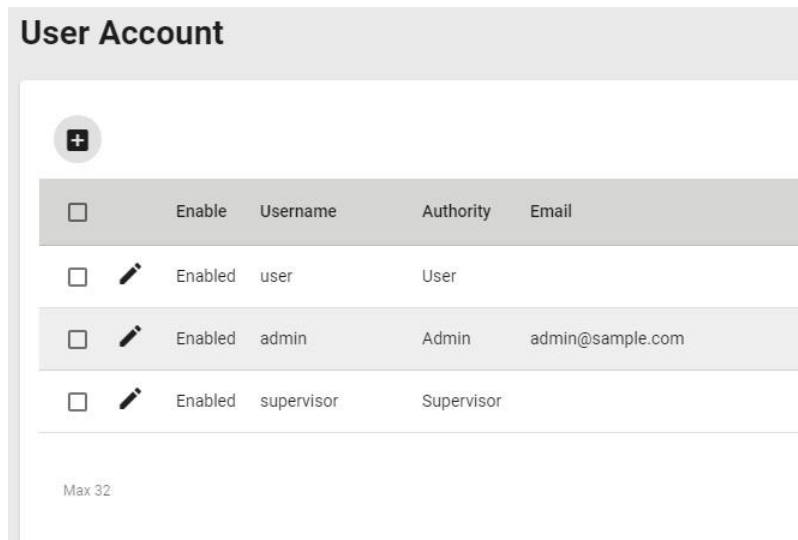
## Account Management

The Account Management feature allows users to manage the accounts of the switch. You can enable different accounts with different roles to facilitate convenient management and safe access.




### User Account

This section describes how to manage the existing accounts of the switch. Here, you can add, edit, and delete user accounts for the switch. By default, there is only one account: admin. In order to enhance security, we suggest you create a new account with the user authority.







There is a search function on the upper right of the User Account page. Type the username you want to search for.

## Editing Existing Accounts

Select the account you want to edit and click the  icon.

### User Account



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

Max 32

Configure the following settings.

### Edit Account Settings

Enable \*  
Enabled ▼

Username  
test CHANGE PASSWORD

At least 4 characters 4 / 32

Authority \*  
User ▼

Email  
0 / 63

CANCEL
APPLY

### **Enabled**

Setting	Description	Factory Default
Enabled	This enables the user account.	Enabled
Disabled	This disables the user account.	

To change the password, click **CHANGE PASSWORD**.

### Edit Account Password

Username  
test  
At least 4 characters 4 / 32

New Password \*   
At least 4 characters 0 / 63

Confirm Password \*   
At least 4 characters 0 / 63

BACK
APPLY

#### ***New Password***

Setting	Description	Factory Default
0 to 63 characters	Enter the password to use for this account.	None

#### ***Confirm Password***

Setting	Description	Factory Default
0 to 63 characters	Reenter the password to confirm it.	None

Click **APPLY** to finish changing the password.

#### ***Authority***

Setting	Description	Factory Default
admin	This account has read/write access for all configuration parameters.	admin
supervisor	This account has read/write access for some specific configuration parameters.	
user	This account can only view some specific configuration parameters.	

#### ***Email***

Setting	Description	Factory Default
Input an email address	Input an email address for the account if required.	None

When finished, click **APPLY** to save your changes.




### **NOTE**


Refer to Appendix A for detailed descriptions for read/write access privileges for the admin, supervisor, and user authority levels.



## Creating a New Account

You can create new account by clicking the  icon on the configuration page.

### User Account



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

Max 32

Configure the following settings.

### Create New Account



Enable \*  
Enabled ▼

---

Username \*  
At least 4 characters 0 / 32

Authority \* ▼

---

New Password \*  Confirm Password \*   
 At least 4 characters 0 / 63 At least 4 characters 0 / 63

Email 0 / 63

CANCEL
CREATE

#### **Enabled**

Setting	Description	Factory Default
Enabled	This enables the account.	Enabled
Disabled	This disables the account.	

#### **Username**

Setting	Description	Factory Default
Input a username, 4 to 32 characters	Input a new username for this account.	None

### Authority

Setting	Description	Factory Default
admin	This account has read/write access of all configuration parameters.	None
supervisor	This account has read/write access for some specific configuration parameters.	
user	This account can only view some specific configuration parameters.	

In order to enhance security, we suggest you create a new account with the user authority.

### New Password

Setting	Description	Factory Default
0 to 63 characters	Input a new password for this account.	None

### Confirm Password


Setting	Description	Factory Default
0 to 63 characters	Reenter the password to confirm.	None

### Email


Setting	Description	Factory Default
Input an email address	Input an email address for the account if required.	None





When finished, click **CREATE** to complete.

## Delete an Existing Account

To delete the existing account, simply select the account you want to delete, and then click the  on the configuration page.

### User Account



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

Click **DELETE** to delete the account.

### Delete Account

Are you sure you want to delete the selected account?

[CANCEL](#) [DELETE](#)

## Password Policy

In order to prevent hackers from cracking weak passwords, a password policy can be set. The password policy can force users to create passwords with a minimum length and complexity, and can also set a maximum lifetime for the password to ensure it is changed periodically.

### Password Policy

Minimum Length \*

4

4 - 63

**Password Complexity Strength Check**

At least one digit (0-9)

At least one upper case letter (A-Z)

At least one lower case letter (a-z)

At least one special character ({}|~!@#\$%^&\*-\_.)

Password Max-life-time \*

0

0 - 365 day

**APPLY**

### Minimum Length

Setting	Description	Factory Default
Input from 4 to 63	This sets the minimum length of the password.	4

### Password Complexity Strength Check

Setting	Description	Factory Default
digit, letter cases, special characters	These determine the required complexity for the password. Multiple options may be checked.	None

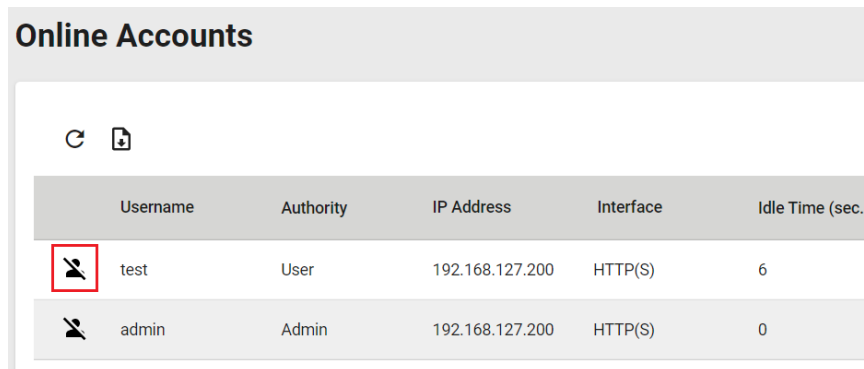
### Password Max-life-time (day)



Setting	Description	Factory Default
Input from 0 to 365	This determines how long the password can be used before it must be changed.	0

When finished, click **APPLY** to save your changes.

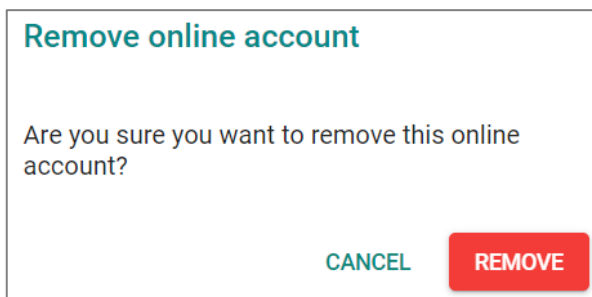
## Online Accounts

The **Online Accounts** function allows users to view who has connected to the device. You may immediately remove the user who is currently online.



Username	Authority	IP Address	Interface	Idle Time (sec.)
 test	User	192.168.127.200	HTTP(S)	6
 admin	Admin	192.168.127.200	HTTP(S)	0

Select the  icon and select **REMOVE** to disconnect the user.



## Out of band management

### Out of band management (OOBM) Overview

The Moxa managed switch offers an out-of-band port for user access to device management, even during high in-band traffic loads.

The default IP address for OOBM is **192.168.126.253** with a default subnet mask of 255.255.255.0

User can access the device for management via SSH, Telnet, HTTP, HTTPS, SNMP v1/v2c/v3.

### How out of band management works

Moxa managed switches offer multiple ways to connect for remotely management and configuration: in-band network interfaces or out-of-band network interfaces.

#### In Band

In-band management utilizes line module ports for network communication, potentially impacting transmitting traffic or user data. During network downtime or congestion, users may be unable to connect to the device.

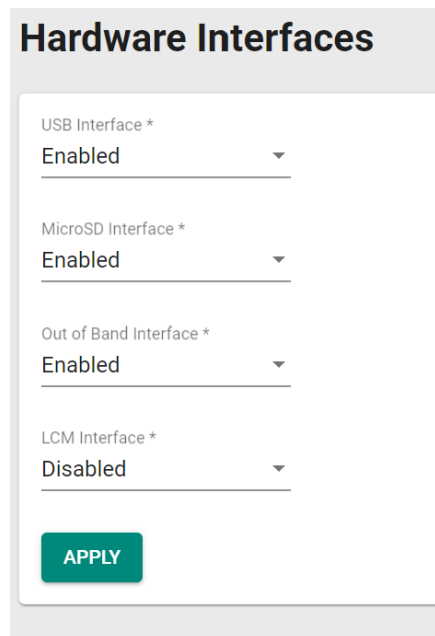
#### Out of Band

Out-of-band management (OOBM) utilizes dedicated ports to manage the switch independently of in-band traffic or network congestion. Unlike USB and serial console management, OOBM can be accessed using a standard RJ45 connector without requiring additional cable types, facilitating access even during network downtime. This feature separates the management and user data planes, preventing traffic forwarding between in-band and out-of-band interfaces.

## OOBM Settings and Status

This section describes how to configure Out-of-Band management.

Enable/disable out of band interfaces from **Hardware Interfaces**. **Out of Band Interface** is **Enabled** by default.



**Hardware Interfaces**

USB Interface \*  
Enabled

MicroSD Interface \*  
Enabled

Out of Band Interface \*  
Enabled

LCM Interface \*  
Disabled

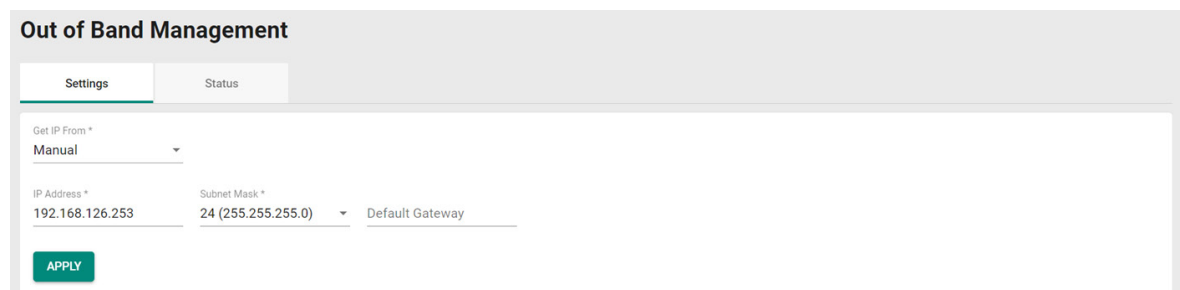
APPLY

Click **Out of Band Management** on the menu.

## Settings

Click the Settings to configure OOBM IP. Choose **Manual** or from **DHCP** IP assignment.

Click **Apply** when you are done.



**Out of Band Management**

Settings    Status

Get IP From \*  
Manual

IP Address \*    Subnet Mask \*    Default Gateway  
192.168.126.253    24 (255.255.255.0)   

APPLY

### Get IP From

Setting	Description	Factory Default
Manual	Specify the OOBM IP manually.	Manual
DHCP	Specify the OOBM IP by DHCP.	

### IP address

Setting	Description	Factory Default
Input IP address	Specify the IP address for OOBM access	192.168.126.253

### Netmask

Setting	Description	Factory Default
Select the subnet mask from the drop-down list	Select the subnet mask from the list.	None

### Default Gateway

Setting	Description	Factory Default
Input default gateway address	Specify the default gateway for OOBM interface.	None

When finished, click **APPLY** to continue.



### NOTE

The OOBM interface IP address and netmask must be different from the in-band interface.

## Status

Click the **Status** tab to view the detailed status of OOBM interface information.

Admin Status	Link Status	Flow Control	MDI/MDIX
Enabled	1G, Full (Auto)	Disabled	MDI

## Time

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

- System Time
- NTP Server
- Time Synchronization



### NOTE

The user must update the Current Time and Current Date after the switch has been powered off for an extended period of time (e.g., three days). The user must pay particular attention to this when there is no NTP server or Internet connection available.

# System Time

The section describes how to configure the system time.

## Time

Click the **Time** tab.

**System Time**

Time      Time Zone      NTP Authentication

Current Time  
2018-12-21 20:45:04 UTC+00:00

Clock Source \*  
Local

Date \*  
2018-12-21

Time \*  
08:45 PM

APPLY      SYNC FROM BROWSER

### Current Time

Setting	Description	Factory Default
None	This automatically shows the current time according to your default settings.	Local

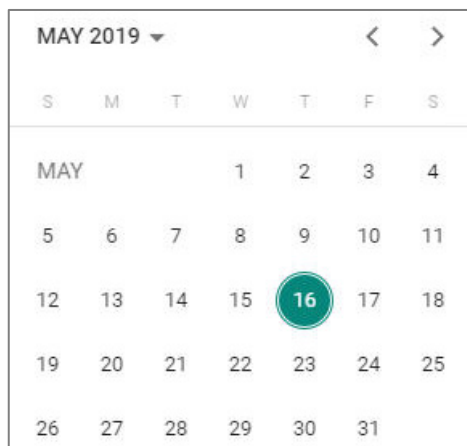
### Clock Source

Setting	Description	Factory Default
Select from the drop-down list	Specify whether to set the time manually (Local), from an SNTP server, from an NTP server, or from a PTP master.	Local

## Clock Source is from Local

### Date

Setting	Description	Factory Default
Select the date	Select the current date.	Local



The image shows a date selection interface for May 2019. At the top, it says 'MAY 2019' with a dropdown arrow and navigation arrows. Below are the days of the week: S, M, T, W, T, F, S. The calendar grid shows the following dates: Row 1: MAY, 1, 2, 3, 4; Row 2: 5, 6, 7, 8, 9, 10, 11; Row 3: 12, 13, 14, 15, 16 (highlighted with a green circle), 17, 18; Row 4: 19, 20, 21, 22, 23, 24, 25; Row 5: 26, 27, 28, 29, 30, 31.

### Time

Setting	Description	Factory Default
Input the current time	Specify the current time. You can manually input the time, or you can click <b>SYNC FROM BROWSER</b> to set the time based on the time used by your web browser.	None

## Clock Source is from SNTP

### Time Server 1

Setting	Description	Factory Default
Input the address of the 1st SNTP time server	Specify the IP or domain address of the 1st SNTP server to use (e.g., 192.168.1.1, time.stdtime.gov.tw, or time.nist.gov).	Time.nist.gov

### Time Server 2

Setting	Description	Factory Default
Input the address of the 2nd SNTP time server	Specify the IP or domain address of the secondary SNTP server to use if the first SNTP server fails to connect.	None

Click **APPLY** to complete.

## Clock Source is from NTP

If the switch is connecting to an NTP server that requires authentication, refer to the [Error! Reference source not found.](#) section to configure the NTP key to use.

### Time Server 1

Setting	Description	Factory Default
Input the address of the 1st NTP time server	Specify the IP or domain address of the 1st NTP server to use (e.g., 192.168.1.1, time.stdtime.gov.tw, or time.nist.gov).	time.nist.gov

### Time Server 2

Setting	Description	Factory Default
Input the address of the 2nd time server	Specify the IP or domain address of the secondary NTP server to use if the first NTP server fails to connect.	None

Click **APPLY** to complete.

## Clock Source is from PTP

Select PTP from the drop-down list of **Clock Source**. Click **APPLY** to complete.



## Time Zone

Users can configure the time zone for the switch. Click the **Time Zone** tab.

### System Time

Time
Time Zone
NTP Authentication

Time Zone \*  
UTC+00:00

**Daylight Saving**  
Daylight Saving \*  
Enabled

Offset  
01:00

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

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

**APPLY**

### Time Zone

Setting	Description	Factory Default
Select from the drop-down list	Specify the time zone to use for the switch.	GMT (Greenwich Mean Time)

## Daylight Saving Time

The Daylight Saving Time settings are used to automatically adjust the time according to regional standards.

### Daylight Saving Time

Setting	Description	Factory Default
Enabled	Enables Daylight Saving Time.	Disabled
Disabled	Disables Daylight Saving Time.	

### Offset

Setting	Description	Factory Default
User-specified hour	Specify the offset (in HH:MM format) to use during Daylight Saving Time.	None

### Start Date


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

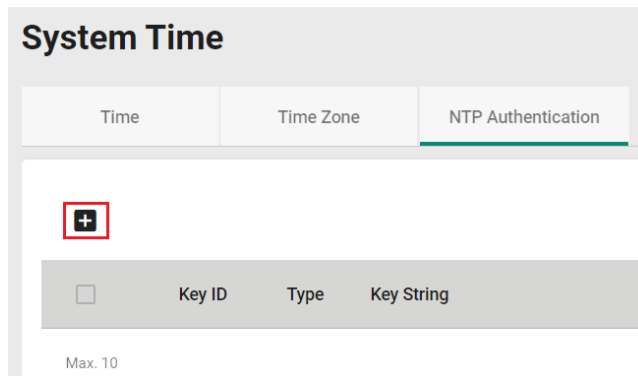
### End Date

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

When finished, click **APPLY** to activate the time zone settings.

## NTP Authentication

This section describes how to configure NTP Authentication. Click the **NTP Authentication** tab, and then click the  icon on the page.




Configure the following settings.

### Create Entry

Key ID \*

Type \*

MD5 ▼

Key String \* 

0 / 32

CANCEL CREATE

### Key ID

Setting	Description	Factory Default
Input the Key ID from 1 to 10	Input the Key ID to use for NTP authentication.	None

### Type

Setting	Description	Factory Default
Input the authentication type	Input the authentication type.	MD5

### Key String

Setting	Description	Factory Default
Input the key string for authentication, from 0 to 32 characters.	Input the password to use for the authentication key.	None

When finished, click **CREATE**.

## NTP Server

Click the **NTP Server** on the function menu to perform further configurations.

### NTP Server

Setting	Description	Factory Default
Enabled	Enable the NTP server.	Disabled
Disabled	Disable the NTP server.	

### Client Authentication

Setting	Description	Factory Default
Enabled	Enable NTP authentication.	Disabled
Disabled	Disable NTP authentication.	

When finished, click **APPLY** to save your changes.

## Time Synchronization

Click **Time Synchronization** on the function menu.

### General Settings

Click the **General** tab for the general settings.

### Time Synchronization

General
Port Settings
Status
Port Status

Time Synchronization \*  
Disabled ▼

Profile  
IEEE 1588 Default-2008 ▼

Clock Type \*  
Boundary Clock ▼

Delay Mechanism \*  
End-to-End ▼

Transport Mode \*  
802.3 Ethernet ▼

Priority 1 \*  
128

0 - 255

Priority 2 \*  
128

0 - 255

Domain Number \*  
0

0 - 255

Clock Mode \*  
Two Step ▼

Accuracy Alert \*  
1000

50 - 250000000 ns

Maximum Steps Removed \*  
255

0 - 255

APPLY

### Time Synchronization

Setting	Description	Factory Default
Enabled	Enable time synchronization.	Disabled
Disabled	Disable time synchronization.	

**Profile (read-only)**

Setting	Description	Factory Default
IEEE 1588 Default-2008	Show the current time synchronization profile.	IEEE 1588 Default-2008

**Clock Type**

Setting	Description	Factory Default
Boundary Clock	Set the Boundary Clock as the clock type.	Boundary Clock
Transparent Clock	Set the Transparent Clock as the clock type.	

**Delay Mechanism**

Setting	Description	Factory Default
End-to-End	Set End-to-End as the delay mechanism.	End-to-End
Peer-to-Peer	Set Peer-to-Peer as the delay mechanism.	

**Transport Mode**

Setting	Description	Factory Default
802.3 Ethernet	Set 802.3 Ethernet as the transport mode.	802.3 Ethernet
UDP IPv4	Set UDP IPv4 as the transport mode.	

**Priority 1**

Setting	Description	Factory Default
0 to 255	Set the priority 1 value.	128

**Priority 2**

Setting	Description	Factory Default
0 to 255	Set the priority 2 value.	128

**Domain Number**

Setting	Description	Factory Default
0 to 255	Set domain number value.	0

**Clock Mode**

Setting	Description	Factory Default
One Step	Set One Step as the clock mode.	802.3 Ethernet
Two Step	Set Two Step as the clock mode.	

**Accuracy Alert**


Setting	Description	Factory Default
50 to 250000000 (ns)	Set the accuracy alert value.	1000

**Maximum Steps Removed**

Setting	Description	Factory Default
0 to 255	Set the value of the maximum steps removed.	255

When finished, click **APPLY** to activate the general settings.

## Port Settings

Click the **Port Settings** tab. Click the edit icon  to configure the settings.

### Time Synchronization





General

Port Settings

Status

Port Status

IEEE 1588 Default-2008 Profile

	Port	Time Synchronization	Announce Interval	Announce Receipt Timeout (times)
	1/1	Disabled	1 (2 sec.)	3
	1/2	Disabled	1 (2 sec.)	3
	1/3	Disabled	1 (2 sec.)	3
	1/4	Disabled	1 (2 sec.)	3

### Edit Port 1/1 Settings

Time Synchronization \*

Disabled ▼

---

Announce Interval \*

1 (2 sec.) ▼

Announce Receipt Timeout \*

3 times

2 - 10

---

Sync Interval \*


0 (1 sec.) ▼

---

Delay-Request Interval \*

0 (1 sec.) ▼

---

Copy Configurations ... ▼ 

CANCEL
APPLY

### Time Synchronization

Setting	Description	Factory Default
Enabled	Enable time synchronization.	Disabled
Disabled	Disable time synchronization.	

### Announce Interval

Setting	Description	Factory Default
From 1 (2 sec.) to 4 (16 sec.)	Set announce interval value.	1 (2 sec.)

### Announce Receipt Timeout

Setting	Description	Factory Default
2 to 10 (times)	Set announce receipt timeout value.	3

### Sync Interval

Setting	Description	Factory Default
From -3 (0.125 sec.) to 5 (32 sec.)	Set synchronization interval value.	0 (1 sec.)

### Delay-Request Interval

Setting	Description	Factory Default
From -3 (0.125 sec.) to 5 (32 sec.)	Set delay-request interval value.	0 (1 sec.)

### Copy Configurations to Ports

Setting	Description	Factory Default
Select the port(s) from the drop-down list	Select the port(s) you want to copy the same configurations to.	0 (1 sec.)

When finished, click **APPLY** to save your changes.

## Status

Click the **Status** tab to view the detailed status of time synchronization.

### Time Synchronization

General

Port Settings

Status

Port Status

IEEE 1588 Default-2008 Profile 2022-01-19 14:07:59

**Status**

Time Synchronization	Synchronization Status	Clock Type	PTP Slave Port	PTP Clock Time
Enabled	Freerun	Boundary Clock	---	2018-12-21 19:29:20

**Current Data Set**

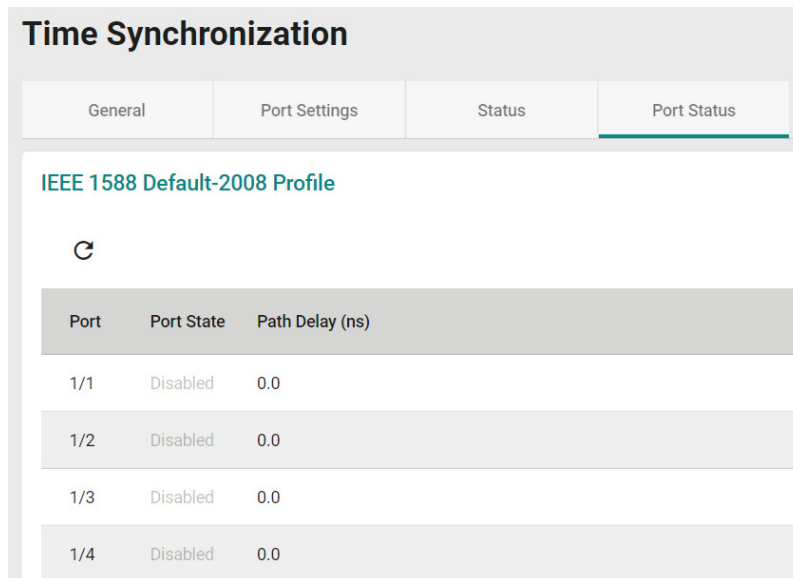
Offset From Master (ns)	Mean Path Delay (ns)	Steps Removed
0.0	0.0	0

**Parent Data Set**

Parent Identity	Grandmaster Identity	Grandmaster Priority 1	Grandmaster Priority 2
00:00:00:00:00:00	00:90:e8:ff:fe:72:56:12	128	128
Grandmaster Clock Class	Grandmaster Clock Accuracy		
248	254		

## Port Status

Click the **Port Status** tab to view the information of the port status.

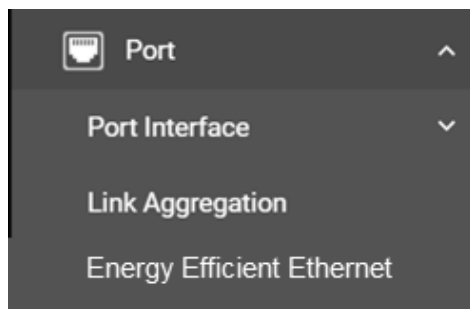


The screenshot shows the 'Time Synchronization' configuration page with the 'Port Status' tab selected. Below the tabs, the 'IEEE 1588 Default-2008 Profile' is displayed. A refresh icon is present. A table lists the status of four ports (1/1 to 1/4), all of which are 'Disabled' with a 'Path Delay (ns)' of 0.0.

Port	Port State	Path Delay (ns)
1/1	Disabled	0.0
1/2	Disabled	0.0
1/3	Disabled	0.0
1/4	Disabled	0.0

## Port

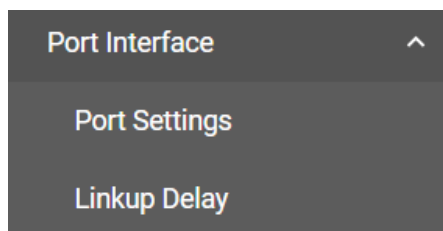
This section describes how to configure the **Port Interface**, **Link Aggregation**, and **Energy Efficient Ethernet** functions for the switch.



The screenshot shows a dark-themed menu for the 'Port' configuration. The 'Port' item is expanded, showing sub-items: 'Port Interface', 'Link Aggregation', and 'Energy Efficient Ethernet'.


## Port Interface

Two functions are included in this section: **Port Settings** and **Linkup Delay**.







The screenshot shows a dark-themed menu for the 'Port Interface' configuration. The 'Port Interface' item is expanded, showing sub-items: 'Port Settings' and 'Linkup Delay'.

## Port Settings

Under **Port Settings**, select the **Settings** tab and then click the  icon on the port you want to configure.

### Port Settings

Settings
Status

Port	Admin Status	Media Type	Description	Speed/Duplex	Flow Control	MDI/MDIX
 1/1	Enabled	XGFX,miniGBIC		--	Disabled	--
 1/2	Enabled	XGFX,miniGBIC		--	Disabled	--
 1/3	Enabled	XGFX,miniGBIC		--	Disabled	--
 1/4	Enabled	XGFX,miniGBIC		--	Disabled	--

Configure the following parameters.

### Edit Port 1/1 Settings

Admin Status \*  
Enabled ▼

Media Type  
 XGFX,miniGBIC

Description  
 0 / 127

Speed/Duplex ▼

Flow Control \*  
Disabled ▼ i

MDI/MDIX ▼

Copy Configurations ... ▼

CANCEL APPLY

### Admin Status

Setting	Description	Factory Default
Enable	Allows data transmission through this port.	Enabled
Disabled	Disables data transmission through this port.	

### Media Type

Setting	Description	Factory Default
Media type	Displays the media type for each module's port.	1000TX,RJ45,PTP



### Description

Setting	Description	Factory Default
Max. 63 characters	Specify an alias for the port to help differentiate between different ports (e.g., PLC1).	None

### Speed/Duplex

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
10M Half	Choose a fixed speed option if the connected Ethernet device has trouble auto-negotiating line speed.	
10M Full		
100M Half		
100M Full		
1G Full		
10G Half		
10G Full		

### Flow Control

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 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 changes the port type accordingly.	Auto
MDI	Choose MDI or MDIX if the connected Ethernet device has trouble auto-detecting the port type.	
MDIX		

### Copy Configurations to Ports

Setting	Description	Factory Default
Select the port(s) from the drop-down list	Allows you to copy the configuration to other port(s).	None

When finished, click **APPLY** to save your changes.

## Port Status

To view the status of the ports, click the **Status** tab.

Port Settings							
Settings		Status					
Port	Admin Status	Media Type	Link Status	Description	Flow Control	MDI/MDIX	Port State
1/1	Enabled	XGFX,miniGBIC	Link Down		Disabled	Invalid	Discarding
1/2	Enabled	XGFX,miniGBIC	Link Down		Disabled	Invalid	Discarding
1/3	Enabled	XGFX,miniGBIC	Link Down		Disabled	Invalid	Discarding
1/4	Enabled	XGFX,miniGBIC	Link Down		Disabled	Invalid	Discarding

# Linkup Delay

## Linkup Delay Overview

Linkup delay is used to prevent a port alternating between link up and link down. It is also sometimes called link flap prevention. This feature is useful when the link connection is unstable. An unstable connection might be caused by a faulty cable, faulty fiber transceiver, duplex mismatch, etc. This feature helps administrators to mitigate the risk of an unstable network, particularly when the topology changes frequently.



### NOTE

When using XG fiber and 2.5 fiber & copper, linkup delay will be enabled by default.

## Linkup Delay Settings

This section describes how to configure the linkup delay for the ports. Click the **Linkup Delay** menu. The default value is disabled, which means linkup delay is disabled for all ports.

Linkup Delay \*


Disabled





APPLY

### Enable

Setting	Description	Factory Default
Enable	Enables linkup delay.	Disabled
Disabled	Disables linkup delay.	

When finished, click **APPLY** to save your changes.

To configure linkup delay for a port, click the  icon on the port you want to configure.

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

Some parameters need to be configured.

### Edit Port 1/1 Settings

Linkup Delay \*  
Disabled ▼

Delay Time \*  
2

1 - 1000      sec.

Copy Configurations ... ▼ i

CANCEL
APPLY

#### Linkup Delay

Setting	Description	Factory Default
Enable	Enables linkup delay for the port.	Disabled
Disable	Disables linkup delay for the port.	

#### Delay Time (sec.)

Setting	Description	Factory Default
1 to 1000	Specify the linkup delay time from 1 to 1000 seconds.	2

#### Copy Configurations to Ports

Setting	Description	Factory Default
Select the port(s) from the drop-down list	Allows you to copy the configurations to other port(s).	None

When finished, click **APPLY** to save your changes.

## Link Aggregation

### Link Aggregation (Port Channel) Overview

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

Link aggregation includes the following features:

- **Static Trunk:** Manually configure up to 8 target ports and aggregate the links which are made by the target ports into a group.
- **LACP (Link Aggregation Control Protocols):** Dynamic link aggregation based on IEEE 802.3ad



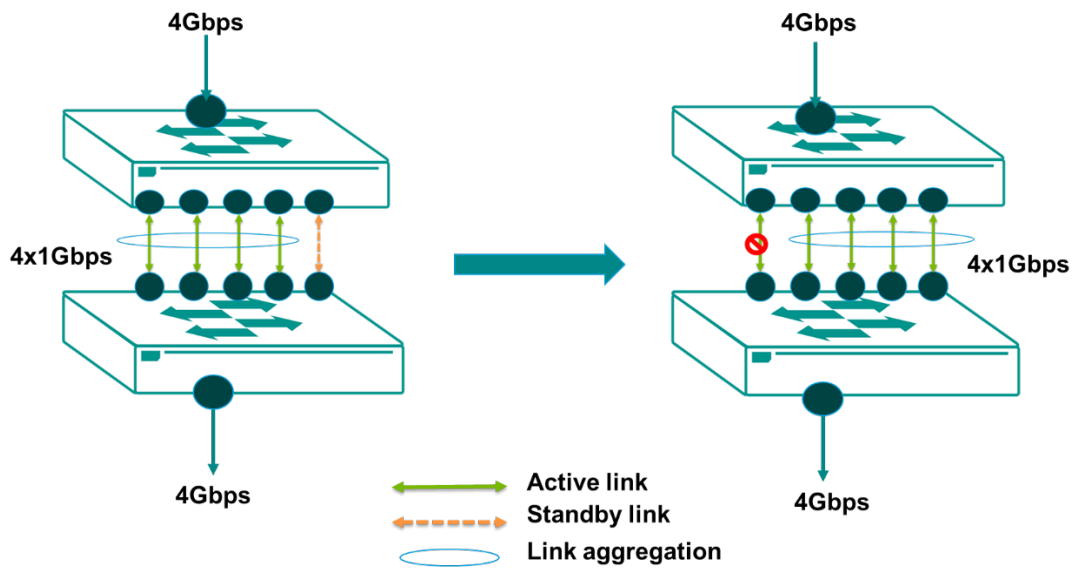
#### NOTE

Link aggregation requires link and port speeds to match.

### How Link aggregation works

Link aggregation can be configured to bundle the multiple links to enhance the bandwidth and achieve link redundancy. For example, the following figure illustrates 4 active links aggregated with physical connections

between two switches. Higher bandwidth can be efficiently achieved without upgrading hardware. Additionally, manually configuring standby ports for standby link as backups, allows link failure. In the event of a failover of one or more active links, the standby link switch to an active link to maintain the original bandwidth.



## LACP

The Link Aggregation Control Protocol (LACP) allows a network device to negotiate an automatic bundling of several ports by sending LACP packets to the peer, a directly connected device that also uses LACP.

## Static Trunk

For some networking applications, a situation can arise where traffic from multiple ports is required to be filtered through one port. For example, if there are 30 UHD IP surveillance cameras deployed and connected in a ring, the traffic can reach up to 1 Gbps, causing a surge in traffic that can increase network loading by up to 50%. Hence, the uplink port needs to use the static trunk function to provide more bandwidth and redundancy protection.

Additionally, the **High-availability Static Trunk (HAST) policy** can be applied to Static Trunk and enhance the availability by manually configuring standby ports. There are two policies available: Non-revertive and Revertive.

**Non-revertive:** When standby ports are configured, the standby links will activate when member port links are down and will remain activated, even if member ports revert to link up status.

**Revertive:** When the standby ports are configured, they will activate when member port links go down. When member port links are restored, activated standby ports will revert to standby. This feature can help maintain original link status automatically after confirming primary link recovery.



### NOTE

The high-availability static trunk policy will be effective only if LLDP is enabled and corresponding switch supports high-availability static trunk policies.

## Algorithm


In Link Aggregation, three load-sharing hash algorithms can be used: **SMAC**, **DMAC**, and **SMAC + DMAC**.

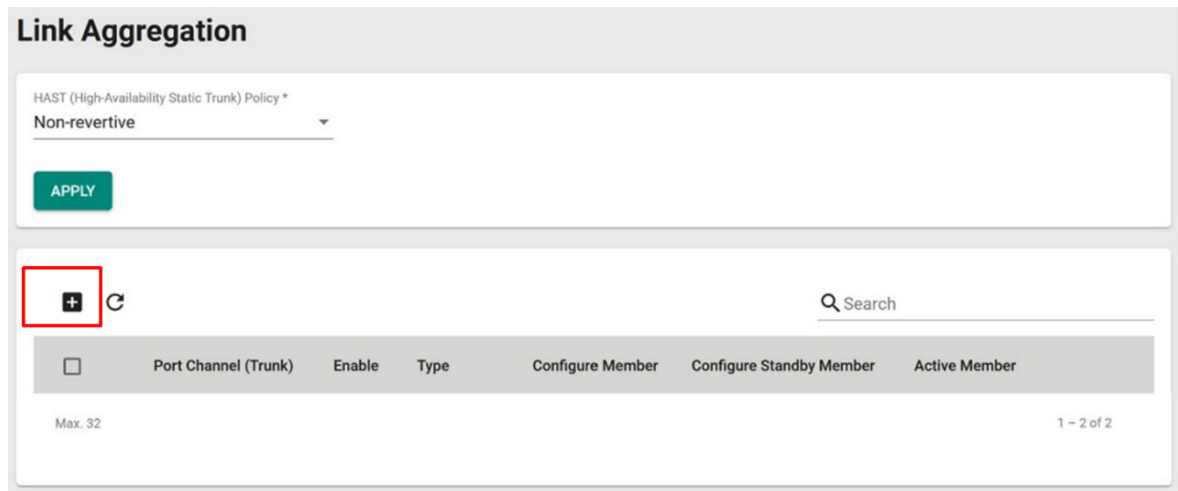
**SMAC:** SMAC stands for **Source MAC**, often used as a tool to optimize algorithm parameters. It is also an algorithm to evaluate the most efficient network data communication. SMAC is used for many different client situations.

**DMAC:** DMAC stands for **Destination MAC**. The packets will be distributed and transmitted to the destination MAC address hash algorithm, and is usually used in many different destination servers situation.

**SMAC + DMAC:** This can be used for more complex hash algorithm, but where the network just has a few clients and servers.

## Link Aggregation Settings

This section describes how to configure link aggregation for each port. Click **Link Aggregation** on the menu and then click the  icon on the configuration page.




To create a link aggregation group, configure the following parameters.

### Create Link Aggregation

LA Group Status \*

Type \*

Config Member Port \* 

Algorithm \*

### LA Group Status

Setting	Description	Factory Default
Enable	Enable link aggregation grouping.	Enabled
Disable	Disable link aggregation grouping.	

### Type

Setting	Description	Factory Default
Manual	Configure the link aggregation type manually.	None

LACP	Configure the link aggregation type by LACP.	
------	--	--

#### Config Member Port

Setting	Description	Factory Default
Select from the ports	Select the ports you want to create for link aggregation grouping.	None



#### Config Standby Port (Manual only)

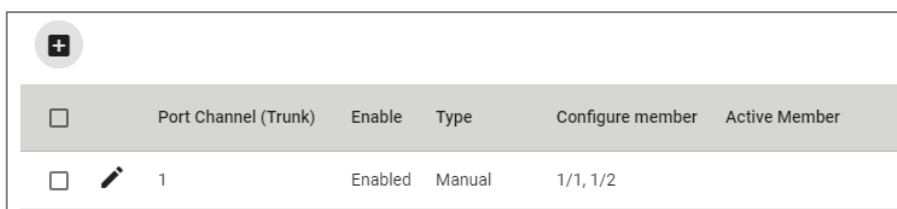
Setting	Description	Factory Default
Select from the ports	Select the ports you want to create for standby link aggregation grouping.	None

#### Algorithm (in Advanced Mode only)

Setting	Description	Factory Default
SMAC	Use SMAC as algorithm configuration.	SMAC + DMAC
DMAC	Use DMAC as the algorithm configuration.	
SMAC + DMAC	Use both SMAC and DMAC as the algorithm configuration.	

When finished, click **CREATE** to continue.

You can view the current Link Aggregation or Port Channel (Trunk) status on the configuration page. You can also edit or delete by clicking the  or  icon on the page.



<input type="checkbox"/>	Port Channel (Trunk)	Enable	Type	Configure member	Active Member
<input type="checkbox"/>	1	Enabled	Manual	1/1, 1/2	

To apply the HAST policy, configure the following parameters.

### Link Aggregation

HAST (High-Availability Static Trunk) Policy \*

Non-revertive ▼

**APPLY**

#### HAST (High-Availability Static Trunk) Policy

Setting	Description	Factory Default
Non-revertive	Maintain the link status regardless of member ports link up	Non-revertive
revertive	Return to original link status when member ports link up	

When finished, click **APPLY** to continue.

The following steps configure one or more ports as member ports for the primary link. You can also configure standby ports for backup links with high availability static trunk (HAST) policy to return the original link status after member ports recovery with static trunks.



1. Enable Group Status.
2. Select Type from drop-down list and choose Manual.
3. Select member ports (max. 8 ports)
4. Select standby ports (max. 8 ports)
5. After creating the configuration, select HAST policy from drop-down list and choose Revertive.
6. Click **APPLY**.



## NOTE

1. Member ports and standby ports must be unique. Duplicate or re-used ports in same or different sessions is not supported.
2. The high-availability static trunk policy will be effective only if LLDP is enabled and corresponding switch supports high-availability static trunk policies.
3. The high-availability static trunk policy will not be effective if no standby port is specified.

## Editing Port Setting for Link Aggregation

To edit each port's setting for Link Aggregation, click the  icon on the port name. You can also check the port and then click the  icon for editing the port settings for Link Aggregation.

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

Edit the following port settings.

### Edit Port Channel 1 Settings

LA Group Status \*  
Enabled

Type \*  
LACP

Config Member Port \*  
1/2

Algorithm \*  
SMAC + DMAC

### LA Group Status

Setting	Description	Factory Default
Enable	Enable link aggregation grouping.	None
Disable	Disable link aggregation grouping.	

### Type

Setting	Description	Factory Default
Manual	Configure link aggregation manually.	None
LACP	Configure link aggregation by LACP.	

### Config Member Port

Setting	Description	Factory Default
Select from the ports	Select the ports you want to create link aggregation grouping for.	None

### Config Standby Port (Manual only)


Setting	Description	Factory Default
Select from the ports	Select the ports to create standby link aggregation grouping for.	None

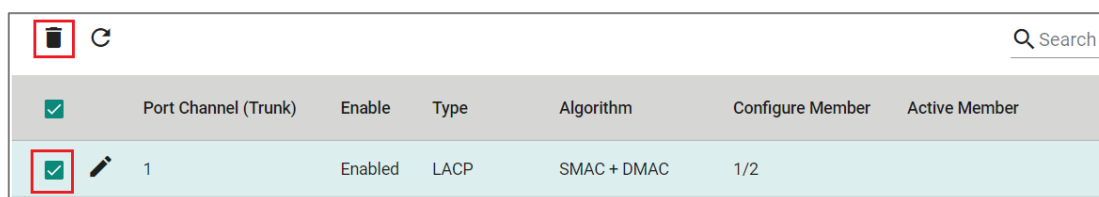
### Algorithm (in Advanced Mode only)

Setting	Description	Factory Default
SMAC	Use SMAC as the algorithm configuration.	SMAC + DMAC
DMAC	Use DMAC as the algorithm configuration.	
SMAC + DMAC	Use both SMAC and DMAC as the algorithm configuration.	

When finished, click **APPLY** to continue.

## Deleting the Port for Link Aggregation

To delete the port for Link Aggregation, check the port and then click  con.



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

Click **DELETE** to finish. Note that some features, such as RSTP and VLAN will be set to default values once you delete the Link Aggregation setting.

### Delete Link Aggregation

Warning:  
Some features (like RSTP, VLAN...etc.) related to selected Link Aggregation will be set to default values.

Are you sure you want to delete the selected Link Aggregation?



# Energy Efficiency Ethernet

## Energy Efficiency Ethernet (EEE) Overview

Energy Efficiency Ethernet function which is based on standard 802.3az can be enabled to save the power when there is no traffic on the link. This function can support only on 100/1000/2500M copper.

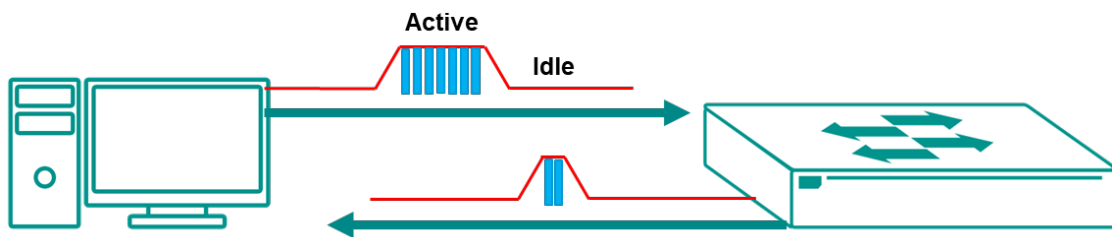


### NOTE

OOB port is not supporting EEE function.

## How Energy Efficiency Ethernet works

802.3az EEE is designed to reduce power consumption by detecting active traffic on the link when both sides of ports are up. This function operates at the PHY layer. Ports will enter LPI (Low Power Idle) mode when no data transmission is detected over the link, saving the power during periods of no traffic.



## EEE Settings and Status

This section describes how to configure EEE.

### Settings

Locate EEE, and then click the Settings tab to configure.

### Energy Efficient Ethernet (EEE)

Settings    Status


Energy Efficient Ethernet (EEE) \*  
Enabled

APPLY



Port can be enabled even port doesn't support EEE.

Port	Energy Efficient Ethernet (EEE)
1/1	Enabled
1/2	Enabled
1/3	Enabled
1/4	Enabled
1/5	Enabled
1/6	Enabled
1/7	Enabled
1/8	Enabled

All ports are enabled by default.

Click the  icon to configure a specific port.

Port can be enabled even port doesn't support EEE.

Port	Energy Efficient Ethernet (EEE)
 1/1	Enabled
 1/2	Enabled

Configure the following:

### Edit Port 1/1 Settings

Energy Efficient Ethernet (EEE) \*

Enabled ▼

Copy configurations to... ▼ ⓘ

CANCEL APPLY

#### Energy Efficient Ethernet (EEE)

Setting	Description	Factory Default
Enabled	Enable Energy Efficient Ethernet (EEE)	Enabled
Disabled	Disable Energy Efficient Ethernet (EEE)	

#### Copy Configurations to Ports

Setting	Description	Factory Default
Select the port(s) from the drop-down list	Select the destination port(s) for copying the configuration.	

When finished, click **APPLY** to save your changes.

## Status

Click the **Status** tab to view the information of the port status.

### Energy Efficient Ethernet (EEE)

Settings

Status

↻
🔍 Search

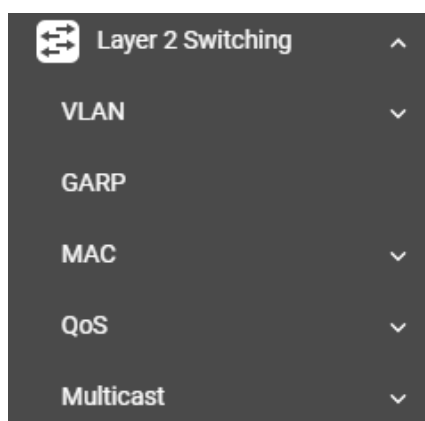
Port	EEE Status ↑	Local Capability	Neighbor Capability	Media Type	Link Status
3/1	Active	Supported	Supported	1000TX,RJ45	1G, Full (Auto)
3/2	Inactive	Supported	Not Supported	1000TX,RJ45	Link Down
3/3	Active	Supported	Supported	1000TX,RJ45	1G, Full (Auto)
3/4	Inactive	Supported	Not Supported	1000TX,RJ45	Link Down

Refer to the following table for a detailed description of each item.

Item	Description
Port	The port number on this device.
EEE Supported	Indicates the status of EEE support
Local Capability	Indicates local port support for EEE
Neighbor Capability	Indicates neighbor port support for EEE
Media Type	Displays the media type of each module port.
Link Status	Link Up: The port is connected. Link Down: The port is disconnected.

## Layer 2 Switching

This section describes how to configure various parameters, such as **VLAN**, **GARP**, **MAC**, **QoS**, and **Multicast**, for Moxa's switch. Click **Lay 2 Switching** on the function menu.



## VLAN

VLAN (Virtual Local Area Network) is a network management technology where IEEE 802.11Q is widely applied.

### IEEE 802.1Q Overview

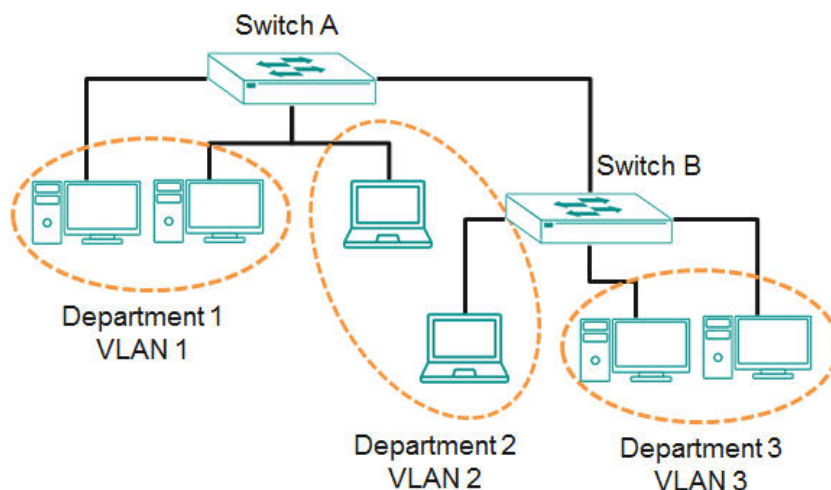
The IEEE 802.1Q is a network communication protocol that falls under the IEEE 802.1 standard regulation, allowing various segments to use a physical network at the same time to block broadcast packets by different segmentations. It specifies the VLAN tagging for Ethernet frames on switches that can control the path process.

## How A VLAN Works

### What is a VLAN?

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

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



### Benefits of VLANs

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

- **VLANs ease the relocation of devices on networks:** With traditional networks, network administrators spend much of their time dealing with changes. If users move to a different subnetwork, the addresses of each host must be updated manually. With a VLAN setup, if a host originally on the Marketing VLAN is moved to a port on another part of the network, and retains its original subnet membership, you only need to specify that the new port is on the Marketing VLAN. You do not need to do any re-cabling.
- **VLANs provide extra security:** Devices within each VLAN can only communicate with other devices on the same VLAN. If a device on the Marketing VLAN needs to communicate with devices on the Finance VLAN, the traffic must pass through a routing device or Layer 3 switch.
- **VLANs help control traffic:** With traditional networks, congestion can be caused by broadcast traffic that is directed to all network devices, regardless of whether or not they need it. VLANs increase the efficiency of your network because each VLAN can be set up to contain only those devices that need to communicate with each other.

### VLANs and the Moxa switch

Your Moxa switch includes support for VLANs using IEEE Std 802.1Q-2005. This standard allows traffic from multiple VLANs to be carried across one physical link. The IEEE Std 802.1Q-2005 standard allows each port on your Moxa switch to be placed as follows:

- On a single VLAN defined in the 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:

- Management VLAN ID 1 can be changed
- 802.1Q VLAN default ID 1 cannot be deleted

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 with devices on a different VLAN, a router or Layer 3 switching device with connections to both VLANs need 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

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

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

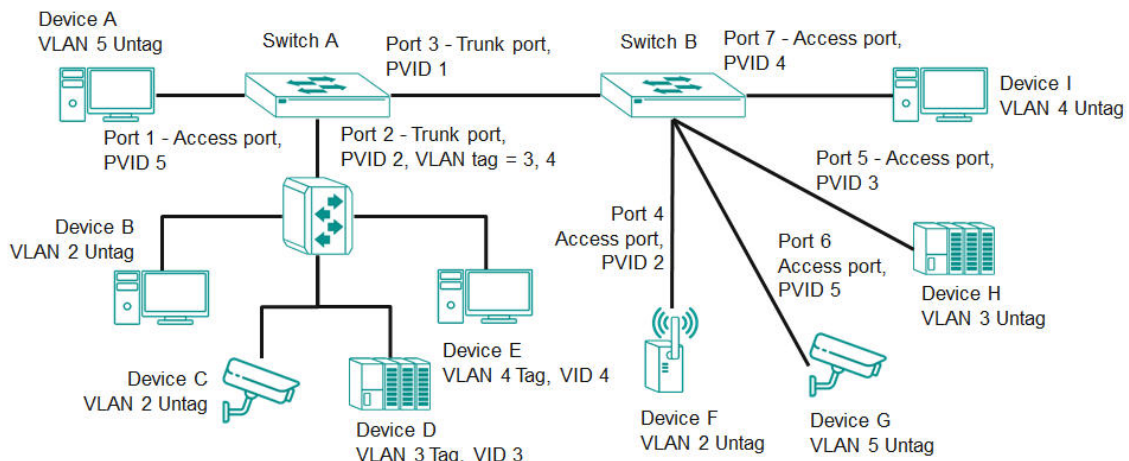
The IEEE Std 802.1Q-2005 defines how VLANs operate within an open packet-switched network. An 802.1Q compliant packet carries additional information that allows a switch to determine which VLAN the port belongs to. If a frame is carrying the additional information, it is known as a tagged frame.

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 to which VLAN. To communicate between VLANs, a router must be used.

Moxa's 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 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 and tagged devices. In general, the traffic of the Trunk Port must have a Tag. Users can also assign a PVID to a Trunk Port. The untagged packet on the Trunk Port will be assigned the default port PVID as its VID.
- **Hybrid Port:** The port is similar to a Trunk port, except users can explicitly assign tags to be removed from egress packets.

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



In this application:

- Port 1 connects a single untagged device and assigns it to VLAN 5; it should be configured as an **Access Port** with PVID 5.
- Port 2 connects a LAN with two untagged devices belonging to VLAN 2. One tagged device with VID 3 and one tagged device with VID 4. It should be configured as a **Hybrid Port** with PVID 2 for untagged 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 a **Trunk Port**. GVRP protocol will be used through the Trunk Port.
- Port 4 connects a single untagged device and assigns it to VLAN 2; it should be configured as an **Access Port** with PVID 2.
- Port 5 connects a single untagged device and assigns it to VLAN 3; it should be configured as an **Access Port** with PVID 3.
- Port 6 connect a single untagged device and assigns it to VLAN 5; it should be configured as an **Access Port** with PVID 5.
- Port 7 connects a single untagged device and assigns it to VLAN 4; it should be configured as an **Access Port** with PVID 4.

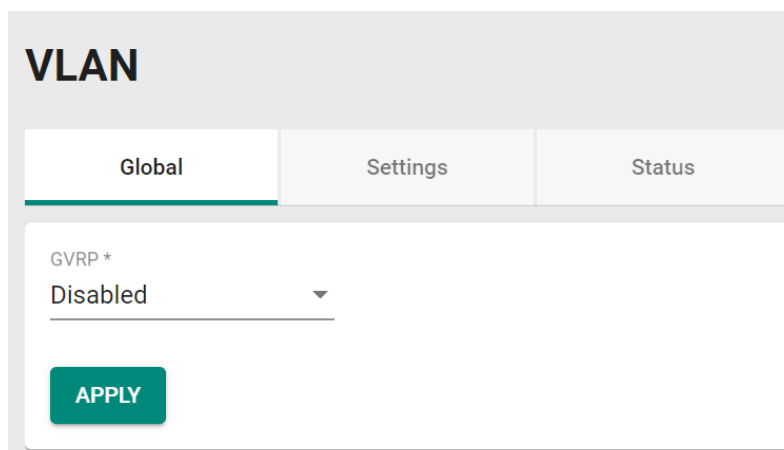
After the application is properly configured:

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

## VLAN Settings

To configure VLAN, click **VLAN** on the function menu. GVRP (Generic VLAN Registration Protocol) is an IEEE 802.1Q standard protocol that helps specify how to define a method of tagging frames with VLAN configuration data. It essentially facilitates management of VLAN within a larger network data communication.

To edit the GVRP function, click the **Global** tab.



The screenshot shows the 'VLAN' configuration page. At the top, there are three tabs: 'Global', 'Settings', and 'Status'. The 'Global' tab is currently selected and highlighted with a green underline. Below the tabs, there is a dropdown menu labeled 'GVRP \*' with the value 'Disabled' selected. A green 'APPLY' button is located below the dropdown menu.


Configure the following setting.

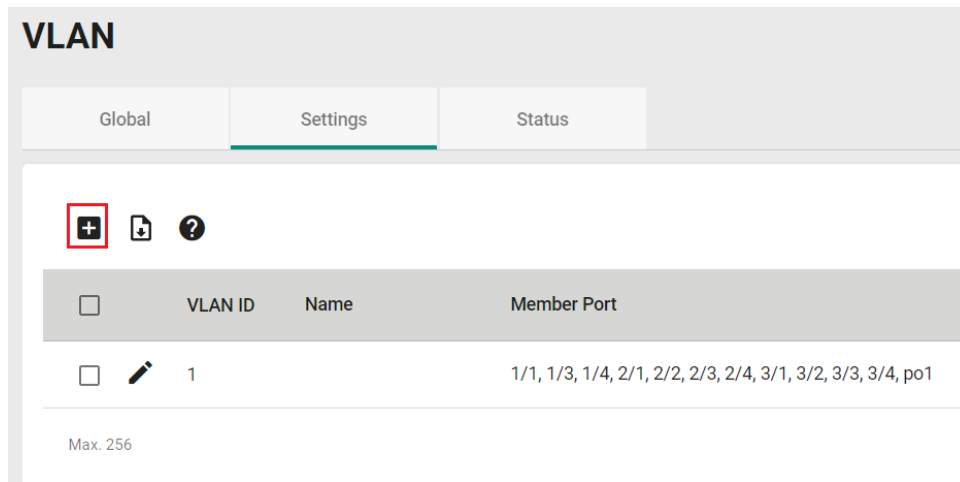
**GVRP**

Setting	Description	Factory Default
Disabled	Disables GVRP.	Disabled
Enabled	Enables GVRP.	

Click **APPLY** to finish.




## Detailed VLAN Settings

Click the **Settings** tab, and then click the  icon.



**VLAN**

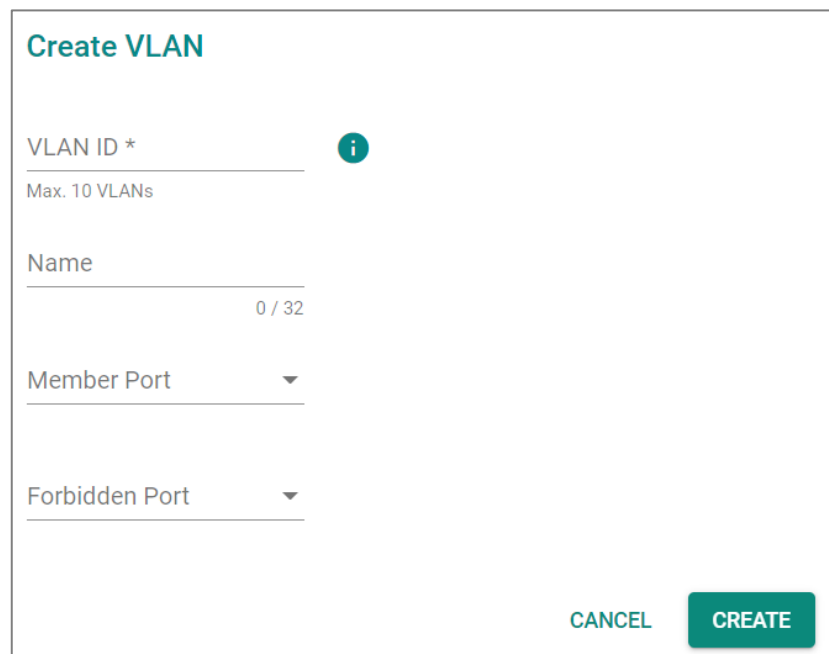
Global Settings Status


<input type="checkbox"/>	VLAN ID	Name	Member Port
<input type="checkbox"/>	1		1/1, 1/3, 1/4, 2/1, 2/2, 2/3, 2/4, 3/1, 3/2, 3/3, 3/4, po1

Max. 256

Configure the following parameters.



**Create VLAN**

VLAN ID \*   
 Max. 10 VLANs

Name  
 0 / 32

Member Port ▼

Forbidden Port ▼

CANCEL CREATE

**VLAN ID**

Setting	Description	Factory Default
Input a VLAN ID, (10 VLANs max.)	Input a VLAN ID.	None

### Name

Setting	Description	Factory Default
Input a name for the VLAN, (32 characters max.)	Specify a name for the VLAN.	None

### Member Port


Setting	Description	Factory Default
Select the port from the drop-down list.	Specify the ports that are the member ports for the VLAN.	None

### Forbidden Port (in Advanced Mode only)

Setting	Description	Factory Default
Select the port from the drop-down list	Specify the ports that are forbidden for the VLAN.	None

When finished, click **CREATE**.

## Editing the Existing VLAN Settings

To edit the exiting VLAN settings, click the  icon of the VLAN you want to edit.

### VLAN

Global Settings Status

+ ↕ ?

<input type="checkbox"/>	VLAN ID	Name	Member Port
<input type="checkbox"/>	1		1/1, 1/3, 1/4, 2/1, 2/2, 2/3, 2/4, 3/1, 3/2, 3/3, 3/4, po1

Max. 256

Configure the following settings.

### Edit VLAN 1 Settings

VLAN ID  
1  
Max. 10 VLANs

Name  
0 / 32

Member Port  
1/1, 1/3, 1/4, 2/1, 2/2...

Forbidden Port

CANCEL APPLY



### VLAN ID

Setting	Description	Factory Default
Show the VLAN ID	Display the VLAN ID.	None

### Name

Setting	Description	Factory Default
Show the name of the VLAN	Display the VLAN name.	None

### Member Port


Setting	Description	Factory Default
Select the port from the drop-down list	Specify the ports that are member ports for the VLAN.	None




### Forbidden Port (in Advanced Mode only)

Setting	Description	Factory Default
Select the port from the drop-down list	Specify the ports that are forbidden for the VLAN.	None

When finished, click **Apply** to save your changes.

## Editing the Port Settings

To edit the port settings, in the **VLAN** tab select the  icon on the port you want to configure on the lower part of the page.

	Port	Mode	PVID	GVRP	Untagged VLAN	Tagged VLAN
	1/1	Access	1	Disabled	1	
	1/3	Access	1	Disabled	1	
	1/4	Access	1	Disabled	1	

Configure the following settings.

### Edit Port 1/1 Settings

Mode \*  
Access ▼

PVID \*  
1 ▼

GVRP  
Disabled ▼

Tagged VLAN  
 ▼

Untagged VLAN  
All Member VLAN IDs ▼

Copy Configurations ... ▼ i

CANCEL
APPLY

#### Mode

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

#### PVID

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

#### GVRP

Setting	Description	Factory Default
Enabled	Enables GVRP.	Disabled
Disabled	Disables GVRP.	

#### Tagged VLAN

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

#### Untagged VLAN


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

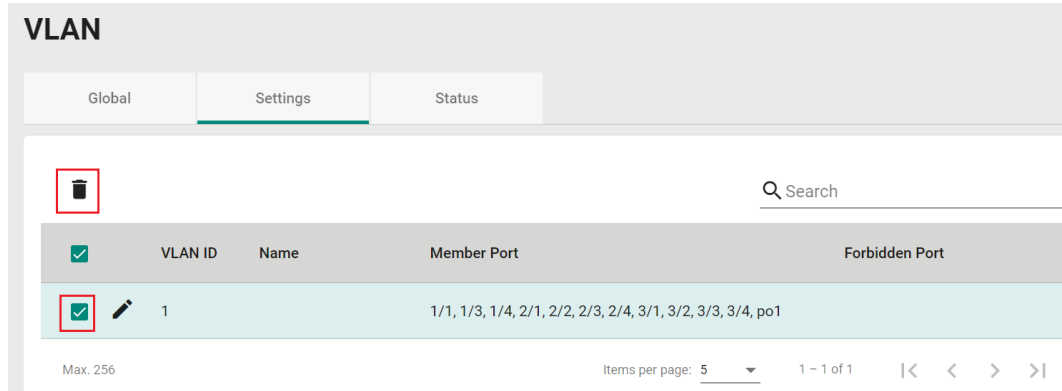
### Copy Configurations to Ports

Setting	Description	Factory Default
Select the port(s) from the drop-down list	Copy the configuration to other port(s).	None

When finished, click **APPLY** to save your changes.

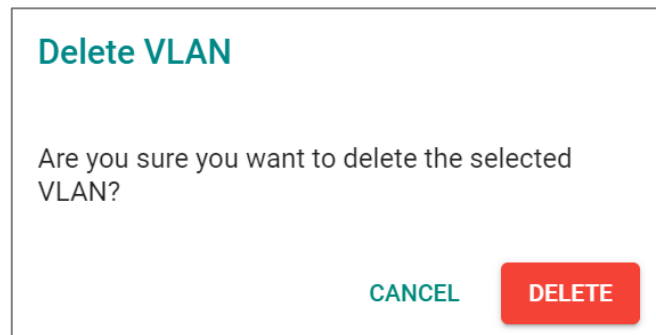
## Deleting an Existing VLAN

In Settings tab, check the VLAN you want to delete, and click the delete icon  .



The screenshot shows the 'VLAN' configuration page with the 'Settings' tab selected. A table lists VLAN configurations. The first row is selected, and a delete icon is highlighted in a red box. The table has columns: VLAN ID, Name, Member Port, and Forbidden Port. The selected row has VLAN ID 1, Name (empty), Member Port '1/1, 1/3, 1/4, 2/1, 2/2, 2/3, 2/4, 3/1, 3/2, 3/3, 3/4, po1', and Forbidden Port (empty). A search bar is visible at the top right of the table area.

Click **DELETE** to delete the VLAN.




The dialog box is titled 'Delete VLAN'. It contains the text 'Are you sure you want to delete the selected VLAN?'. At the bottom, there are two buttons: 'CANCEL' and 'DELETE'.

## GARP Overview

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

## GARP Settings

Select **GARP** on the menu page, and then click the  icon on the port you want to configure.

	Port	Join Time	Leave Time	Leave All Time
	1/1	200	600	10000
	1/3	200	600	10000
	1/4	200	600	10000

Configure the following settings.

### Edit Port 1/1 Settings

Join Time \*

200

10 - 1073741810

Leave Time \*


600

30 - 2147483630

Leave All Time \*

10000

40 - 2147483640

Copy Configurations ... 

### Join Time (sec.)

Setting	Description	Factory Default
10 to 499999980	Input the join time from 10 to 499999980 seconds.	200

### Leave Time (sec.)

Setting	Description	Factory Default
30 to 499999980	Input the leave time from 30 to 499999980 seconds.	600

### Leave All time (sec.)

Setting	Description	Factory Default
30 to 499999990	Input the leave all time.	10000

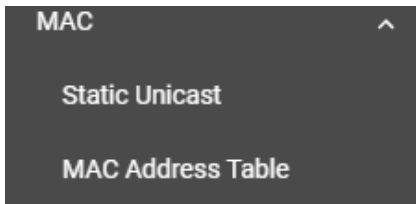
### Copy Configurations to Ports

Setting	Description	Factory Default
Select the port(s) from the drop-down list	Copy the configurations to other port(s).	None

When finished, click **APPLY** to save your changes.

# MAC

This section explains Independent VLAN learning and describes how to configure **Static Unicast** and the **MAC Address Table**.



## Independent VLAN Learning

Moxa's switch uses the **Independent VLAN Learning (IVL)** mode.

In an **IVL Mode**, a MAC table will be created in each VLAN, which will constitute many MAC tables. However, the same VID record will be selected and put in a table. A MAC table will be stored in the format of MAC + VID, the same MAC will be stored in different tables with different VIDs.

## Static Unicast

Click **Static Unicast** on the function menu page and click the **+** icon on the configuration page.



Configure the following settings.

### Add Static Unicast Entry

VLAN ID \*  MAC Address \*

Port \*

### VLAN ID

Setting	Description	Factory Default
Input a VLAN ID	Input a VLAN ID.	None

### MAC Address

Setting	Description	Factory Default
MAC address of the port	Input the MAC address of the port.	None

### Port

Setting	Description	Factory Default
Select the port from the drop-down list	Specify the port you want to create a VLAN for.	None

When finished, click **CREATE**.

## MAC Address Table

Select **MAC Address Table** and configure the following settings.

### MAC Address Table

MAC Learning Mode  
Independent VLAN Learning

Aging Time \*  
300

10 - 300 sec.

**APPLY**

### MAC Learning Mode

Information	Description	Factory Default
Independent VLAN learning	Show the current MAC Learning Mode.	Independent VLAN learning

### Aging Time

Setting	Description	Factory Default
10 to 300	Input a VLAN ID.	None

When finished, click **APPLY** to save your changes.

You can view the current MAC Address Table on the bottom part of the configuration page.

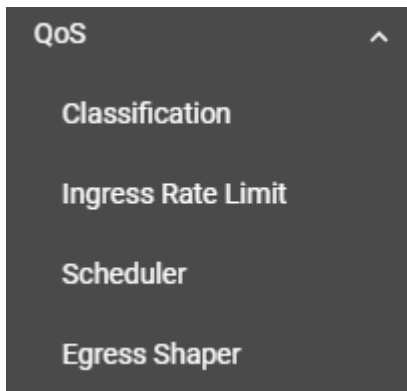
Refresh Download

Index	VLAN	MAC Address	Type	Port
1	1	c8:cb:b8:02:26:5f	Learnt Unicast	3/4

Item Name	Description
Index	The number of the MAC address.
VLAN	The VLAN number
MAC Address	The MAC address on this device.
Type	Learnt Unicast, Learnt Multicast, Static Unicast, Static: Multicast
Port	The forwarding port of this MAC address.

# QoS

This section describes how QoS works and how to configure the settings.



## QoS Overview

The 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 switch can inspect both IEEE 802.1p/1Q layer 2 CoS (Class of Service) tags, and even layer 3 DSCP (Differentiated Services Code Point) information to provide consistent classification of the entire network. The switch's QoS capability improves the performance and determinism of industrial networks for mission-critical applications.

## The Traffic Prioritization Concept

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

- Improve network performance by controlling a wide variety of traffic and by managing congestion.
- Assign priorities to different categories of traffic. For example, set higher priorities for time-critical or mission-critical applications.
- Provide predictable throughput for multimedia applications, such as video conferencing or voice over IP, and minimize traffic delay and jitter.
- Optimize the network utilization depending on application usage and usage needs. Hence, asset owners do not always need to expand their backbone bandwidth as the amount of traffic increases.

Traffic prioritization uses eight traffic queues to ensure that higher priority traffic can be forwarded separately from lower priority traffic, which guarantees Quality of Service (QoS) to your network.

Moxa switch traffic prioritization is based on two standards:

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

## IEEE 802.1p Class of Service

The IEEE Std 802.1D 2005 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 IEEE 802.1p occupying 3 bits of the tag follows the destination MAC address and Source MAC address.

The IEEE Std 802.1D 2005 Edition priority marking scheme assigns an IEEE 802.1p priority level between 0 and 7 to each frame, which specifies the level of service that the associated packets shall be handled. The table below shows an example of how different traffic types can be mapped to the eight IEEE 802.1p priority levels.

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

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

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

## Differentiated Services (DiffServ) Traffic Marking

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

The advantages of DiffServ over IEEE 802.1Q are as follows:

- You can prioritize and assign different traffic with appropriate latency, throughput, or reliability by each port.
- No extra tags are required.
- The DSCP priority tags are carried in the IP header, which can pass the WAN boundaries and through the Internet.
- DSCP is backwards compatible with Ipv4 ToS (Type of Service), which allows operation with legacy devices that use Ipv4 layer 3.

## Traffic Prioritization

Moxa switches classify traffic based on layer 2 of the OSI 7 layer model, and the switch prioritizes outbound traffic according to the priority information defined in the received packet. Incoming traffic is classified based upon the IEEE 802.1p service level field and is assigned to the appropriate egress priority queue. The traffic flow through the switch is as follows:

- A packet received by the Moxa switch may or may not have an 802.1p tag associated with it. If it does not, then it is given a default CoS value (according to the port settings in the classification section). Alternatively, the packet might be marked with a new 802.1p value, which will result in all knowledge of the previous 802.1p tag being lost.
- Each egress queue has associated 802.1p priority levels, and can be defined by users, the packet will be placed in the appropriate priority queue. When the packet reaches the head of its queue and is about to be transmitted, the device determines whether or not the egress port belongs to the VLAN group. If it is, then the new 802.1p tag is used in the extended 802.1D header.

## 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 undergoes 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:

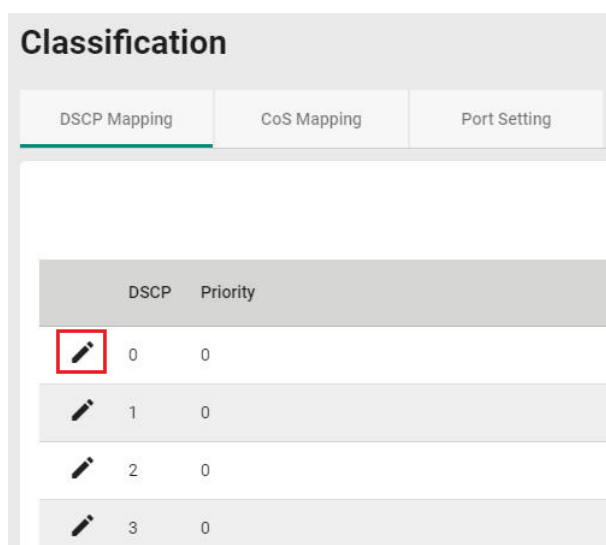
- **Weight Fair:** This method services all the traffic queues, giving priority to the higher priority queues. Under most circumstances, the Weight Fair method gives high priority precedence over low priority, but in the event that high priority traffic does not reach the link capacity, lower priority 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.

## Classification

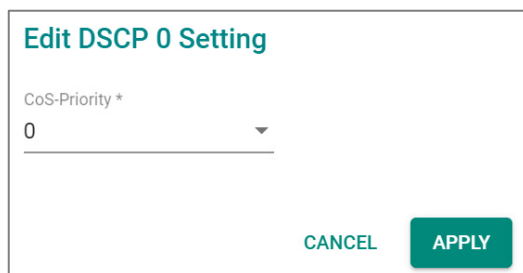
There are three parameters in this section: **DSCP Mapping**, **CoS Mapping**, and **Port Setting**. The three parameters are described below in detail.

### DSCP to CoS Mapping

In the **Classification** menu, click the **DSCP Mapping** tab, and then click the  icon.



Configure the priority setting from the drop-down list for this port.



#### DSCP Value and Priority

Setting	Description	Factory Default
0 to 7	Different DSCP values map to one of eight different priorities from 0 to 7.	0
8 to 15		1
16 to 23		2
24 to 31		3
32 to 39		4
40 to 47		5
48 to 55		6
56 to 63		7





When finished, click **APPLY** to save your changes.

## CoS to Queue Mapping

In the **Classification** menu, click the **CoS Mapping** tab, and then click the  icon.

### Classification

DSCP Mapping
CoS Mapping
Port Setting

	CoS	Queue
	0	1
	1	2
	2	3
	3	4

Configure the Queue priority setting for the port.

### Edit CoS 0 Setting

Queue \*

1
▼

CANCEL
APPLY

### Queue Priority





Setting	Description	Factory Default
0	Different 802.1p values map to one of the eight different queues from 1 (lowest priority) to 8 (highest).	1
1		2
2		3
3		4
4		5
5		6
6		7
7		8

## Port Settings

In the **Classification** menu, click the **Port Setting** tab, and then click the  icon.

### Classification

DSCP Mapping
CoS Mapping
Port Setting

	Port	Trust Type	Priority
	1/1	CoS	3
	1/2	CoS	3
	1/3	CoS	3
	1/4	CoS	3

Configure the following settings.

### Edit Port 1/1 Settings

Trust Type \*


CoS ▼

---

Untag Default Priority \*

3 ▼

---

Copy Configurations ... ▼ 

CANCEL
APPLY

#### **Trust Type**

Setting	Description	Factory Default
CoS	Enables the port with CoS-based traffic classification.	CoS
DSCP	Enables the port with DSCP-based traffic classification.	

#### **Untag Default Priority**

Setting	Description	Factory Default
0 to 7	802.1p tag (CoS) can be range from 0 (lowest) to 7 (highest).	3

#### **Copy Config to Ports**

Setting	Description	Factory Default
Select from the drop-down list	Copy the settings to other ports you select.	None

When finished, click **APPLY** to save your changes.

# Ingress Rate Limit

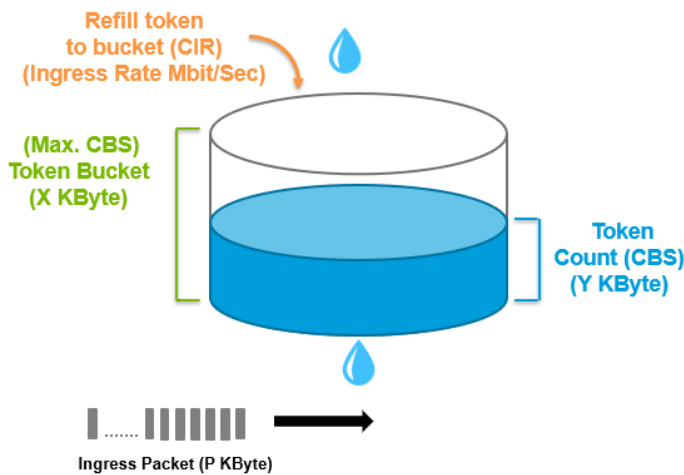
## Ingress Rate Limit Overview

The rate limit is composed of the meter and the marker. The meter is the monitoring of the data rates for a particular class of traffic. When the data rate exceeds user-configured values, marking or dropping of packets occurs immediately. The meter does not buffer the traffic; therefore, the transmission delay is not affected. When traffic exceeds the user's specified value, you can instruct the system to either drop the packets or mark QoS fields in them. The meter algorithms include simple token bucket and SrTCM (Single Rate Three Color Marker) (RFC2697). The marker of the rate limit is included and remarked in the 802.1p or the DSCP field of the packet.

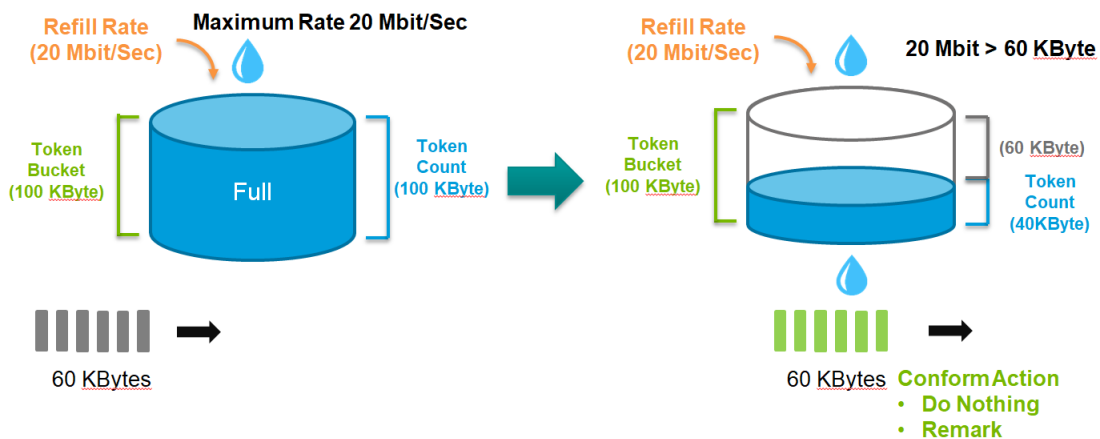
## Simple Token Bucket

### The Token Bucket Concept

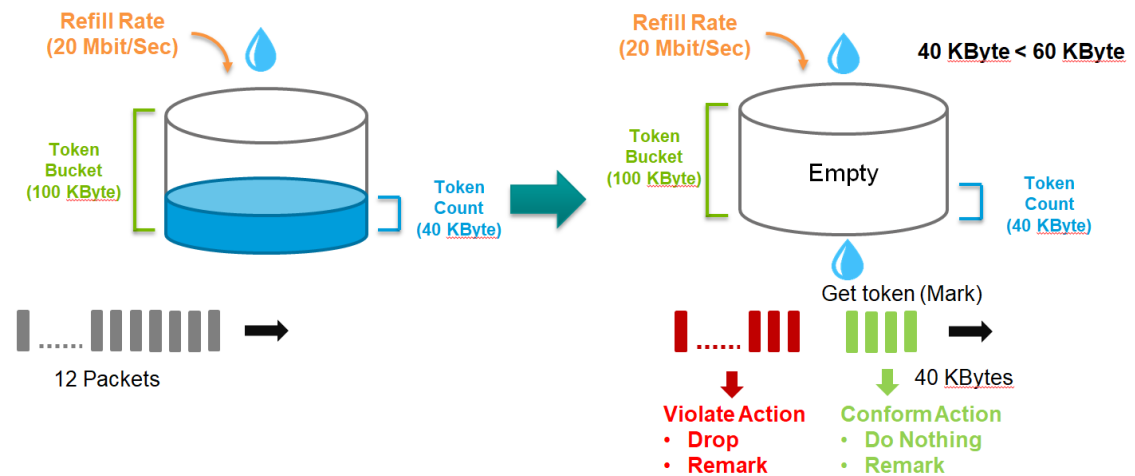
Token Bucket is an algorithm used to achieve an efficient network flow control and manage bandwidth. This algorithm is based on a token bucket that allows for a traffic surge for short periods. When a token is unavailable, no burst of packets can be sent. Under this concept, the number of tokens will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



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



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

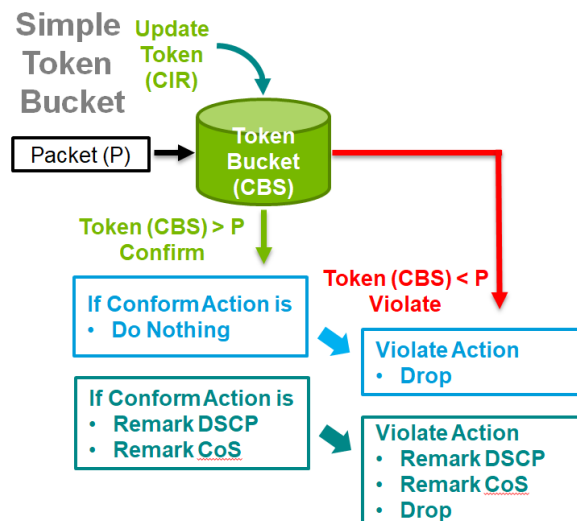


## Simple Token Bucket Concept

In the Simple Token Bucket algorithm, two methods will be used:

**CIR: Committed Information Rate:** Users can pre-configure the CIR. To determine the size of the bucket, they will be sent along with the available tokens. When tokens are unavailable, the packets will not be sent until the tokens are added into the bucket. This guarantees sufficient network bandwidth and efficient flow control.

**CBS: Committed Burst Rate:** The tokens will be saved in both the CBS bucket and EBS bucket. When both buckets are full of tokens, the exceeding tokens will be dropped. This ensures that the specific amount of tokens are available so that the packet transmission can be stable.



# SrTCM (Single Rate Three Color Marker)

## SrTCM Overview

SrTCM stands for A Single Rate Three Color Marker, which is another policing scheme for ingress rate limit. Traffic marking is based on a Committed Information Rate (CIR) and two associated burst sizes, a Committed Burst Size (CBS) and an Excess Burst Size (EBS). A packet is marked green if it does not exceed the CBS, yellow if it does exceed the CBS, but not the EBS, and red otherwise.

## How SrTCM Works

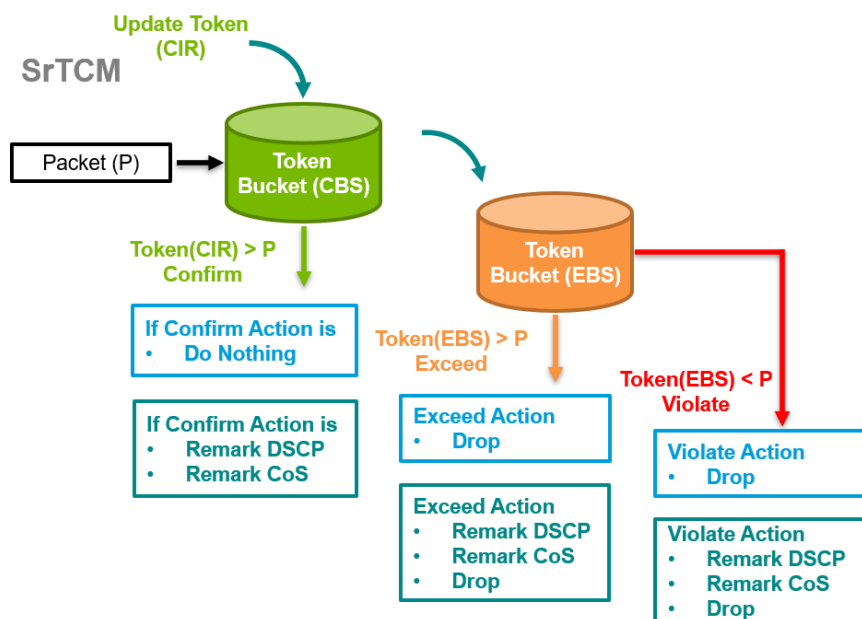
SrTCM will categorize the ingress packet by its length, and mark it as one of three colors:

**Red:** performs the "violate" action.

**Yellow:** performs the "exceed" action. The Token Bucket (EBS) will deduct corresponding tokens.

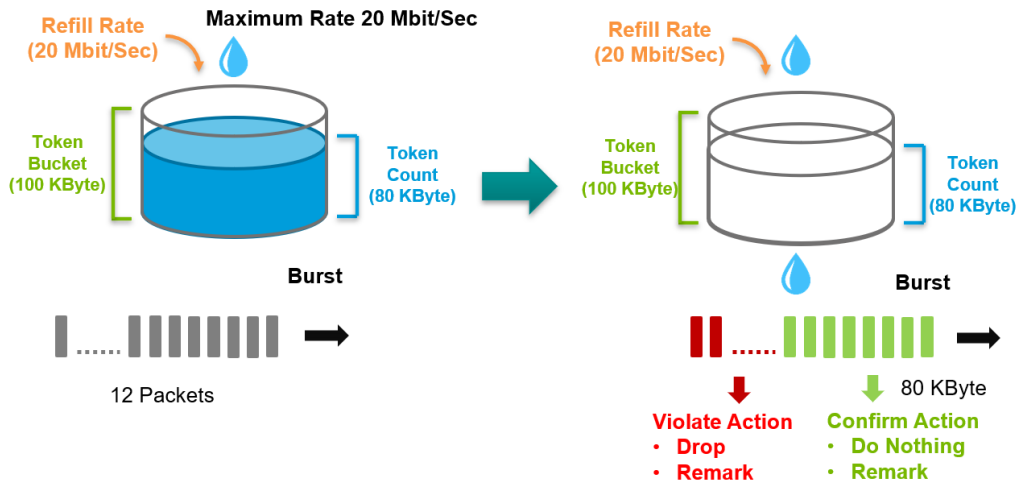
**Green:** performs the "conform" action. The Token Bucket (CBS) will deduct corresponding tokens.

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




## Exceed Rate Limit Threshold Port Shutdown





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



## Editing Ingress Rate Limit

Switch to **Advanced Mode** before configuring the settings in this section.

On the **Ingress Rate Limit** menu, click the **General** tab, and then click the  icon.

Ingress Rate Limit									
General		Port Shutdown							
Port	Type	Ingress Rate (CIR)	CBS	EBS	Mode	Confirm Action	Exceed Action	Violate Action	
	1/1	Simple Token Bucket	1000	1024	1024	Color-Blind	Do Nothing	Drop	Drop
	1/2	Simple Token Bucket	1000	1024	1024	Color-Blind	Do Nothing	Drop	Drop
	1/3	Simple Token Bucket	1000	1024	1024	Color-Blind	Do Nothing	Drop	Drop
	1/4	Simple Token Bucket	1000	1024	1024	Color-Blind	Do Nothing	Drop	Drop

Configure the following settings.

### Edit Port 1/1 Settings

Type \*  
Simple Token Bucket ▼

---

Ingress Rate (CIR) \*  
10000  
1 - 10000 Mbps

CBS \*  
1024  
10 - 10240 KByte

Conform Action \*  
Do Nothing ▼

Violate Action \*  
Drop ▼

Copy Configurations ... ▼ i

CANCEL
APPLY

#### Type

Setting	Description	Factory Default
Simple Token Bucket	Specify Simple Token Bucket as Ingress Limit type.	Simple Token Bucket
SrTCM	Specify SrTCM as Ingress Limit type.	

#### Ingress Rate (CIR) (Mbps)

Setting	Description	Factory Default
1 to 1000	Define the specific incoming data communication speed given to this port.	1000

#### CBS (Committed Burst Size) (Kbyte)

Setting	Description	Factory Default
0 to 10240	Input the specific data communication speed given to this port when the data rate exceeds the CIR rate. The data that exceeded the CIR rate will be saved in temporary storage, and will be sent when bandwidth is available.	1024

#### EBS (Excess Burst Size) (Kbyte)

Setting	Description	Factory Default
0 to 10240	Input the specific data communication speed given to this port when the data rate exceeds the CIR rate. The data that exceeded the CIR rate will be saved in temporary storage, and will be sent when bandwidth is available.	1024

#### Confirm Action

Setting	Description	Factory Default
Do Nothing	Do nothing.	Do Nothing
Remark CoS	Remark the CoS value.	
Remark DSCP	Remark the DSCP value.	



### Violate Action

Setting	Description	Factory Default
Drop	Drop the packet if the packet violates CIR and CBS.	Drop
Remark CoS	Remark the CoS value if the packet is marked as violated.	
Remark DSCP	Remark the DSCP value if the packet is marked as violated.	

### Copy Configurations to Ports

Setting	Description	Factory Default
Select the port(s) from the drop-down list	Copy the configurations to other port(s).	None

When finished, click **APPLY** to save your changes.

## Editing Port Shutdown

To edit the port shutdown configurations, click the **Port Shutdown** tab.

**Ingress Rate Limit**

General | **Port Shutdown**

Port Shutdown \*  
Disabled

Release Interval \*  
60  
0 - 10080 min.

**APPLY**

Configure the following settings.

### Enable

Setting	Description	Factory Default
Enable	Enable the port to be shut down.	Disabled
Disable	Disable the ability for the port to be shut down.	



### Release Interval (min.)

Setting	Description	Factory Default
0 to 10080	Specify the release interval for the port to shut down. 0 means this port will be shut down until manually enabled.	60

When finished, click **APPLY** to save your changes.

## Editing the Port for Port Shutdown

Edit the specific port that you want to edit the port shutdown configurations for.

	Port	Enable	Threshold (Mbps)
	1/1	Disabled	1000
	1/2	Disabled	1000
	1/3	Disabled	1000
	1/4	Disabled	1000

Configure the following settings.


### Edit Port 1/1 Settings

Port Shutdown \*  
 Disabled ▼

---

Threshold \*  
 10000

1 - 10000 Mbps

Copy Configurations ... ▼ 

CANCEL APPLY

### Enable

Setting	Description	Factory Default
Enable	Enable port shutdown for this port.	Disable
Disable	Disable port shutdown for this port.	

### Threshold (Mbps)

Setting	Description	Factory Default
1 to 1000	Specify the threshold for port shutdown	1000

### Copy Configuration to Ports

Setting	Description	Factory Default
Select the port(s) from the drop-down list	Copy the configurations to other port(s).	None

When finished, click **APPLY** to save your changes.

## Scheduler

### Scheduler Overview

Scheduler is an arbiter in switch forwarding path to prioritize traffic flows by users' defined criteria. This essentially enhances data transmission efficiency and guarantees that critical packets can be transmitted earlier. Moxa's switches support two scheduling algorithms: Strict Priority and Weighted Round Robin.


### Strict Priority





The Strict Priority type allows users to determine to transmit packets in the highest priority queue first, while packets with lower priority will be transmitted later. This guarantees that traffic with the highest level of priority for data transmission will go first.

### Weighted Round Robin

The Weighted Round Robin type allows users to give priority to specific packets in the higher weighted queue to ensure those packets will be sent first. Moxa switches now have 8 queues, and the weights from highest to lowest are 8:8:4:4:2:2:1:1.

### Scheduler Settings


Select Scheduler in the menu and then click the  icon on the port you want to configure.

Scheduler		
Port	Type	
 1/1	SP	
 1/2	SP	
 1/3	SP	
 1/4	SP	

Configure the following settings.

#### Edit Port 1/1 Settings

Type \*  
Strict Priority ▼

Copy Configurations ... ▼ 

CANCEL **APPLY**

### Type

Setting	Description	Factory Default
Strict Priority	Set scheduler algorithm as Strict Priority.	Strict Priority
Weighted Round Robin	Set the scheduler algorithm as Weighted Round Robin: The queued packet will be forwarded by its associated weight.	

### Copy Configurations to Ports


Setting	Description	Factory Default
Select the port from the drop-down list	Copy the same settings to other ports.	None

When finished, click **APPLY** to save your changes.





## Egress Shaper Overview

A shaper typically delays excess traffic using a buffer or queueing mechanism to hold packets and shape the flow when the data rate of the source is higher than expected. There are two possible metering algorithms: token bucket, or leaky bucket. The leaky bucket algorithm works similarly to the way an actual leaky bucket holds water: The leaky bucket takes data and collects it up to a maximum capacity. Credit in the bucket is only released from the bucket at a set rate. When the bucket consumes all data, the leaking will stop. If incoming data would overflow the bucket, then the packet is considered to be non-conformant and is not added to the bucket. Data will be added back to the bucket as space becomes available for conforming packets.

## Egress Shaper Settings and Status

This section describes how to configure Egress Shaper. Switch to **Advanced Mode** first and select **Egress Shaper** in the menu and then click the  icon on the port you want to configure.

### Egress Shaper

	Port	Egress Rate (CIR)	CBS
	1/1	1000	1024
	1/2	1000	1024
	1/3	1000	1024
	1/4	1000	1024

Configure the following settings.

### Edit Port 1/1 Settings

CIR \*  
  
1 - 10000 Mbps

CBS \*  
  
10 - 10240 KByte

Copy Configurations ... i

CANCEL
APPLY

**CIR (Committed Information Rate) (Mbps)**

Setting	Description	Factory Default
1 to 1000	The average committed data transmission rate.	1000

**CBS (Committed Burst size) (Kbyte)**

Setting	Description	Factory Default
10 to 10240	The maximum traffic amount (in Kbyte) that can be transmitted within a very short interval of time or burst.	1024

**Copy Configurations to Ports**

Setting	Description	Factory Default
Select the port from the drop-down list	Copy the same settings to the other ports.	None

When finished, click **APPLY** to save your changes.

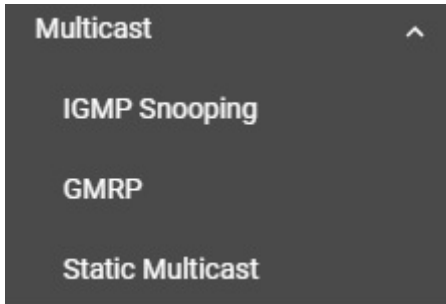
You can view the Egress Shaper status.

### Egress Shaper

	Port	Egress Rate (CIR)	CBS
	1/1	1000	1024
	1/2	1000	1024
	1/3	1000	1024
	1/4	1000	1024

# Multicast

Multicast filtering improves the performance of networks that carry multicast traffic. This section will explain the Layer 2 multicast settings, such as **IGMP Snooping**, **GMRP**, and **Static Multicast**.



## IGMP Snooping

### IGMP Snooping Overview

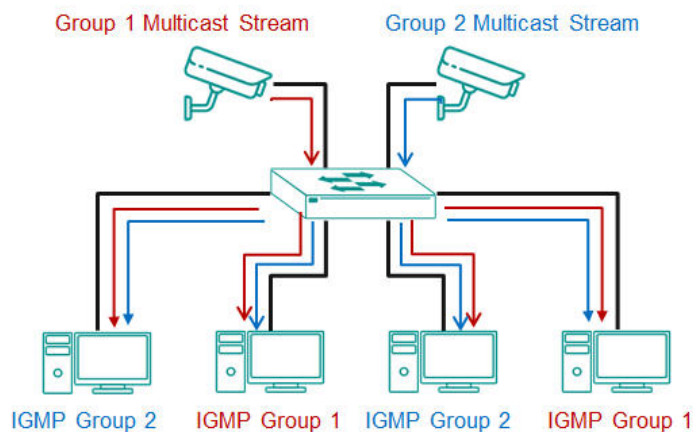
IGMP stands for **Internet Group Management Protocol**, which is a network communication protocol that hosts nearby routers on networks to construct multicast group memberships.

IGMP snooping allows a network switch to listen in on the IGMP conversation between hosts and routers. By listening to these conversations, the switch maintains an association mapping table between port(s) and multicast group.

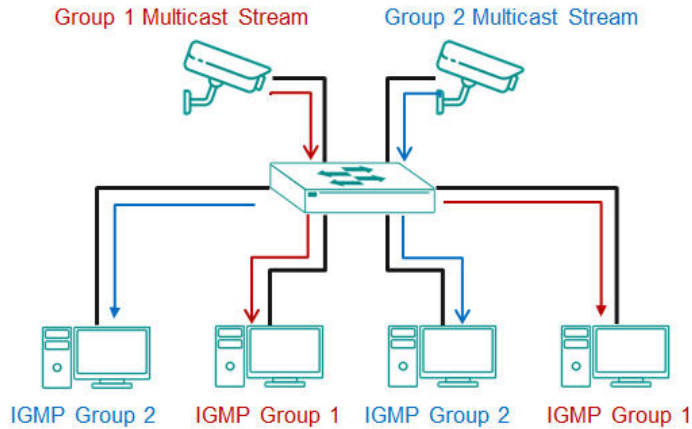
### How IGMP Snooping Works

A switch will, by default, flood multicast traffic to all the other ports, aside ingress, in a broadcast domain (or the VLAN equivalent). Multicast can cause unnecessary loading for host devices by requiring them to process packets they have not solicited. IGMP snooping is designed to prevent hosts on a local network from receiving traffic for a multicast group they have not explicitly joined. It provides switches with a mechanism to forward multicast traffic to specific ports that receive IGMP hosts. Hence, IGMP snooping can utilize the network bandwidth more efficiently.

### Without IGMP Snooping



## With IGMP Snooping



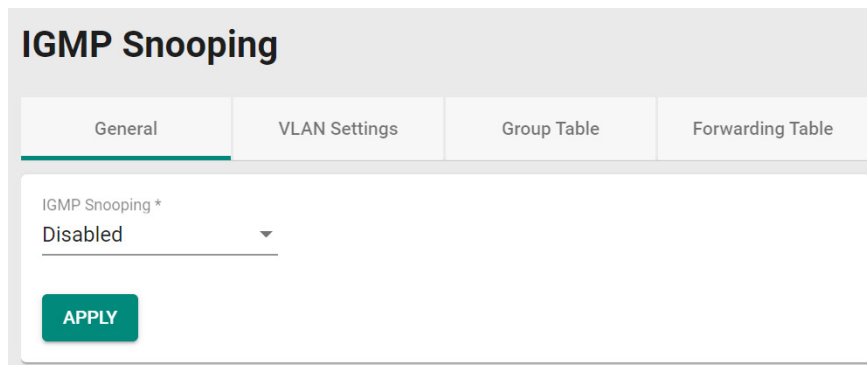
## Differences Between IGMP Snooping V1, V2, and V3

IGMP protocols regulate the communication mechanism between querier and listener. IGMP Snooping has three different versions. Refer to the following table for the detailed differences.

IGMP Version	Main Features	Reference
V1	The IGMPv1 querier will periodically send out a "query". Listeners can solicit a "report" of their interested group. However, IGMPv1 does not have a "leave group" message, and the querier might need to implement a timeout mechanism for each registered group.	RFC-1112
V2	Compatible with V1 and the following functions: 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 if multiple capable queries are present.	RFC-2236
V3	Compatible with V1, V2, and the following functions: Source filtering enables hosts to specify: - the multicast traffic from a specified source - the multicast traffic from any source except a specified source	RFC-3376

## IGMP Snooping Settings

First, select **IGMP Snooping** on the menu and then click the **General** tab on the configuration page.




The screenshot shows the 'IGMP Snooping' configuration page with the 'General' tab selected. The 'IGMP Snooping \*' dropdown menu is set to 'Disabled'. An 'APPLY' button is visible at the bottom left.

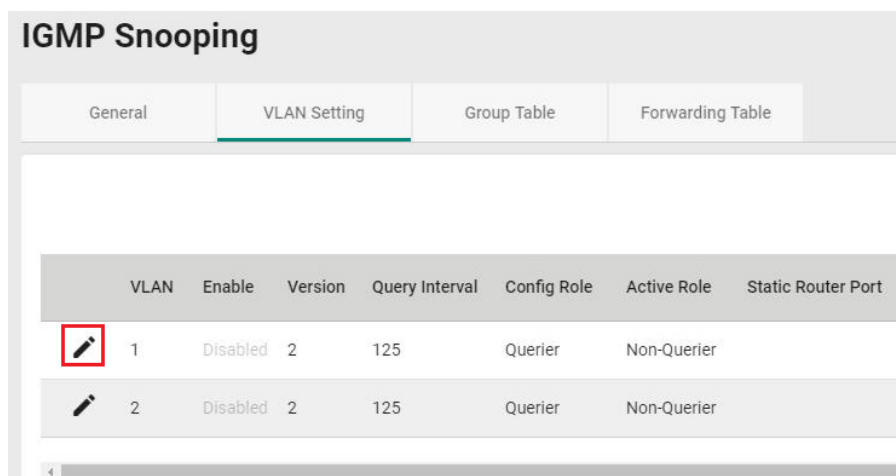
### Enable

Setting	Description	Factory Default
Enabled	Enable IGMP Snooping on a specific VLAN.	Disabled
Disabled	Disable IGMP Snooping on a specific VLAN.	



When finished, click **APPLY** to save your changes.

## Configuring VLAN Setting

Click the **VLAN Setting** tab, and then click the  icon to configure the VLAN settings.



The screenshot shows the 'IGMP Snooping' configuration page with the 'VLAN Setting' tab selected. A table lists VLAN settings for VLAN 1 and VLAN 2. The 'Enable' column for both is 'Disabled'. The 'Query Interval' is 125 for both. The 'Config Role' is 'Querier' and the 'Active Role' is 'Non-Querier' for both. A pencil icon is highlighted in a red box next to the first row.

	VLAN	Enable	Version	Query Interval	Config Role	Active Role	Static Router Port
	1	Disabled	2	125	Querier	Non-Querier	
	2	Disabled	2	125	Querier	Non-Querier	



### Edit VLAN 1 Settings

IGMP Snooping \*  
 Disabled ▼

---

Version \*  
 2 ▼

---

Query Interval \*  
 125  
 20 - 600 sec.

---

Static Router Port ▼

---

Config Role \*  
 Querier ▼

---

CANCEL APPLY

#### **IGMP Snooping**

Setting	Description	Factory Default
Enabled	Enable IGMP Snooping on a switch.	Disabled
Disabled	Disable IGMP Snooping on a switch.	

#### **Version**

Setting	Description	Factory Default
1, 2, 3	Specify the IGMP version of the packets that the switch listens to and send queries for.	2

#### **Query Interval (sec)**

Setting	Description	Factory Default
20 to 600	Specify the query interval for the Querier function globally (Querier has to be enabled.)	125

#### **Static Router Port**

Setting	Description	Factory Default
Check the port from the drop-down list	The router port is the port that connects to the upper level router (or IGMP querier), or to the upper level router of downstream multicast streams. All of the received IGMP signaling packets or multicast streams will be forwarded to those static router ports.	None

#### **Config Role**

Setting	Description	Factory Default
Querier	The switch will act as the Querier role.	Querier
Non-Querier	The switch will not act as the Querier role.	

When finished, click **APPLY** to save your changes.

## Viewing the Group Table

Click the **Group Table** tab, which allows you to view the current Group Table status.

VLAN	Group Address	Filter Mode	Port	Source Address
1	239.255.255.250	Exclude	3/4	0.0.0.0

Refer to the following table for the detailed description for each item.

Item	Description
VLAN	The VLAN ID.
Group Address	The registered multicast group.
Filter Mode	Only applicable for IGMPv3. (v1 and v2 will display "N/A") Include: source-specific multicast address group Exclude: source-specific exclusive multicast address group
Port	The forwarded port.
Source Address	Only applicable for IGMPv3. (v1 and v2 will display N/A)

## Viewing the Forwarding Table

Click the **Forwarding Table** tab to view the current forwarding table.

VLAN	Group Address	Source Address	Port
1	239.255.255.250	192.168.127.1	3/4

Refer to the following table for a description of each item.

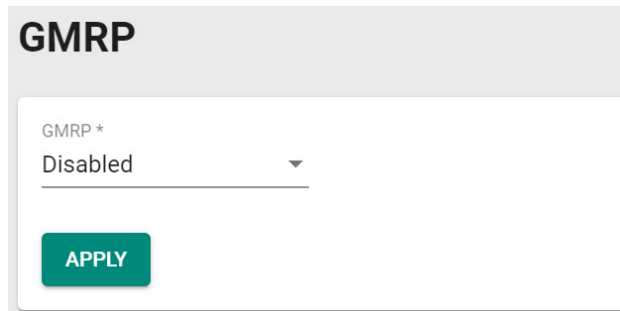
Item	Description
VLAN	The VLAN ID.
Group Address	The associated multicast group address of the streaming data.
Source Address	The source address of the streaming data.
Port	The forwarded port.

## GMRP

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

### Configuring GMRP Setting

To configure the GMRP settings, click **GMRP** on the menu.




Configure the following settings.




#### **GMRP**

Setting	Description	Factory Default
Enabled	Enable GMRP.	Disabled
Disabled	Disable GMRP.	

When finished, click **APPLY** to save your changes.

### Configuring GMRP Settings for Each Port

Next, click the  icon on the port you want to configure.

	Port	Enable	Group Restrict
	1/1	Disabled	Disabled
	1/3	Disabled	Disabled
	1/4	Disabled	Disabled

Configure the following settings.

### Edit Port 1/1 Settings

GMRP \*  
Disabled ▼

Group Restrict \*  
Disabled ▼

Copy Configurations ... ▼ i

CANCEL
APPLY

**GMRP**

Setting	Description	Factory Default
Enabled	Enable GMRP for this port.	Disabled
Disabled	Disable GMRP for this port.	

**Group Restrict**

Setting	Description	Factory Default
Enabled	Enable Group Restrict on the port. This specific port will not process any GMRP control packets.	Disabled
Disabled	Disable Group Restrict on the port. The specific port will receive and process incoming GMRP control packets.	

**Copy Config to Ports**

Setting	Description	Factory Default
Select the port(s) from the drop-down list	Allows you to copy the configurations to other port(s).	None

When finished, click **APPLY** to save your changes.

## Static Multicast

Click **Static Multicast** on the menu to view the current multicast table.

### Adding Static Multicast Entry

To add more tables, click the + icon.

### Static Multicast Table

+
+

	VLAN	MAC Address	Egress Port	Forbidden Port
<input type="checkbox"/>				

Max 256

Configure the following settings.

### Add Static Multicast Entry

VLAN ID \* ▼

---

MAC Address \*

---

Port \* ▼

---

Forbidden Port ▼

---

CANCEL
CREATE

**VLAN ID**

Setting	Description	Factory Default
Input the VID	Specify the multicast group's associated VLAN ID.	None

**MAC Address**

Setting	Description	Factory Default
Input the MAC address	Specify the multicast MAC address.	None

**Port**

Setting	Description	Factory Default
Input the port from the drop-down list	Set the port(s) as an egress port(s) so that multicast streams can be forwarded to this port.	None

**Forbidden Port**

Setting	Description	Factory Default
Input the port from the drop-down list	Set the port as forbidden so that packets cannot be forwarded to this port.	None

When finished, click **CREATE**.

# Network Redundancy

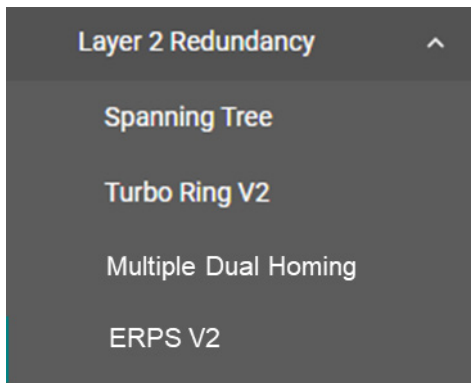
Setting up the Redundancy Protocol on your network helps protect critical links against failure, protects against network loops, and keeps network downtime to a minimum.

The Redundancy Protocol allows you to set up redundant paths on the network to provide a backup data transmission route in the event that a cable or one of the switches is inadvertently disconnected or damaged. This is a particularly important feature for industrial applications, since it can take several minutes to address the link down port or failed switch. For example, if a Moxa switch is used as a key communications device for a production line, several minutes of downtime can cause a big loss in production and revenue. Moxa switches support the following Redundancy Protocol functions:

- **Spanning Tree**
- **Turbo Ring V2**
- **Multiple Dual Homing**
- **ERPS V2**

## Layer 2 Redundancy

First select **Network Redundancy** on the menu and then click **Layer 2 Redundancy**.



# Spanning Tree

## Spanning Tree Overview

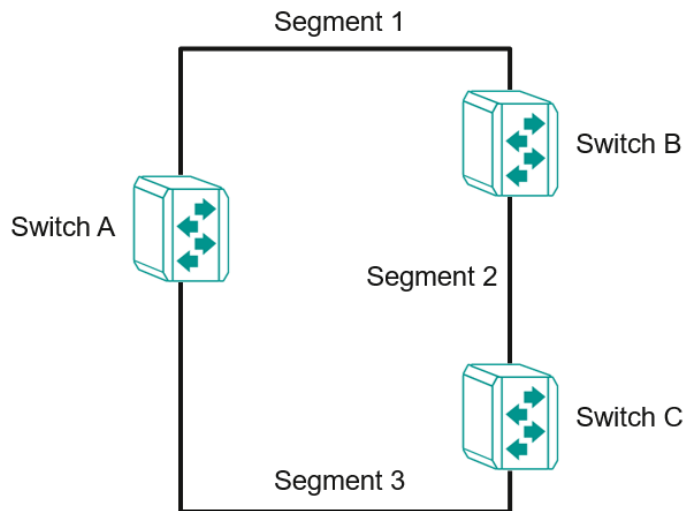
Spanning Tree Protocol (STP) was designed to help construct a loop-free logical topology on an Ethernet network and provide an automatic means of avoiding any network loops. This is particularly important for networks that have a complicated architecture, since unintended loops in the network can cause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

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

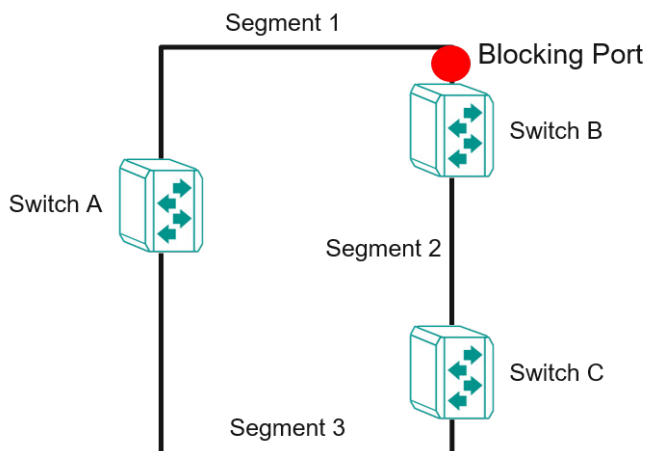
- Locate and then disable less efficient paths (e.g., paths that have lower bandwidth).
- Enable one of the less efficient paths if a more efficient path fails.

## How STP Works

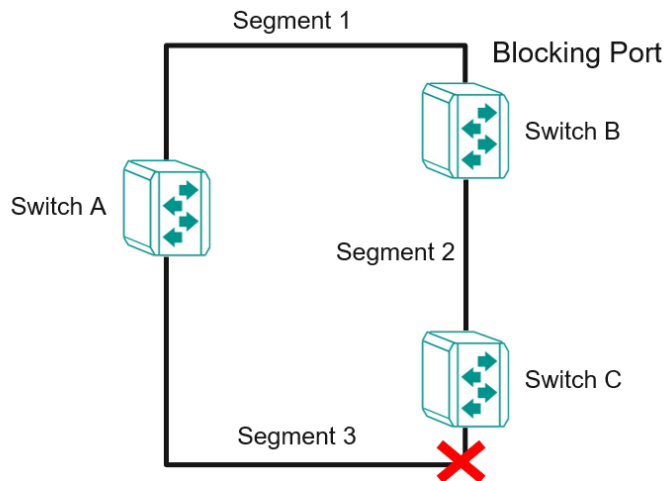
The figure below shows a network made up of three LANs separated by three bridges. Each segment uses at most two paths to communicate with the other segments. Since this configuration can give rise to loops, the network will overload if STP is not enabled.



If STP is enabled, it will detect duplicate paths or block one of the paths from forwarding traffic. In the following example, STP determined that traffic from segment 2 to segment 1 flows through switches C and A since this path is in a forwarding state and is processing BPDUs. However, switch B on segment 1 is in a blocking state.



What happens if a link failure is detected? As shown in the figure below, the STP will change the blocking state to a forwarding state so that traffic from segment 2 flows through switch B to segment 1 through a redundant path.



STP will determine which path between each segment is most efficient, and then assign a specific reference point on the network. When the most efficient path has been identified, the other paths are blocked. In the previous three figures, STP first determined that the path through switch C was the most efficient, and as a result, blocked the path through switch B. After the failure of switch C, STP re-evaluated the situation and opened the path through switch B.

## Difference Between STP and RSTP

RSTP is similar to STP but includes additional information in the BPDUs that allow each bridge to confirm that it has taken action to prevent loops from forming when it decides to enable a link to a neighboring bridge. Adjacent bridges connected via point-to-point links will be able to enable a link without waiting to ensure that all other bridges in the network have had time to react to the change. The main benefit of RSTP is that the configuration decision is made locally rather than network-wide, allowing RSTP to carry out automatic configuration and restore a link faster than STP.

STP and RSTP spanning tree protocols operate without regard to a network's VLAN configuration and maintain one common spanning tree throughout a bridged network. Thus, these protocols map one loop-free, logical topology on a given physical topology.



## STP/RSTP Settings and Status

This section describes how to configure Spanning Tree settings.

### General

Click **Spanning Tree** on the menu and then select the **General** tab.

The screenshot shows the 'Spanning Tree' configuration interface with the 'General' tab selected. The 'STP Mode' dropdown menu is set to 'Disabled'. Below the dropdown is a green 'APPLY' button.

Configure the following settings.

#### STP Mode

Setting	Description	Factory Default
Disabled	Disable Spanning Tree.	Disabled
STP/RSTP	Specify STP/RSTP as the STP mode.	
MSTP	Specify MSTP as the STP mode.	

### STP/RSTP Mode Settings

If you select **STP/RSTP** as the STP mode, configure the following settings.

The screenshot shows the 'Spanning Tree' configuration interface with the 'General' tab selected. The 'STP Mode' is set to 'STP/RSTP', 'Compatibility' to 'RSTP', and 'Bridge Priority' to '32768'. Below these are four input fields: 'Forward Delay Time' (15), 'Hello Time' (2), 'Max. Age' (20), and 'Error Recovery Time' (300). Each field has a range and unit below it. A green 'APPLY' button is at the bottom.

#### STP Mode

Setting	Description	Factory Default
STP/RSTP	Use the STP/RSTP mode as the Spanning Tree protocol.	STP/RSTP

#### Compatibility

Setting	Description	Factory Default
STP	To be compatible with STP mode only	RSTP
RSTP	To be compatible with RSTP and STP modes	

### Bridge Priority

Setting	Description	Factory Default
0 to 61440	Increase this device's bridge priority by selecting a lower number. A device with a higher bridge priority has a greater chance of being established as the root of the Spanning Tree topology.	32768

### Forwarding Delay Time (sec.)

Setting	Description	Factory Default
4 to 30	The amount of time the device waits before checking to see if it should change to a different state.	15

### Hello Time (sec.)

Setting	Description	Factory Default
1 or 2	The root of the Spanning Tree topology periodically sends out a "hello" message to other devices on the network to check if the topology is healthy. The "hello time" is the amount of time the root waits between sending hello messages.	2

### Max Age (sec.)

Setting	Description	Factory Default
6 to 40	If this device is not the root, and it has not received a hello message from the root in the amount of time equal to "Max. Age," then this device will reconfigure itself as a root. Once two or more devices on the network are recognized as a root, the devices will renegotiate a new Spanning Tree topology.	20

### Error Recovery Time (sec.)

Setting	Description	Factory Default
30 to 65535	If the BPDU guard is triggered on a port, it will automatically recover to the normal state after the Error Recovery Time.	300

When finished, click **APPLY** to save your changes.

If you select **MSTP** as the STP mode, configure the following settings.

## Spanning Tree

General   Guard   Status

STP Mode \* MSTP   Compatibility \* MSTP

Forward Delay Time *	Hello Time *	Max. Age *	Error Recovery Time *
15	2	20	300
4 - 30 sec.	1 - 2 sec.	6 - 40 sec.	30 - 65535 sec.
Region Name	Region Revision *	Max. Hops *	
MSTP	0	20	
4 / 32	0 - 65535	6 - 40	

**APPLY**

**STP Mode**

Setting	Description	Factory Default
MSTP	Use the MSTP mode as the Spanning Tree protocol.	MSTP

**Compatibility**

Setting	Description	Factory Default
MSTP	To only be compatible with MTP mode.	MSTP
STP	To only be compatible with STP mode.	
RSTP	To be compatible with RSTP and STP modes.	

**Forwarding Delay Time (sec.)**

Setting	Description	Factory Default
4 to 30	The amount of time the device waits before checking to see if it should change to a different state.	15

**Hello Time (sec.)**

Setting	Description	Factory Default
1 or 2	The root of the Spanning Tree topology periodically sends out a "hello" message to other devices on the network to check if the topology is healthy. The "hello time" is the amount of time the root waits between sending hello messages.	2

**Max Age (sec.)**

Setting	Description	Factory Default
6 to 40	If this device is not the root, and it has not received a hello message from the root in the amount of time equal to "Max. Age," then this device will reconfigure itself as a root. Once two or more devices on the network are recognized as a root, the devices will renegotiate a new Spanning Tree topology.	20

**Error Recovery Time (sec.)**

Setting	Description	Factory Default
30 to 65535	If the BPDU guard is triggered on a port, it will automatically recover to the normal state after the Error Recovery Time.	300

**Region Name**

Setting	Description	Factory Default
0 to 32 characters	Provide the region name.	MSTP

**Region Revision**


Setting	Description	Factory Default
0 to 65535 (characters)	Provide the region revision.	0




**Max. Hops**

Setting	Description	Factory Default
6 to 40	Provide the maximum hops value.	20

When finished, click **APPLY** to save your changes.

## Editing Spanning Tree for a Port

To edit the spanning tree settings for a specific port, click the  icon on the port you want to configure.

	Port	Enable	Edge	Priority	Path Cost	Link Type
	1/1	Disabled	Auto	128	0	Auto
	1/3	Disabled	Auto	128	0	Auto
	1/4	Disabled	Auto	128	0	Auto

Configure the following settings.

### Edit Port 1/1 Settings

Enable \*  
Disabled ▼

Edge \*  
Auto ▼

Priority \*  
128  
0 - 240, multiples of 16

Path Cost \*  
0 ⓘ  
0 - 200000000

Link Type \*  
Auto ▼

Copy Configurations ... ⓘ

CANCEL APPLY

### Enable

Setting	Description	Factory Default
Enabled	Enable Spanning Tree.	Disabled
Disabled	Disable Spanning Tree.	

### Edge

Setting	Description	Factory Default
Auto	Automatically detect to be the edge port.	Auto
Yes	Set as an edge port.	
No	Do not set as an edge port.	

### Priority

Setting	Description	Factory Default
0 to 240 (multiples of 16)	Increase the priority of a port by selecting a lower number. A port with a higher priority has a greater chance of being a root port.	128

### Path Cost

Setting	Description	Factory Default
0 to 20000000	The path cost value will be automatically assigned according to the different port speed if the value is set to zero.	0

### Link Type

Setting	Description	Factory Default
Point-to-point	Set to Point-to-point when port operating in full-duplex mode, such as a switch.	Auto
Shared	Set to Shared when port operating in half-duplex mode, such as a hub.	
Auto	Automatically select Point-to-point or Shared mode.	

### Copy Configurations to Ports

Setting	Description	Factory Default
Select the port(s) from the drop-down list	Copy the configurations to other port(s).	None

Click **APPLY** to finish.

## BPDU Overview

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

### BPDU Guard

BPDU Guard is a protection mechanism that prevents a port from receiving BPDUs. When an RSTP-enabled port receives BPDUs, it will automatically be in the error-disable state, which means the port will in turn switch to Block state. When STP is enabled, all ports are involved in the STP domain, sending and receiving BPDUs. However, when BPDU Guard is enabled, all ports will not receive or send any BPDUs, as all computers and unmanaged switches do not support STP. When BPDU Guard is enabled, all communications will be treated as error-disabled, and the related ports will be blocked, therefore no more data will be sent or received, protecting the network from a loop chain.

### Root Guard

**Root Guard** prevents a designated port role from changing to root port role on reception of superior information.


### Loop Guard

**Loop Guard** prevents temporary loops in a network caused by **non-designated ports** changing to the spanning-tree **forwarding** state due to a link failure in the topology.




### BPDU Filter

**BPDU Filter** prevents a port from sending and processing BPDUs. A BPDU filter enabled port cannot transmit any BPDUs and drop all received BPDU either.

## Configuring BPDU Filter, BPDU/Root/Loop Guard Settings

First click **Spanning Tree** on the menu and then select the **Guard** tab. Next, click the  icon on the port you want to configure.

## Spanning Tree

General	Guard	Status		
Port	BPDU Guard	rootGuard	Loop Guard	BPDU Filter
 1/1	Disabled	Disabled	Disabled	Disabled
 1/3	Disabled	Disabled	Disabled	Disabled
 1/4	Disabled	Disabled	Disabled	Disabled

Configure the following settings.


### Edit Port 1/1 Settings

BPDU Guard \*

Root Guard \*

Loop Guard \*

BPDU Filter \*

Copy Configurations ... 

### ***BPDU Guard***

Setting	Description	Factory Default
Enabled	Enable BPDU Guard.	Disabled
Disabled	Disable BPDU Guard.	



### **NOTE**

To establish a redundant port e.g. it is highly recommended that you do not enable BPDU filter.

### ***Root Guard***

Setting	Description	Factory Default
Enabled	Enable Root Guard.	Disabled
Disabled	Disable Root Guard.	

### Loop Guard

Setting	Description	Factory Default
Enabled	Enable Loop Guard.	Disabled
Disabled	Disable Loop Guard.	

### BDPU Filter

Setting	Description	Factory Default
Enabled	Enable BDPU Filter.	Disabled
Disabled	Disable BDPU Filter.	

### Copy Configurations to Port

Setting	Description	Factory Default
Select the port(s) from the drop-down list	Copy the same settings to other port(s).	None

When finished, click **APPLY** to save your changes.

## Viewing Current Spanning Tree Status

Click the **Status** tab to view the current Spanning Tree status.

## Spanning Tree

- General
- Guard
- Status**

### Root Information

Bridge ID  
32768/00:90:e8:72:56:12

Root Path Cost  
0

Forward Delay Time  
15 (sec.)

Hello Time  
2 (sec.)

Max. Age  
20 (sec.)

### Bridge Information

Bridge ID  
32768/00:90:E8:72:56:12

Running Protocol  
RSTP

Forward Delay Time  
15 (sec.)

Hello Time  
2 (sec.)

Max. Age  
20 (sec.)

In addition, the status for each port will also be shown below.

Port	Edge	Port Role	Port State	Root Path Cost	Path Cost	Link Type	BPDU Inconsistency	Root Inconsist
1/1	No	Disabled	Discarding	0	2000	Point-to-Point	No	No
1/3	No	Disabled	Discarding	0	2000	Point-to-Point	No	No
1/4	No	Disabled	Discarding	0	2000	Point-to-Point	No	No
2/1	No	Disabled	Forwarding	0	20000	Point-to-Point	No	No
2/2	No	Disabled	Discarding	0	20000	Point-to-Point	No	No
2/3	No	Disabled	Discarding	0	20000	Point-to-Point	No	No
2/4	No	Disabled	Discarding	0	20000	Point-to-Point	No	No

Refer to the following table for detailed description of each item.

Item	Description
Port	The port number on this device.
Edge	Show if this port is connected to an edge device.
Port Rule	Root: The port is connected directly or indirectly to the root device. Designated: The port is designated if it can send the best BPDU on the segment to which it is connected. Alternate: The alternate port receives more useful BPDU from another bridge and is the blocked port. Backup: The backup port receives more useful BPDU from the same bridge and is the blocked port. Disabled: The function is disabled.
Port State	Forwarding: The traffic can be forwarded through this port. Blocked: The traffic will be blocked. Disabled: The function is disabled.
Root Path Cost	The total path cost to the root bridge.
Path Cost	The path cost on this link.
Link Type	Edge Port: The port is connected to an edge device. Point-to-Point Non Edge Port: The port is connected to another bridge and is full duplex. Shared Non Edge Port: The port is connected to another bridge and is half duplex.
BPDU Inconsistency	BPDU is received on a port enabled by a BPDU guard.
Root Inconsistency	A port is changed to a root port when enabled by a loop guard.
Loop Inconsistency	A loop is detected on this port by a loop guard.

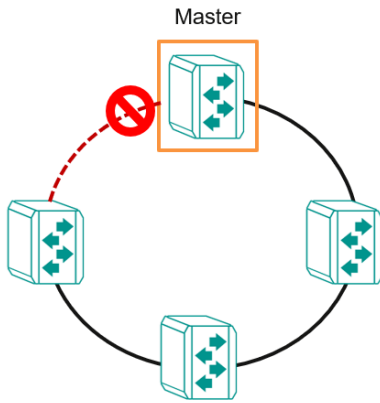
## Turbo Ring v2

### Turbo Ring v2 Overview

Moxa Turbo Ring is a proprietary self-healing technology that enables fast fault recovery of under 20 ms for Fast Ethernet, and 50 ms for Gigabit Ethernet. Turbo Ring supports two topology expansions—ring coupling and dual-ring—to reduce redundant network cabling and network planning costs and to ensure high reliability of your industrial network applications.

The Turbo Ring v2 protocols identify one switch as the **master** of the network, and then automatically block one port beside master on the ring (red line) to avoid network's redundant loops. In the event that one branch of the ring gets disconnected from the rest of the network, the protocol automatically readjusts the ring so that the part of the network that was disconnected can reestablish contact with the rest of the network.



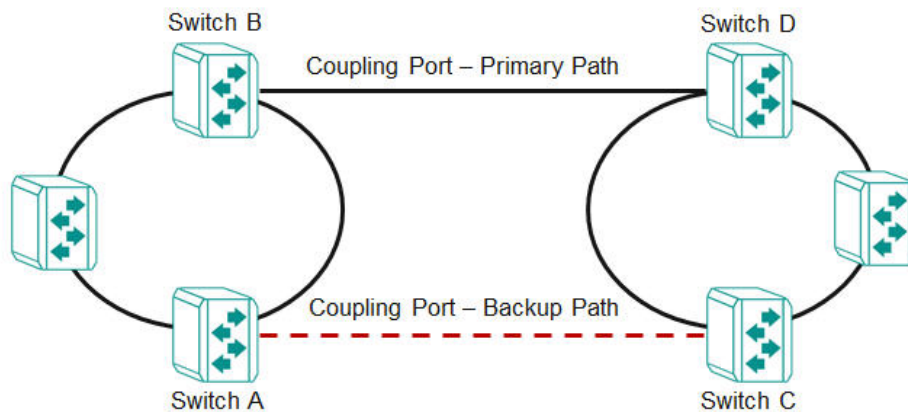


## How Turbo Ring v2 Works

Turbo Ring v2 is an advanced technology for network redundancy, which ensures recovery times of less than 20 ms for Fast Ethernet, and 50 ms for Gigabit Ethernet when the network is down. In addition, it allows more switches within the network rings. Users can select different network typologies for Turbo Ring redundancy to allow more network reliability and reduce cabling costs. Below are three examples of how Turbo Ring v2 works.

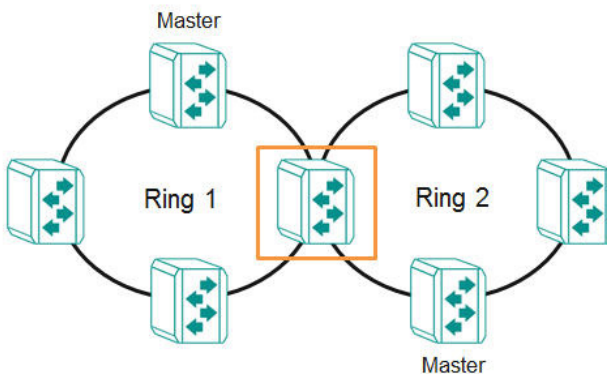
### Ring Coupling

Ring Coupling helps users separate distributed devices into different smaller redundant rings, but in such a way that the smaller rings at different remote sites will be able to communicate with each other. This is useful for applications where some devices are located at remote sites.



### Dual-Ring

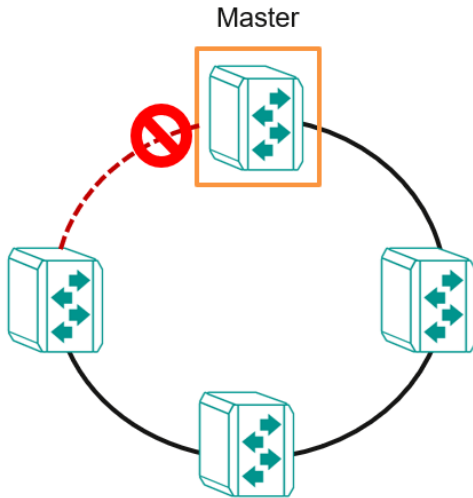
Dual-Ring adds reliability by using a single Moxa switch to connect two separate rings for applications that present cabling difficulties. It provides another ring coupling configuration where two adjacent rings can share one switch. This typology is an ideal solution for applications that have inherent cabling difficulties.



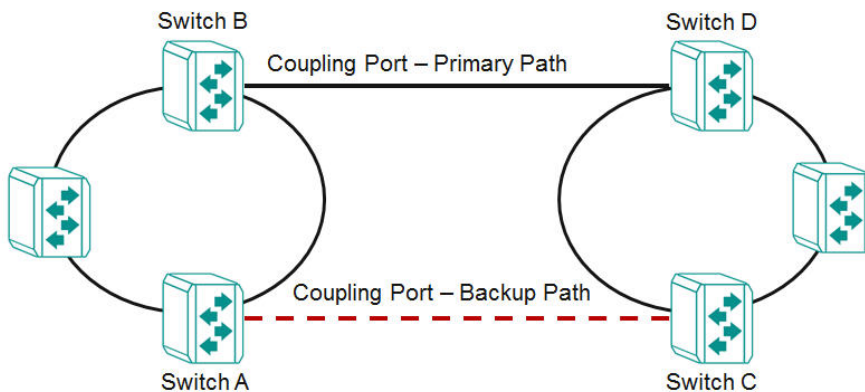
## How to Determine the Redundant Path

For Turbo Ring v2, the master is determined by two methods, one is a system MAC address election, the smallest MAC address will play the Master role; the other is user manual configuration to enable Master role on the switch.

The redundant path is determined by "Ring Port 2", which means the port set on "Ring Port 2" will become the blocking port.



## Ring Coupling for a "Turbo Ring V2" Ring



For Turbo Ring V2, Ring Coupling is enabled by configuring the **Coupling Port (Primary)** on Switch B, and the **Coupling Port (Backup)** on Switch A only.

The **Coupling Port (Backup)** on Switch A is used for the backup path, and connects directly to an extra network port on Switch C. The **Coupling Port (Primary)** on Switch B monitors the status of the main path, and connects directly to an extra network port on Switch D. With ring coupling has been established, Switch A can activate the backup path as soon as it detects a problem with the main path.



### ATTENTION

Ring Coupling needs to be enabled on one coupling primary switch and one coupling backup switch as the Ring Coupler. The Coupler must designate different ports as the two Turbo Ring ports and the coupling port.

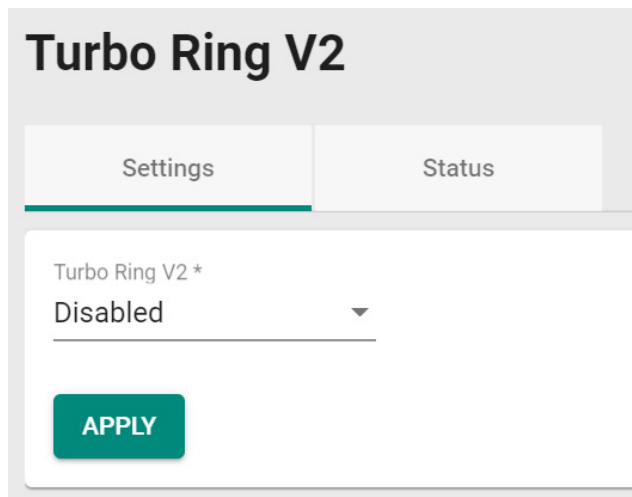


### NOTE

You do not need to use the same switch for both Ring Coupling and Ring Master.

## Turbo Ring V2 Settings and Status

Click **Turbo Ring V2** on the menu, and then select the **Setting** tab.




Configure the following setting.

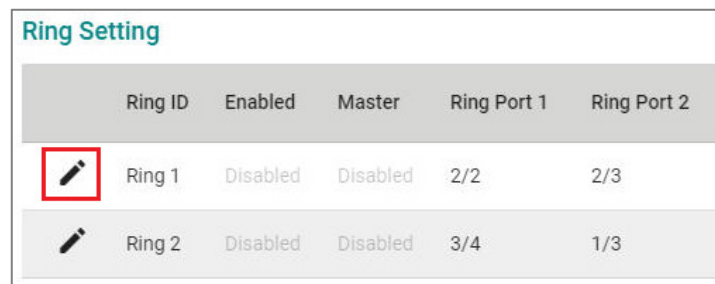
### **Turbo Ring V2**



Setting	Description	Factory Default
Enabled	Enable Turbo Ring V2.	Disabled
Disabled	Disable Turbo Ring V2.	

When finished, click **APPLY** to save your changes.

## Ring Settings

In **Ring Setting**, click the  icon.



Ring ID	Enabled	Master	Ring Port 1	Ring Port 2
 Ring 1	Disabled	Disabled	2/2	2/3
 Ring 2	Disabled	Disabled	3/4	1/3

Configure the following settings. When finished, click **Apply** to save your changes.

### Ring 1 Settings

Enabled \*  
Disabled ▼

Master \*  
Disabled ▼

Ring Port 1 \*  
1/1 ▼

Ring Port 2 \*  
2/2 ▼

CANCEL
APPLY

#### Enable

Setting	Description	Factory Default
Enabled	Enable Ring Setting.	Disabled
Disabled	Disable Ring Setting.	

#### Master

Setting	Description	Factory Default
Enabled	Enable this Ring as the Master.	Disabled
Disabled	Disable this Ring as the Master.	

#### Ring Port 1

Setting	Description	Factory Default
Select the port from the list	Specify this port as the 1st redundant port.	1/1

#### Ring Port 2

Setting	Description	Factory Default
Select the port from the list	Specify this port as the 2nd redundant port.	1/2


## Ring Coupling Overview

Ring Coupling helps users separate distributed devices into different smaller redundant rings, but in such a way that the smaller rings at different remote sites will be able to communicate with each other. This is useful for the applications where some devices are located at remote sites.

### Ring Coupling Settings and Status

In the **Ring Coupling Setting**, click the  icon.

#### Ring Coupling Setting

	Coupling Mode	Enabled	Coupling Port
	Primary Path	Disabled	2/1

Configure the following settings.

### Ring Coupling Settings

Enabled \*  
Disabled ▼

Coupling Mode \*  
Coupling Primary Path ▼

Coupling Port \*  
2/1 ▼

CANCEL
APPLY

**Enable**

Setting	Description	Factory Default
Enabled	Enable Ring Coupling.	Disabled
Disabled	Disable Ring Coupling.	

**Coupling Mode**

Setting	Description	Factory Default
Coupling Backup Path	Select Coupling Mode to assign the coupling port as the backup path.	Coupling Primary Path
Coupling Primary Path	Select Coupling Mode to assign the coupling port as the primary path.	

**Coupling Port**

Setting	Description	Factory Default
Select the port from the list	Select the port as the coupling port.	2/1

When finished, click **APPLY** to save your changes.

## Ring Settings and Ring Coupling Setting Status

Click **Status** in the Turbo Ring V2 menu to view the current Ring settings and the Ring Coupling Status.

### Turbo Ring V2

Setting
Status

#### Ring Status

Ring ID	Master ID	Status	Master	Ring Port 1	Ring Port 2
Ring 1	00:00:00:00:00:00	Disabled	Slave	Disabled	Disabled
Ring 2	00:00:00:00:00:00	Disabled	Slave	Disabled	Disabled

#### Ring Coupling Status

Coupling Mode	Coupling Port
Disabled	Disabled

Refer to the following table for a detailed description for each item of the Ring status.

Item	Description
Ring ID	The ID number of the Ring.
Master ID	The MAC address of the Ring Master.
Status	Healthy: The Ring and the ports are working properly. Break: One or more Rings have been broken.
Master	The device is Master/Slave on this Ring.
Ring Port 1	The port of the first Ring port.
Ring Port 2	The port of the second Ring port.

Refer to the following table for a detailed description for the status of Coupling Mode and Coupling Port.

Item	Description
Coupling Mode	Primary: The main path of Ring Coupling. Backup: The backup path of Ring Coupling.
Coupling Port	The port of the Ring Coupling.

# Multiple Dual Homing

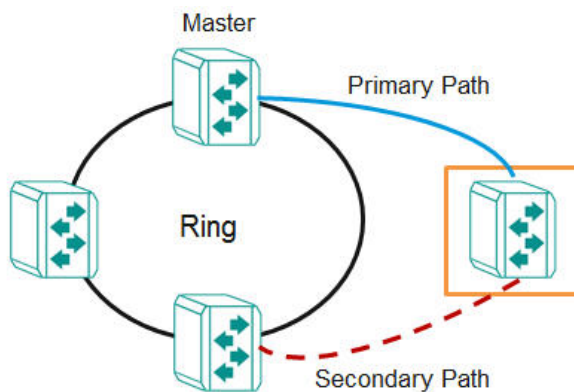
## Multiple Dual Homing Overview

Dual Homing is a layer 2 function, which uses a single Ethernet switch to connect two network topologies, both of which can run any redundancy protocols. It involves coupling two separate devices or even coupling to two separate rings with a single switch connecting to two independent connection points. The secondary path will be activated if the primary path fails. Multiple Dual Homing supports multiple sets of dual homing sessions.

## How Dual Homing Works

Dual Homing is a redundant path technology that allows a single switch to connect to any topology.

The primary and secondary paths require manual configuration: Select a primary port as the primary path and the secondary port as the secondary path. The default path switching mode is "primary path always first", which means when failover occurs, the primary path will switch to the secondary path, but if the primary path recovers, the path will switch back to the primary path again even if the secondary path is healthy.



## Path Switching Mode

There are three path switching modes available:

**Primary path always first:** Always selects the path switching mode as the primary path first. When path switching occurs, the primary path will always be the first path for data communication.

**Maintain current path:** Select the path switching mode to maintain the current path. When path switching occurs, maintain the current path to keep the network stable and do not change paths for data communication.

**Primary path sensing recovery:** Specify the primary path first and switch to the primary path after ensuring the system is ready. When the primary port is connected, it will not switch to the primary port immediately, waiting for system readiness. The path will change directly after 10 mins.

## Dual Homing Settings and Status

Click **Dual Homing** in the menu and select **Settings**.

Configure the following settings.

### Dual Homing

Setting	Description	Factory Default
Enabled	Enable Dual Homing.	Disabled
Disabled	Disable Dual Homing.	

### Primary Port

Setting	Description	Factory Default
Select the port from the list	Specify the port as the primary port.	1/1

### Secondary Port

Setting	Description	Factory Default
Select the port from the list	Specify the port as the secondary port.	1/1

### Path Switching Mode









Setting	Description	Factory Default
Primary path always first	Always selects path switching mode as the primary path first.	Primary path always first
Maintain current path	Always selects the path switching mode to maintain the current path.	
Primary path sensing recovery	Always selects path switching mode as the primary path first but switching path after sensing system ready	

When finished, click **APPLY** to save your changes.



## Dual Homing Settings

In Dual Homing Settings, click the edit icon.

	Session ID	Enabled	Primary Port	Secondary Port
	1	Disabled	1/1	1/2
	2	Disabled	1/3	1/4
	3	Disabled	1/5	1/6
	4	Disabled	1/7	1/8
	5	Disabled	1/9	1/10
	6	Disabled	1/11	1/12
	7	Disabled	1/13	1/14
	8	Disabled	1/15	1/16

Configure the following settings.

### Edit Session 1 Settings

Enabled \*  
Disabled ▼

Primary Port \*  
1/1 ▼

Secondary Port \*  
1/2 ▼

CANCEL APPLY

### Enabled

Setting	Description	Factory Default
Enabled	Enable the session.	Disabled
Disabled	Disable the session.	

### Primary Port

Setting	Description	Factory Default
Select the port from the list	Specify the primary port.	Session 1: 1/1 Session 2: 1/3 Session 3: 1/5 Session 4: 1/7 Session 5: 1/9 Session 6: 1/11 Session 7: 1/13 Session 8: 1/15

### Secondary Port

Setting	Description	Factory Default
Select the port from the list	Specify the secondary port.	Session 1: 1/2 Session 2: 1/4 Session 3: 1/6 Session 4: 1/8 Session 5: 1/10 Session 6: 1/12 Session 7: 1/14 Session 8: 1/16

When finished, click **APPLY** to save your changes.

### Status

Click the **Status** tab to view the detailed status of each Dual Homing session.

#### Dual Homing

Settings
Status

↻
🔍 Search

Session ID	Primary Port	Primary Link Status	Primary Port Status	Secondary Port	Secondary Link Status	Secondary Port Status
1	1/1	Link Down	Disabled	1/2	Link Down	Disabled
2	1/3	Link Down	Disabled	1/4	Link Down	Disabled
3	1/5	Link Down	Disabled	1/6	Link Down	Disabled
4	1/7	Link Down	Disabled	1/8	Link Down	Disabled
5	1/9	Link Down	Disabled	1/10	Link Down	Disabled
6	1/11	Link Down	Disabled	1/12	Link Down	Disabled
7	1/13	Link Down	Disabled	1/14	Link Down	Disabled
8	1/15	Link Down	Disabled	1/16	Link Down	Disabled

Refer to the following table for a detailed description of each item.

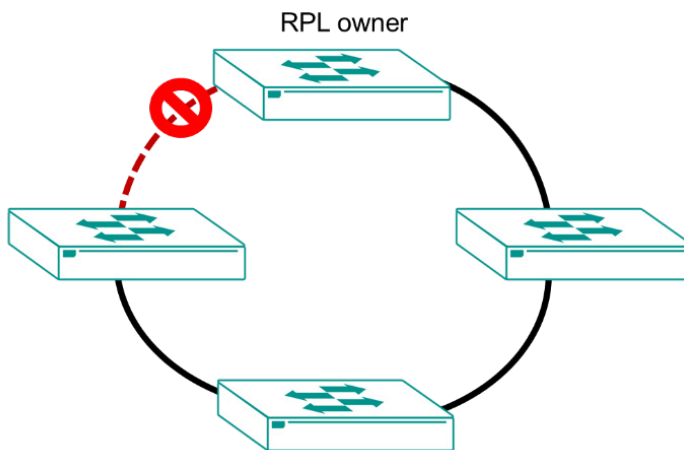
Item	Description
Session ID	The ID number of the Session.
Primary Port	The port used as the primary path.
Primary Link Status	Link Up: The port is connected. Link Down: The port is disconnected.
Primary Port Status	Forwarding: The port is forwarding traffic. Blocking: The port is blocking traffic. Disabled: The function is disabled. Learning: The port is not ready and transitioning to next status (primary path sensing recovery mode)
Secondary Port	The port that is used as the secondary path.
Secondary Link Status	Link Up: The port is connected. Link Down: The port is disconnected.
Secondary Port Status	Forwarding: The port is forwarding traffic. Blocking: The port is blocking traffic. Disabled: The function is disabled.

## ERPS V2

### ERPS V2 Overview

The G.8032 Ethernet Ring Protection (ERP) protocol was defined in ITU-T G.8032 was designed to protect network loops in ring topology by blocking ports. ERPV2 is an open protocol that provides accelerated redundant path switching in the event of a link failure in industrial environments. ERPS supports multi-ring and ladder network topologies to easily expand networks with lower network cabling and planning costs.

In ERPS networks, one switch will be identified as the **RPL owner**, which acts as the primary. It blocks a port to form an RPL(Ring Protection Link) as a redundant link (red line in below figure). When one of links disconnects from the rest of the network, ERPS will automatically readjust the ring and switch to a redundant link.



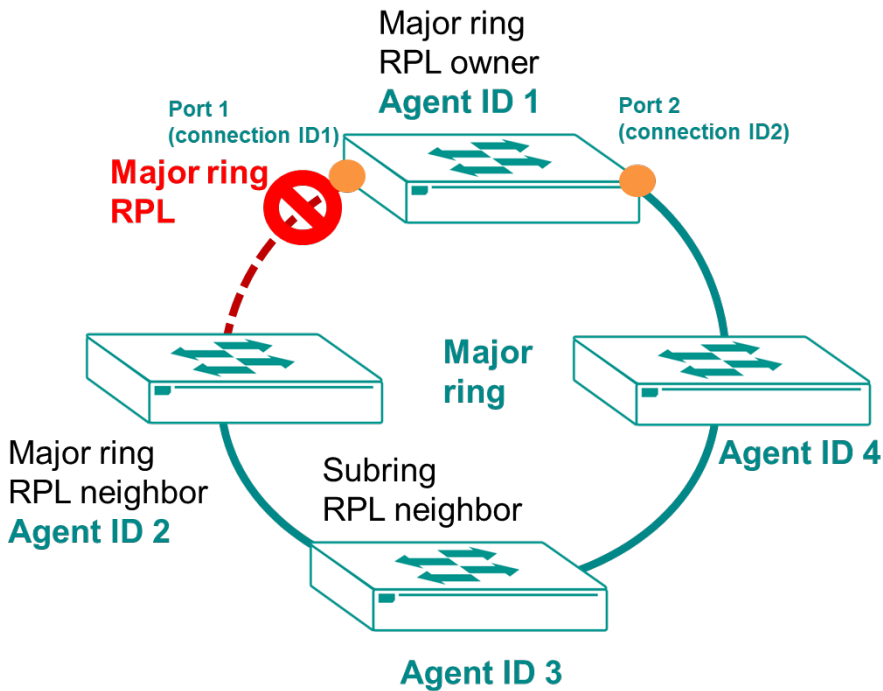
ERPS function is disabled by default. Enabling ERPS should be done on every switch in the same topology for proper operation.

The ERPS function includes the following features:

- **Major Ring:** domain type to form a ring topology.
- **Revertive/ Non-revertive mode:** action after the failed link recovers. In revertive mode, RPL link will return to backup link after failed link recovers and the other is opposite.
- **Forced Switch (FS) and Manual Switch (MS):** administrative commands for blocking a particular ring port.

## How ERPS V2 works

ERPS V2 is an open protocol to form a ring topology by multiple ethernet ring nodes for network redundancy.



## How to Determine the Redundant Path

For ERPS V2, the user must determine and manually configure role of nodes and ring port including to form a ERPS ring.

RPL roles consist of the following:

**RPL owner:** Blocks an RPL port to form a RPL for a loop-free network. Limited to one RPL owner per ring. Another link fails, the RPL owner will unblock the RPL ports to maintain stable network communication.

**RPL neighbor:** a node is adjacent to the RPL owner on the blocked RPL port. The blocked RPL port becomes active when other ports go down.

To simplify ERPS ring settings, this feature provides an **Agent ID** and a **Connection ID** for establishing the connection between each node. While creating an ERPS ring, Connection ID will be automatically assigned by Moxa switch and the Agent ID is user-specified.

## Revertive mode

In ERPS **Revertive mode**, when a downed link recovers, the RPL will return to original blocked status as a backup link. In some cases, there may be no advantage in reverting to the original configuration. In these cases, users can choose to use **Non-revertive mode** to avoid further traffic interruption by switching back.

ERPS V2 also supports switch commands to manually block ports for maintenance. There are three basic commands:

**Force switch (FS):** Executed with the highest priority, this command forcibly blocks the specified ring port to accommodate immediate needs.

**Manual switch (MS):** A lower priority command that manually blocks the specified ring port. This command will have no effect when link failure occurs.

**Clear:** Performs the following operations:

- Clears an existing FS or MS command on the ring ports.
- Clears a non-revertive mode condition at the ring protection link.
- Forces RPL owner ignore the WRT timer and switch traffic to the recovered link.

## R-APS messages overview

R-APS (Ring Automatic Protection Switching) messages are control messages that coordinate switching activities in ERPS rings. They are used to communicate with the RPL owner in the event of a link failure or recovery event. To avoid unnecessary switching processes or to wait for a stable link condition, the ERPS function offers the following timer options:

- **WTR timer:** The Wait-To-Restore (WTR) timer causes the RPL link owner to wait until the network stabilizes before blocking the RPL port. It will be triggered when RPL owner receives an R-APS (NR) control message which means that failed link is restored.
- **Guard timer:** Prevents receiving outdated R-APS messages and processing unnecessary state changes. Triggered on all nodes upon receipt of R-APS messages. The node will not process R-APS messages until the guard timer expires to avoid unexpected network impacts.

## Control VLAN

Distinct from Data VLANs, a control VLAN is used for transmitting R-APS PDUs. Each ERPS ring must be configured with a control VLAN ID, which should be distinct from VLAN IDs used by other ERPS rings.

## ERPS V2 Settings

This section describes how to set up ERPS V2 and corresponding features.

Click **ERPS V2** on the menu, and then click the **Settings** tab.

The screenshot shows the 'ERPS V2' configuration interface. It features two tabs: 'Settings' and 'Status'. The 'Settings' tab is active. Below the tabs, there are three configuration items: a dropdown menu for 'ERPS V2 \*' currently set to 'Enabled', a text input field for 'ERPS V2 Agent ID \*' containing the number '1', and a range indicator '1 - 128'. An 'APPLY' button is located at the bottom left of the settings area.

### ERPS V2


Setting	Description	Factory Default
Enabled	Enable ERPS V2 function	Disabled
Disabled	Disable ERPS V2 function	

### ERPS V2 Agent ID

Setting	Description	Factory Default
1 to 128	Input a value as a specific ID for the local device in ERPS	None

To apply the settings, configure the following parameters.

## ERPS Ring settings

To configure ERPS settings, click the  icon.

### ERPS Ring List




<input type="checkbox"/>	Ring ID ↑	Status	Domain	Control VLAN ID
<input type="checkbox"/>	1	Enabled	Major Ring	1

Configure following settings:

### Edit ERPS V2 Ring 1 Settings

Ring ID \*  
  
1 - 4096

Status \*

Domain  
 

Control VLAN ID \*

**Ring Port 1 Settings**

Ring Port 1  
  
1 - 128

Connection ID 1  
  
1 - 36

Neighbor ERPS V2 Agent ID 1  
  
1 - 128

Neighbor Connection ID 1  
  
1 - 36

**Ring Port 2 Settings**

Ring Port 2  
  
1 - 128

Connection ID 2  
  
1 - 36

Neighbor ERPS V2 Agent ID 2  
  
1 - 128

Neighbor Connection ID 2  
  
1 - 36

Ring Role \*

RPL Port \*

**Advanced Settings**

Revertive Mode \*

Guard Timer \*  
  
10 - 2000, multiple of 10 ms

WTR Timer \*  
  
1 - 12 min.

Switch Command \*

Switch Port \*

CANCEL

APPLY

**Ring ID**

Setting	Description	Factory Default
1 to 4096	Specifies the ID number of the ring.	None

**Status**

Setting	Description	Factory Default
Enabled	Enables selected ERPS ring	Disabled
Disabled	Disables selected ERPS ring	

**Control VLAN ID**

Setting	Description	Factory Default
Select the ID from the list	Select the VLAN ID to serve as the ERPS control VLAN ID.	1

**Ring Port 1**

Setting	Description	Factory Default
Select the port from the list	Specify the primary redundant port.	None

**Neighbor ERPS V2 Agent ID 1**

Setting	Description	Factory Default
1 to 128	Enter the Neighbor ID which is adjacent to the local agent and connects to ring port 1.	None

**Ring Port 2**

Setting	Description	Factory Default
Select the port from the list	Specify a secondary redundant port.	None

**Neighbor ERPS V2 Agent ID 2**

Setting	Description	Factory Default
1 to 128	Enter the Neighbor ID adjacent to the local agent and connect to ring port 2.	None

**Ring Role**

Setting	Description	Factory Default
None	Specify the role of the selected node.	None
RPL Owner	Specify which Ethernet node serves as RPL owner and blocks RPL ports.	
RPL Neighbor	Specify the Ethernet node to serve as RPL Neighbor and block the end of the RPL.	

**RPL Port (for RPL owner and RPL neighbor)**

Setting	Description	Factory Default
Select the port from the list	Specify the port to be blocked by the RPL port.	None

**Revertive Mode (Advanced mode only)**

Setting	Description	Factory Default
Revertive	Return to blocking RPL on recovery of failed link.	Revertive
Non-revertive	Keep RPL unblocked on recovery of failed link.	

**WTR Timer (min) (Advanced mode only)**

Setting	Description	Factory Default
1-12	Choose how long the RPL owner will wait when receiving a R-APS message concerned failed link recovery.	5


**Switch Command (Advanced mode only)**

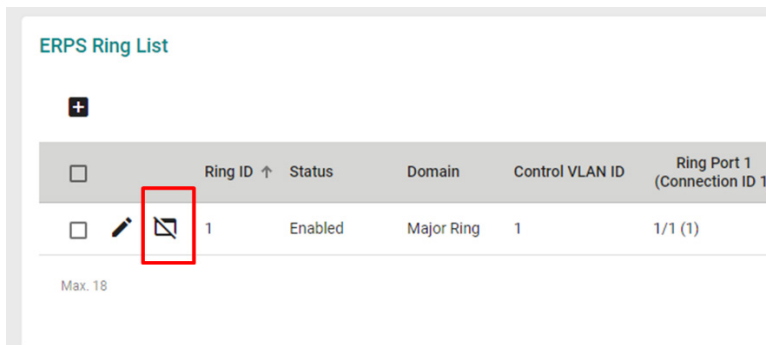
Setting	Description	Factory Default
None	Clear status without any manually blocking ports.	None

Setting	Description	Factory Default
Forced	Force blocking of specified ports, even when the ERPS ring is not idle.	
Manual	Block specified ports when the ERPS ring is idle.	

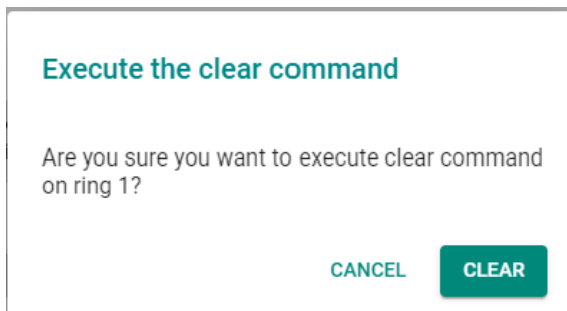
**Switch Port (For forced and manual command) (Advanced mode only)**

Setting	Description	Factory Default
Select the port from the list	Specify the port to block with the switch command.	None

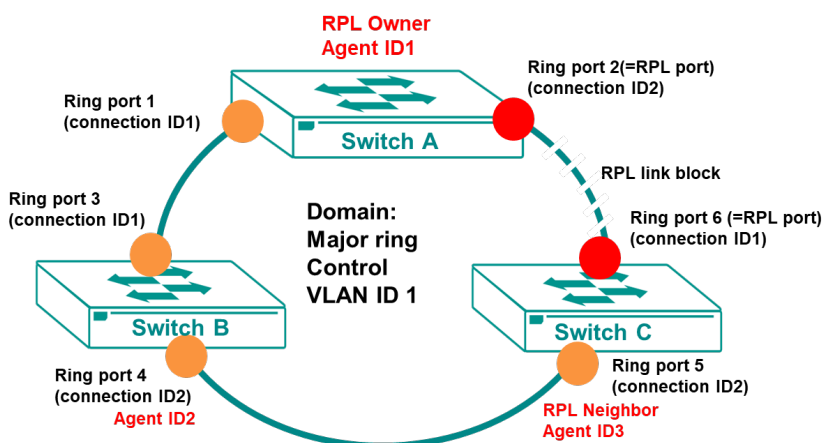
To execute the clear command, click the  icon.



Then, click the clear to confirm executing the clear command.



To configure ERPS ring, users need to consider the entire ring structure and decide the switch role in each ring. The following provides an example of a Major Ring:



The following are the configuration steps:

**To configure Switch A as the RPL owner of the Major ring in this example scenario, do the following:**

1. Determine Agent ID 1 for the Major ring, ensuring it is unique within the ring.



2. Enable the ERPS V2 feature and create an ERPS V2 ring.
3. Assign Ring ID 1 to the ring.
4. Set the Ring Status to **Enabled**.
5. Specify control VLAN ID 1
6. Configure Ring Port 1:  
Choose a port for ring port 1 (Ex. Port 1) and set **Neighbor Agent ID** as 2 and Neighbor connection ID 1, according to the example scenario.
7. Ring Port 2 settings:  
Choose a port for ring port 2 (Ex. Port 2) and set the **Neighbor Agent ID** as 3 and Neighbor connection ID 1, following the example scenario.
8. Set Ring role as **RPL Owner**.
9. Set RPL port to ring port 2.

**To configure Switch C as the RPL neighbor of Major ring for this example scenario.**

1. Determine Agent ID 3.
2. Enable the ERPS V2 feature and create 2 ERPS V2 rings.
3. Assign Ring ID 1 to the ring.
4. Set the Ring Status to **Enabled**.
5. Specify control VLAN ID 1
6. Ring Port 1 Settings:  
Choose a port for ring port 1 (Ex. Port 5) and set **Neighbor Agent ID** as 2 and **Neighbor connection ID 2** according to the example scenario.
7. Ring Port 2 Settings:  
Choose a port for ring port 2 (Ex. Port 6) and set **Neighbor Agent ID** as 1 and **Neighbor connection ID 2** according to the example scenario.
8. Set Ring role as **RPL Neighbor**.
9. (optional) Set the **RPL port** to ring port 2.

**To configure Switch B as member of Major ring for this example scenario.**

1. Determine the Agent ID 2 for both Major ring.
2. Enable the ERPS V2 feature and create 2 ERPS V2 rings.
3. Assign Ring ID 1 to the ring.
4. Set the Ring Status to **Enabled**.
5. Specify control VLAN ID 1.
6. Ring Port 1 Settings:  
Choose a port for ring port 1(Ex. Port 3) and set **Neighbor Agent ID** as 1 and **Neighbor connection ID 1** according to the example scenario.
7. Ring Port 2 Settings:  
Choose a port for ring port 2(Ex. Port 4) and set **Neighbor Agent ID** as 3 and **Neighbor connection ID 2** according to the example scenario.
8. Set Ring role to **None**.

Click the **Status** tab to view the detailed status of ERPS V2 ring status and port status.

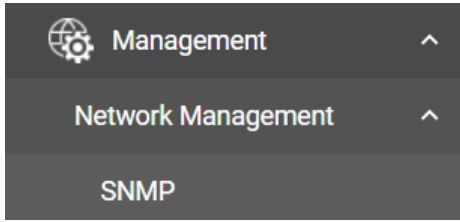
Settings	Status			
<b>ERPS V2 Ring Status</b>				
↻				
Ring ID	Ring State	Ring Role	Remaining Guard Timer (ms)	Remaining WTR Timer (min.)
1	Protection	RPL Owner	500	5
Max. 18				
<b>ERPS V2 Ring Port Status</b>				
↻				
Ring ID	Ring Port	Link Status	Port State	VLAN ID
1	1/1	Link Up	Forwarding	1
	1/2	Link Down	Blocking	1
Max. 18				

Refer to the following table for detailed description of each item:

Item	Description
Ring ID	The ID number of the Ring.
Ring State	Idle: Stable state which means the ring is working normally Protection: A failure occurred in the ring and the RPL link is unblocked. Pending: Transiting from previous state. FS: Force command executing in the ring. MS: Manual command executing in the ring.
Ring Role	RPL owner: Node responsible for blocking the port and forming the RPL. RPL neighbor: Node adjacent to the RPL owner and blocking the port at the end of RPL. None: Members of the ERPS ring with forwarding ports.
Remaining Guard Timer (ms)	Shows the duration of time left on the Guard Timer.
Remaining WTR Timer (ms)	Shows the duration of time left on the WRT timer.
Ring Port	Ports of the ERPS ring.
Link Status	Link Up: The link is active. Link Down: The link is inactive.
Port State	Forwarding: The traffic can be forwarded through this port. Blocked: The port will not forward traffic.
VLAN ID	Represent the VLAN ID that the ERPS ring port joined.

# Management

This section describes how to configure **Network Management** including **SNMP**.



## Network Management

This section demonstrates how to configure SNMP settings. For SNMP Trap/Inform settings, refer to **SNMP Trap/Inform** section under **Diagnostics → Log & Event Notifications**.

### SNMP

Moxa switches support 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. You can also enable data encryption to enhance data security.

Supported SNMP security modes and levels are shown in the table below. 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	None	No	No	Uses an account with admin or user to access objects.
	MD5 or SHA	Authentication based on MD5 or SHA	Disabled	Uses authentication based on HMAC-MD5, or HMAC-SHA algorithms. 8-character passwords are the minimum requirement for authentication.
	MD5 or SHA	Authentication based on MD5 or SHA	Data encryption key: DES, AES	Uses authentication based on HMAC-MD5 or HMAC-SHA algorithms, and data encryption key. 8-character passwords and a data encryption key are the minimum requirements for authentication and encryption.



#### NOTE

SNMPv3 enhances security as it includes authentication and data privacy. If users require a higher level of security, it is recommended to install additional security mechanisms such as a firewall to protect a critical infrastructure.

## General Settings

First click **SNMP** on the menu and then click **General**.

**SNMP**

General    SNMP Account

SNMP Version \*  
V1, V2c

Read Community \*  
public  
At least 4 characters    6 / 32

Read/Write Community \*  
private  
At least 4 characters    7 / 32

**APPLY**

Configure the following settings.

### **SNMP Version**

Setting	Description	Factory Default
V1, V2c, V3	Specify V1, V2c, and V3 as the SNMP version.	V1, V2c
V1, V2c	Specify V1 and V2c as the SNMP version.	
V3 only	Specify V3 as the SNMP version.	

### **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

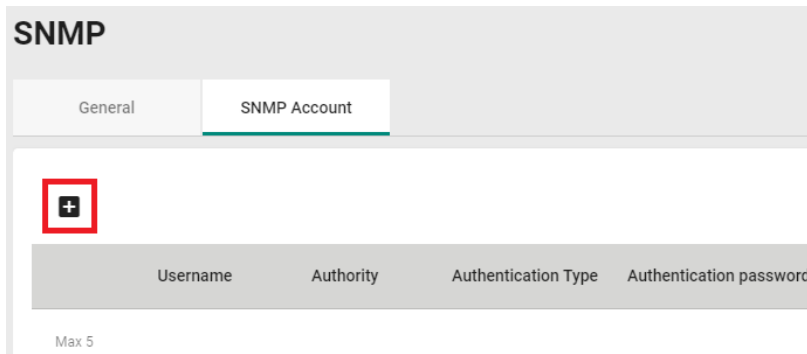
### **Read/Write Community**

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

When finished, click **APPLY** to save your changes.

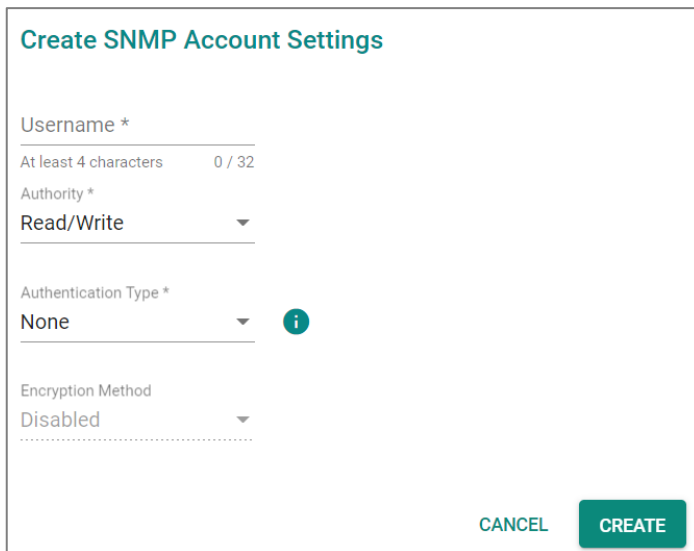
## Creating an SNMP Account

Click **SNMP** on the menu and then click the **SNMP Account**. Next click the  icon on the page.



The image shows the 'SNMP' configuration page with the 'SNMP Account' tab selected. A red box highlights a plus icon in the top left corner. Below the tab, there are four columns: 'Username', 'Authority', 'Authentication Type', and 'Authentication password'. A 'Max 5' label is visible at the bottom left of the table area.

Configure the following settings.



The image shows the 'Create SNMP Account Settings' form. It includes the following fields:
 

- Username \***: A text input field with a character count of '0 / 32' and a note 'At least 4 characters'.
- Authority \***: A dropdown menu currently set to 'Read/Write'.
- Authentication Type \***: A dropdown menu currently set to 'None', with an information icon (i) to its right.
- Encryption Method**: A dropdown menu currently set to 'Disabled'.

 At the bottom right of the form are 'CANCEL' and 'CREATE' buttons.

### **Username**

Setting	Description	Factory Default
At least 4 characters, (max. 32 characters)	Input a username.	None

### **Authority**

Setting	Description	Factory Default
Read Write	The user has read/write access.	None
Read Only	The user only has read access.	

### **Authentication type**

Setting	Description	Factory Default
None	No authentication will be used.	None
MD5	MD5 is the authentication type.	
SHA	SHA is the authentication type.	

### **Authentication password**

Setting	Description	Factory Default
8 to 64 characters	Input the authentication password.	None

### **Encryption Method**


Setting	Description	Factory Default
Disabled	Disable the encryption method.	None
DES	DES is the encryption method.	
AES	AES is the encryption method.	

### Encryption Key


Setting	Description	Factory Default
8 to 30 characters	Enable data encryption.	None

When finished, click **CREATE**.

### Deleting an Existing SNMP Account

To delete an existing SNMP account, select the  icon on the account.



	Username	Authority	Authentication Type
 	test	Read Write	None

Max 5

Click **DELETE** to delete the SNMP account.

### Delete Account

Are you sure you want to delete the selected account?

**CANCEL** **DELETE**

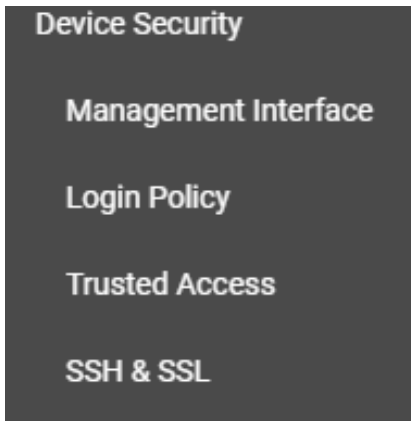
# Security

This section describes how to configure **Device Security**, **Network Security**, and **Authentication**.



## Device Security

This section includes information about the **Management Interface**, **Login Policy**, **Trusted Access**, and **SSH & SSL** configurations.



## Management Interface

This section describes the settings for **User Interface**, **Hardware Interfaces**, and **LCM Interface**.



## User Interface

Click **User Interface** on the menu.

### User Interface

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

APPLY

Configure the following settings.

### HTTP

Setting	Description	Factory Default
Enabled	Enable the HTTP connection.	Enabled
Disabled	Disable the HTTP connection.	



### NOTE

An HTTP session will be redirected to HTTPS if both HTTP and HTTPS are enabled.

### HTTP – TCP Port

Setting	Description	Factory Default
0 to 47808	Specify the HTTP connection port number.	80

### HTTPS

Setting	Description	Factory Default
Enabled	Enable the HTTPS connection.	Enabled
Disabled	Disable the HTTPS connection.	



### **HTTPS – TCP Port**

Setting	Description	Factory Default
1 to 65535	Specify the HTTP connection port number.	443

### **Telnet**

Setting	Description	Factory Default
Enabled	Enable a Telnet connection.	Enabled
Disabled	Disable a Telnet connection.	

### **Telnet – TCP Port**

Setting	Description	Factory Default
1 to 65535	Specify the Telnet connection port number.	23

### **SSH**

Setting	Description	Factory Default
Enabled	Enable the SSH connection.	Enabled
Disabled	Disable the SSH connection.	

### **SSH – TCP Port**

Setting	Description	Factory Default
1 to 65535	Input the SSH connection port number.	22

### **SNMP**

Setting	Description	Factory Default
Enabled	Enable the SNMP connection.	Disabled
Disabled	Disable the SNMP connection.	

### **SNMP – UDP Port**

Setting	Description	Factory Default
0 to 47808	Input the SNMP UDP connection port number.	161



## **NOTE**

Moxa Service is only for Moxa network management software suite.

### **Moxa Service (Encrypted) – TCP Port**

Setting	Description	Factory Default
443 (read only)	Enable a Moxa Service TCP port.	443

### **Moxa Service (Encrypted) – UDP Port**

Setting	Description	Factory Default
40404 (read only)	Enable a Moxa Service UDP port.	40404

### **Maximum number of Login Sessions for HTTP+HTTPS**

Setting	Description	Factory Default
1 to 10	Specify the maximum amount of HTTP login sessions that can happen at the same time.	5

### **Maximum number of Login Sessions for Telnet+SSH**

Setting	Description	Factory Default
1 to 5	Specify the maximum amount of Telnet login sessions that can happen at the same time.	1

When finished, click **APPLY** to save your changes.

## Hardware Interface

Click **Hardware Interface** on the menu.

**Hardware Interfaces**

USB Interface \*  
Enabled

MicroSD Interface \*  
Enabled

Out of Band Interface \*  
Enabled

LCM Interface \*  
Disabled

APPLY

Configure the following settings.

### **USB Interface**

Setting	Description	Factory Default
Enabled	Enable the USB interface on the switch.	Enabled
Disabled	Disable the USB interface on the switch.	

### **MicroSD Interface**

Setting	Description	Factory Default
Enabled	Enable the MicroSD interface on the switch.	Enabled
Disabled	Disable the MicroSD interface on the switch.	

### **Out of Band Interface**

Setting	Description	Factory Default
Enabled	Enable the OOBM (MGMT port) interface on the switch.	Enabled
Disabled	Disable the OOBM (MGMT port) interface on the switch.	

### **LCM Interface**

Setting	Description	Factory Default
Enabled	Enable the LCM interface on the switch.	Enabled
Disabled	Disable the LCM interface on the switch.	

## LCM Interface

### LCM Overview

LCD module (LCM) interface offers another way to display device information. This function allows maintainers to easily check the basic or necessary information without the need to connect with web/CLI. Maintainers can efficiently obtain the target information from the LCM interface by pressing physical buttons.

The following display modes are available:

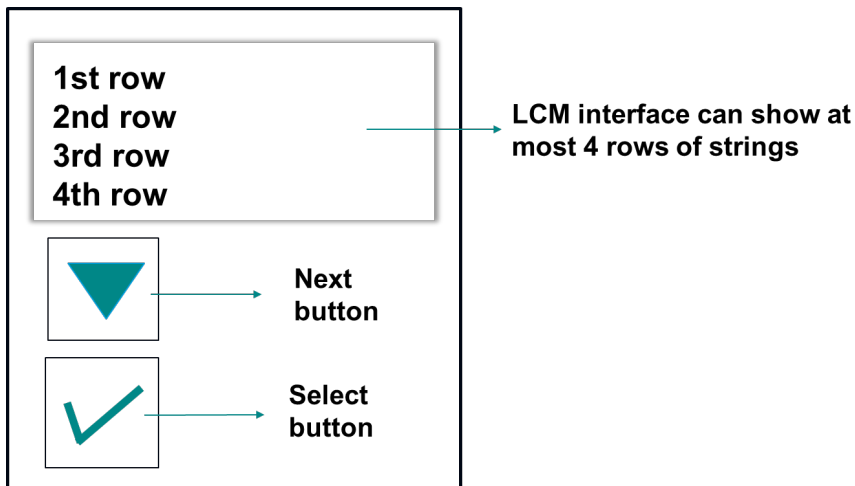
**Menu mode:** Lists all features available by using physical buttons.

**Info mode:** Shows only selected features.

## How LCM interface works

With LCM interface, user can easily confirm system status or obtain the basic information by pressing physical button, without the hassle of extra devices.

The following describes the functions of the LCM.



When the LCM interface is enabled, there is a boot animation indicating boot status. When the system is ready, the animation will disappear and enter display mode.

The LCM can display up to 4 rows of string information. If the length of the string information exceeds the field of the panel, the information will scroll to the end, and restart from the beginning.



### NOTE

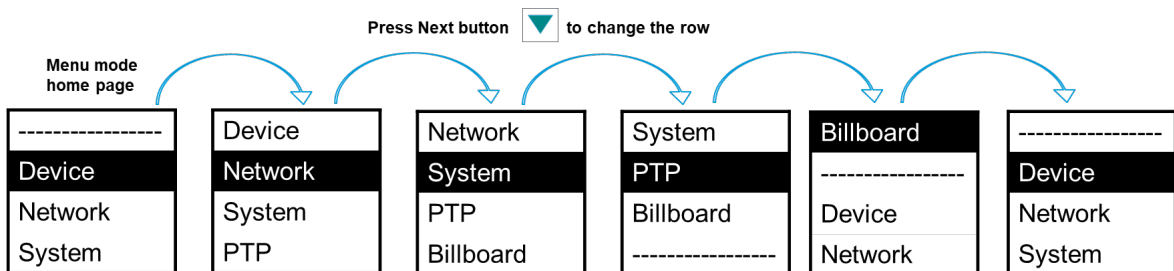
The LCM may not turn off immediately when disabled. Disabling the LCM disables the boot animation.

## Display Mode

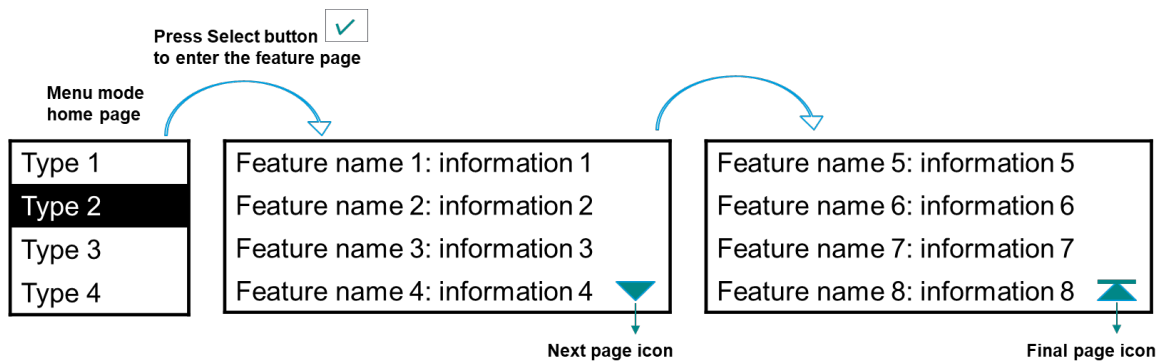
Display Mode shows preselected data continuously on the LCM. Users can toggle between Display Mode's preselected and Menu Mode, which shows all available data.

## Menu Mode

In Menu Mode, users can check device information by choosing a feature type from the home page. Press the **Next** button advance to the next row. Press the **Select** button to check the item under the feature type.



The lower right corner of the screen shows an icon indicating pagination. The icon appears, indicates the end of the list, and subsequently pressing the **Next** button will return to the top of the first page.



In info mode, LCM panel will displays only the selected features (up to 4). This mode can save time by displaying only necessary information without exposing other information unexpectedly. Additional information is available under menu mode.



## NOTE

The LCM continuously display the last page accessed unless a button is pressed to return to the home page or the device reboots.



## ATTENTION

To prolong LCM lifespan, enable Energy Saving mode or disable LCM when not in use.

The following table summarizes the data which can be displayed on the LCM interface.

Type	Feature	Display Name on LCM
Device	Product Model	Model
	Product Revision	Rev
	Device name	Name
	Device Location	Loc
	Serial Number	SN
	Firmware Version	FW
	Firmware Buildtime	FWb
Network	IP Address	IP
	MAC address	MAC
	OOB IP Address	M.IP
	OOB MAC Address	M.MAC
System	System Uptime	UpTm
	Running Redundant Protocol	RED
	Number Of Critical Events	CE#
PTP	PTP Synchronization Status	Sync
	PTP Grandmaster ID	GM.ID
	PTP Parent Clock ID	PC.ID
	PTP Member Ports	M.Prt

## Energy Saving

In some circumstances, it is not necessary to continually run the LCM interface and display information. The Energy Saving feature can be enabled to save the power during a period of disuse by turning off the panel after 60 seconds of idle time. It can be turned on again by pressing any of the physical buttons.

## Billboard

To improve efficiency, billboard feature offers a flexibility to select what will be displayed, regardless of where the features are sorted. The user can select up to 4 frequently used features for the billboard, and

then pin them to the LCM by choosing **Billboard** under Menu mode. In Info mode, LCM will only display the information which are selected for billboard.

## LCM Settings

This section describes how to configure LCM interface.

Enabling/Disabling the LCM interface can be done from **Hardware Interfaces**. The default setting is **Disabled**.

**Hardware Interfaces**

USB Interface \*  
Enabled

MicroSD Interface \*  
Enabled

Out of Band Interface \*  
Enabled

LCM Interface \*  
Disabled

APPLY

## Settings

Click **LCM Interface** on the menu.

You can configure the following parameters to define how information is displayed on the LCM interface.

**LCM Interface**

Ensure to enable LCM interface at "Hardware interfaces" to activate the LCM function.

Energy Saving \*  
Enabled

Display Mode \*  
Info Mode

### Energy Saving

Setting	Description	Factory Default
Enabled	Enable energy saving to turn off LCM interface during the period of inactivity (60 seconds of idle time).	Enabled
Disabled	Disables energy saving for the LCM interface to be on continuously.	

### Display Mode

Setting	Description	Factory Default
Menu mode	Displays complete information list through Menu mode.	Menu mode
Info mode	Displays only the selected information.	

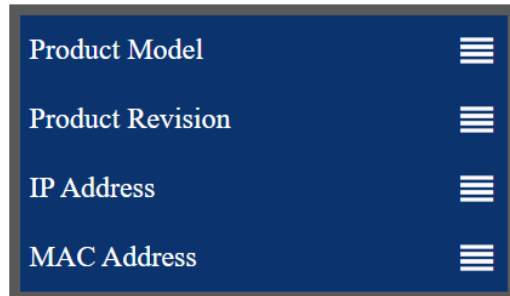
To select which information to display on the billboard, configure following:

Billboard Display Information \*

Selected: 4 features

### Billboard

You can click and drag the features to reorder them on the billboard.



APPLY

#### Billboard Display Information

Setting	Description	Factory Default
Select the feature(s) from the drop-down list	Select the information you want to display on billboard.	Selected: 4 features

#### Billboard

Setting	Description	Factory Default
Drag and reorder the selected features	Arrange how you want to display selected information on billboard.	Product Model Product Revision IP Address MAC Address

After selecting the information to display, you can re-order the information on the billboard by clicking and dragging the corresponding items.

Click **APPLY** to save your changes.

## Login Policy

Click **Login Policy** on the menu.

## Login Policy

Login Message

0 / 500

Login Authentication Failure Message

0 / 500

Account Login Failure Lockout \*

Disabled

Retry Failure Threshold \*

5

1 - 10 times

Lockout Time \*

5

1 - 10 min.

Auto Logout Setting \*

0

0 - 1440 min.

APPLY

Configure the following settings.

### Login Message

Setting	Description	Factory Default
0 to 500 characters	Input the message that will be displayed to users when they log in.	None

### Login Authentication Failure Message

Setting	Description	Factory Default
0 to 500 characters	Input the message that will be displayed when users fail to log in.	None

### Account Login Failure Lockout

Setting	Description	Factory Default
Enabled	Enable the lockout function when a user fails to log in.	Disabled
Disabled	Disable the lockout function when a user fails to log in.	

### Retry Failure Threshold (times)

Setting	Description	Factory Default
1 to 10	Input the maximum number of retry failure times.	5

### Lockout Time (min.)

Setting	Description	Factory Default
1 to 60	Specify the amount of times log in credentials can be entered incorrectly before the user is logged out.	5

### Auto Logout Setting (min.)

Setting	Description	Factory Default
---------	-------------	-----------------

0 to 1440	Specify how long a user has to be inactive before getting logged out.	5
-----------	---	---

When finished, click **APPLY** to save your changes.

## Trusted Access

### Trusted Access Overview

Trusted Access is a mechanism that provides a secure connection to Moxa's switch. Users can use this method to allow the connection from the assigned IP address to ensure safe data transmission.

### Trusted Access Settings and Status

Click **Trusted Access** on the menu.

Configure the following settings.

#### **Enable**

Setting	Description	Factory Default
Enabled	Enable Trusted Access.	Disabled
Disabled	Disable Trusted Access.	




### **NOTE**

1. Trusted Access has to be added before it can be enabled.
2. In order to avoid being disconnected after you enable Trusted Access, you must first add the current IP subnet to Trusted Access. In order to use this function, you should use an RS-232 console to log in or set the device to factory default.

When finished, click **APPLY** to save your changes.




Next, click the  icon.

### Trusted Access

Trusted Access \*  
Disabled ▼

**APPLY**

---



	IP Address	Netmask
<input type="checkbox"/>		

Max. 20

### Create Entry

IP Address \*  
\_\_\_\_\_

Netmask \*  
\_\_\_\_\_

CANCEL
CREATE

Configure the following settings.

**IP Address**


Setting	Description	Factory Default
Input IP address	Specify the IP address that is allowed to connect to Moxa's switch.	None


**Netmask**

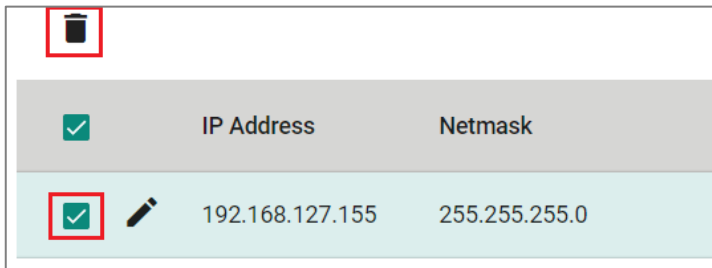
Setting	Description	Factory Default
Input Netmask	Specify the Netmask that is allowed to connect to Moxa's switch.	None


When finished, click **CREATE**.

You can view the Trusted Access status on the figure below.

		IP Address	Netmask
<input type="checkbox"/>		192.168.127.155	255.255.255.0

To delete the trusted access source, select the item and then click the  icon on the top of the page.



<input checked="" type="checkbox"/>	IP Address	Netmask
<input checked="" type="checkbox"/> 	192.168.127.155	255.255.255.0

Click **DELETE** to delete the item.

### Delete Entry

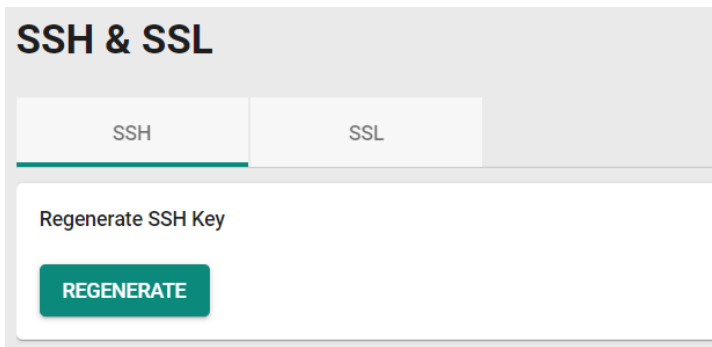
Are you sure you want to delete the selected entry?

[CANCEL](#) [DELETE](#)

## SSH & SSL

### SSH Key Regeneration

Click **SSH & SSL** on the menu and then select the **SSH** tab.



## SSH & SSL

SSH    SSL

Regenerate SSH Key

[REGENERATE](#)

Click **Regenerate** to regenerate the key.

## SSL Certification Regeneration

Click **SSH & SSL** on the menu and select the **SSL** tab. The Certificate Information is shown on this screen.

The screenshot shows the 'SSH & SSL' configuration page. At the top, there are two tabs: 'SSH' and 'SSL', with 'SSL' being the active tab. Below the tabs is a 'Certificate Information' section with the following details: CA Name: Moxa Networking Co., Ltd. and Expired Date: 2198-05-26 18:53:58. Below this is the 'Export SSL certificate Request' section with an 'EXPORT' button. The 'Regenerate SSL Certificate' section has a 'REGENERATE' button. The 'Import Certificate' section has a file selection icon and an 'IMPORT' button.

To import a customer certificate, follow the steps below:

1. Import root CA generated by customer's CA server to a PC.
2. 'Export' the CSR file from the switch and use the customer's CA server to generate a certificate.
3. 'Import' the certificate to the switch.

### **Export SSL Certificate Request**

Setting	Description	Factory Default
Export	Export the SSL certificate to your local computer.	None

### **Regenerate SSL Certificate**

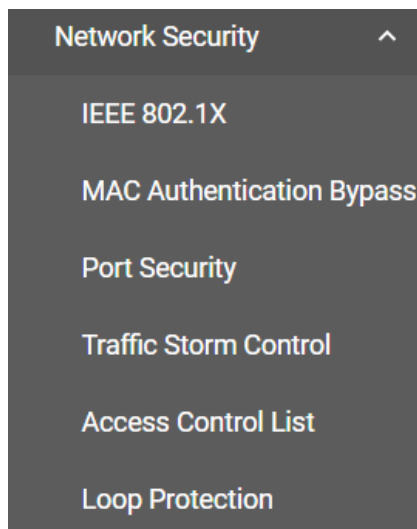
Setting	Description	Factory Default
Regenerate	Regenerate the SSL certificate.	None

### **Import Certificate**

Setting	Description	Factory Default
Select the file	Import the SSL certificate from the location where the SSL certificate is located.	None

# Network Security

This section demonstrates how to configure network security settings, including **IEEE802.1X**, **MAC Authentication Bypass**, **Port Security**, **Traffic Storm Control**, **Access Control List**, and **Loop Protection**.



## IEEE 802.1X

### Port-based IEEE 802.1X Overview

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

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

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

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

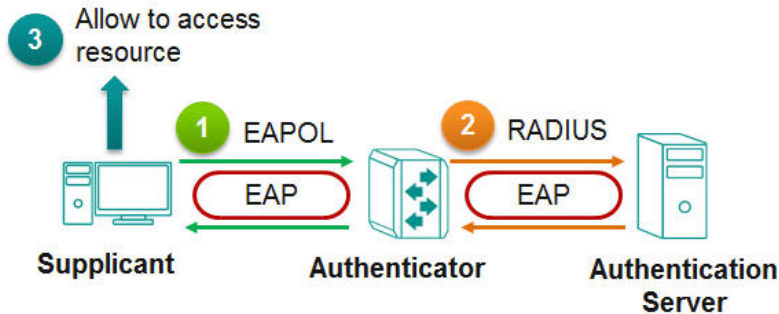
**Authenticator:** Edge switch or wireless access point that acts as a proxy between the supplicant and the authentication server, requesting identity information from the supplicant, verifying the information with the authentication server, and relaying a response to the supplicant.

The Moxa switch acts as an authenticator in the 802.1X environment. A supplicant and an authenticator exchange EAPOL (Extensible Authentication Protocol over LAN) frames with each other. We can either use an external RADIUS server as the authentication server or implement the authentication server in the Moxa switch by using a Local User Database as the authentication look-up table. When we use an external RADIUS server as the authentication server, the authenticator and the authentication server exchange EAP frames.

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

## How IEEE 802.1X Works

802.1X authentication requires three parties: a supplicant, an authenticator, and an authentication server. The supplicant is a client device that wishes to connect to the LAN or WLAN. The supplicant can also use the software to run on the client that offers credentials to the authenticator. Network administrators usually use an Ethernet switch or wireless access point as the authenticator, and running software supporting RADIUS and EAP protocols in the authentication server.



The authenticator serves as a security guard to a protected network. The supplicant is not allowed access through the authenticator to the protected side of the network unless the supplicant's identity has been validated and authorized. With 802.1X port-based authentication, the supplicant provides credentials, such as user name/password or digital certificate, to the authenticator, and the authenticator transmits the credentials to the authentication server for verification. If the authentication server approves the credentials as valid, the supplicant (client device) is allowed to access resources located on the protected side of the network.

## IEEE 802.1X Settings

Click **IEEE802.1X** on the menu and then select the **General** tab.

### IEEE 802.1X

General

RADIUS

Local Database

IEEE 802.1X \*

Authentication Mode \*

Configure the following settings.


### Enable





Setting	Description	Factory Default
Enabled	Enable IEEE 802.1X.	Disabled
Disabled	Disable IEEE 802.1X.	

### Authentication Mode

Setting	Description	Factory Default
Local Database	Use the local database as the authentication mode.	Local Database
RADIUS	Use the RADIUS as the authentication mode.	

When finished, click **APPLY** to save your changes.

To configure the IEEE 802.1X settings for the specific port, click the  icon on the port.

	Port	Enable	Port Control	Max. Request	Quiet Period	Reauthentication
	1/1	Disabled	Auto	2	60	Disabled
	1/2	Disabled	Auto	2	60	Disabled
	1/3	Disabled	Auto	2	60	Disabled
	1/4	Disabled	Auto	2	60	Disabled

Configure the following settings.

### Port 1/1 Settings

Enabled \*  
Disabled ▼

Port Control \*  
Auto ▼

Max. Request \* Quiet Period \*  
2 60

1 - 10 times 0 - 65535 sec.

Reauthentication \* Reauth Period \*  
Disabled ▼ 3600

1 - 65535 sec.

Server Timeout \*  
30


1 - 65535 sec.

Supp Timeout \*  
30

1 - 65535 sec.

Tx Period \*  
30

1 - 65535 sec.

Copy Configurations ... ▼ 

CANCEL
APPLY

**Enable**

Setting	Description	Factory Default
Enabled	Enable IEEE 802.1X.	Disabled
Disabled	Disable IEEE 802.1X.	

### Port Control

Setting	Description	Factory Default
Force Unauthorized	The controlled port has to be held in the Unauthorized state.	Auto
Auto	The controlled port is set to the authorized or unauthorized state in accordance with the outcome of an authentication exchange between the Supplicant and the Authentication Server.	
Force Authorized	The controlled port is required to be held in the authorized state.	

### Max Request (times)

Setting	Description	Factory Default
1 to 10	Enable re-authentication request time.	2

### Quiet Period (sec.)

Setting	Description	Factory Default
0 to 65535	Specify the duration of time that the switch remains in the quiet state following a failed authentication exchange with the client.	60

### Reauthentication

Setting	Description	Factory Default
Enabled	Enable re-authentication.	Disabled
Disabled	Disable re-authentication.	

### Reauth Period (sec.)

Setting	Description	Factory Default
1 to 65535	Input the duration of time between re-authentication attempts.	3600

### Server Timeout (sec.)

Setting	Description	Factory Default
1 to 65535	Input the duration of time that the switch will re-transmit the packets from the switch to the authentication server.	30

### Supp (Supplicant, such as Client PC) Timeout (sec.)

Setting	Description	Factory Default
1 to 65535	Input the duration of time that the switch will re-transmit the packets from the switch to the client.	30

### Tx Period (sec.)

Setting	Description	Factory Default
1 to 65535	Input the duration of time that the switch will re-transmit the data to the client.	30

### Copy Config to Ports

Setting	Description	Factory Default
Select the port(s) from the drop-down list	Allows users to copy configurations to other port(s).	None

When finished, click **APPLY** to save your changes.

## IEEE 802.1X Database

### RADIUS

RADIUS **Remote Authentication Dial in User Service** is a protocol that involves three services in one network protocol: Authentication, Authorization, and Accounting (AAA). The protocol operates on port 1812, and the AAA management for users connecting to a network service.

RADIUS is based on a client/server protocol that runs in the application layer, and can use either TCP or UDP as the mode of transport. The network access servers that contain the RADIUS protocol can allow the client to communicate with the RADIUS server. Through Authentication, Authorization, and Accounting, RADIUS is used to monitor access to the network.

To configure RADIUS settings, click the **RADIUS** tab.

## IEEE 802.1X

General
RADIUS
Local Database

Server Address 1

Auth Port

Share Key

Timeout  sec.

Retransmit  sec.

Server Address 2

Auth Port

Share Key

Timeout  sec.

Retransmit  sec.

**APPLY**

Configure the following settings.

**Server Address 1**

Setting	Description	Factory Default
To input server address 1	Specify the 1st server address.	None

**Auth Port**

Setting	Description	Factory Default
1 to 65535	Specify the authentication port number for the 1st server address.	None

**Share Key**

Setting	Description	Factory Default
Input the share key for the 1st server, (0 to 46)	Specify the share key for the 1st server.	None

**Timeout (sec.)**

Setting	Description	Factory Default
1 to 120	Specify the duration of time before a device is logged out.	None

**Retransmit (sec.)**

Setting	Description	Factory Default
1 to 254	Specify the time for data re-transmission.	None

**Server Address 2**

Setting	Description	Factory Default
To input server address 2	Specify the 2nd server address.	None



### Auth Port

Setting	Description	Factory Default
1 to 65535	Specify the authentication port number for the 1st server address.	None

### Share Key

Setting	Description	Factory Default
Input the share key for the 2nd server (0 to 46)	Specify the share key for the 2nd server.	None

### Timeout

Setting	Description	Factory Default
1 to 120	Specify the duration of time before the device is timed out.	None

### Retransmit (sec.)

Setting	Description	Factory Default
1 to 254	Specify the time for data re-transmission.	None


When finished, click **APPLY** to save your changes.

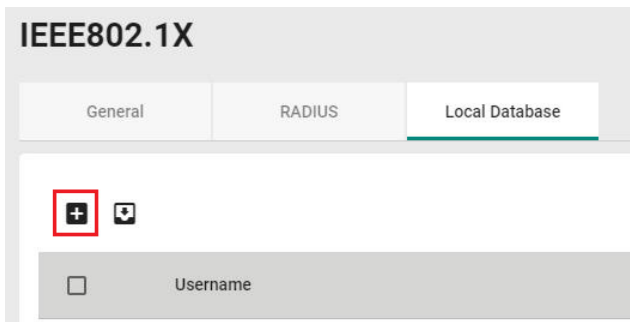


## NOTE

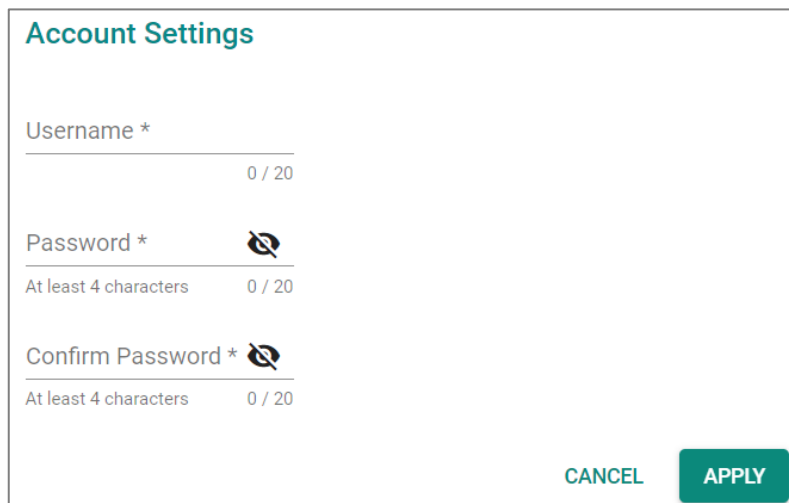
The RADIUS service will be operated via the 1st server first; if it fails, it will be run on the 2nd server.

## Local Database

First click the **Local Database** tab and then click the  icon.



Configure the following settings.



### **Username**

Setting	Description	Factory Default
0 to 20 characters	Specify the username for the local database.	None

### **Password**

Setting	Description	Factory Default
At least 4 characters, (max. 20 characters)	Specify the password for the local database user.	None

### **Confirm Password**

Setting	Description	Factory Default
At least 4 characters, (max. 20 characters)	Confirm the password for the local database user.	None

When finished, click **APPLY** to save your changes.

## **MAC Authentication Bypass**

Click **MAC Authentication Bypass** on the function menu.

### **General**

Click the **General** tab for general settings.

The screenshot shows the 'MAC Authentication Bypass' configuration interface. At the top, there are three tabs: 'General', 'RADIUS', and 'Local Database'. The 'General' tab is active. Below the tabs, there are two dropdown menus: 'MAC Authentication ...' and 'Authentication Mode \*'. At the bottom left of the configuration area, there is a green 'APPLY' button.

### **MAC Authentication Bypass**

Setting	Description	Factory Default
Enabled	Enable MAC authentication bypass function.	None
Disabled	Disable MAC authentication bypass function.	

### **Authentication Mode**

Setting	Description	Factory Default
RADIUS	Select RADIUS as the authentication mode.	None
Local Database	Select local database as the authentication mode.	

When finished, click **APPLY** to save your changes.

## RADIUS

Click the **RADIUS** tab to perform further configurations.

### MAC Authentication Bypass

General
RADIUS
Local Database

Server Address 1

Share Key  0 / 46

Timeout  sec.

Server Address 2

Share Key  0 / 46

Timeout  sec.

Auth Port

Retransmit  sec.

Auth Port

Retransmit  sec.

APPLY

Configure the following settings.

### Server Address 1

Setting	Description	Factory Default
To input server address 1	Specify the 1st server address.	None

### Auth Port

Setting	Description	Factory Default
1 to 65535	Specify the authentication port number for the 1st server address.	None

### Share Key

Setting	Description	Factory Default
Input the share key for the 1st server, (0 to 46)	Specify the share key for the 1st server.	None

### Timeout (sec.)

Setting	Description	Factory Default
1 to 120	Specify the duration of time before a device is logged out.	None

### Retransmit (sec.)

Setting	Description	Factory Default
1 to 254	Specify the time for data re-transmission.	None

### Server Address 2

Setting	Description	Factory Default
To input server address 2	Specify the 2nd server address.	None

### Auth Port

Setting	Description	Factory Default
1 to 65535	Specify the authentication port number for the 1st server address.	None

### Share Key

Setting	Description	Factory Default
Input the share key for the 2nd server (0 to 46)	Specify the share key for the 2nd server.	None

### Timeout

Setting	Description	Factory Default
1 to 120	Specify the duration of time before the device is timed out.	None

### Retransmit (sec.)

Setting	Description	Factory Default
1 to 254	Specify the time for data re-transmission.	None


When finished, click **APPLY** to save your changes.

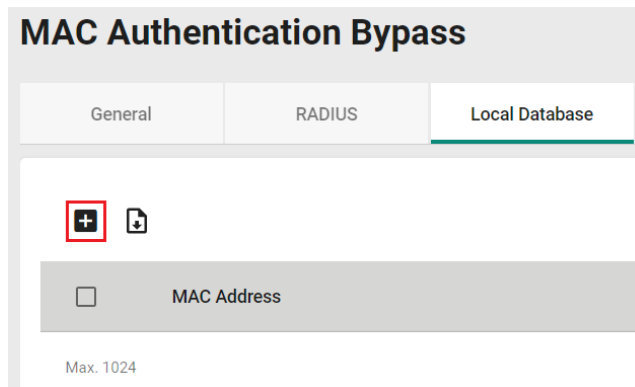


## NOTE

The RADIUS service will be operated via the 1st server first; if it fails, it will be run on the 2nd server.



## Local Database

Click **Local Database** tab, and then click  icon for further configurations.



**MAC Authentication Bypass**

General    RADIUS    **Local Database**

MAC Address

Max. 1024

Configure the following setting.

#### MAC Address

Setting	Description	Factory Default
MAC Address	Specify the MAC address used for MAC authentication bypass.	None

When finished, click **CREATE** to complete.

## Port Security

### MAC Sticky Overview

MAC Sticky is a function that allows users to configure the maximum number of MAC addresses (the Limit) that a port can “learn”. Users can configure what action should be taken (under Secure Action) when a new MAC address tries to access a port after the maximum number of MAC addresses have already been learned. The total number of allowed MAC addresses cannot exceed 1024.

#### How MAC Sticky Works

In MAC Sticky mode, administrators can set a proper limit number and then configure trust devices manually, or let the system configure trust devices automatically. Except for dropping packets as a response to any violations, administrators can set ‘port shutdown’ on a port and achieve a strict security guarantee. When a violation is registered on a port, the port will shut down and an administrator will receive a notification to perform a check.

### MAC Sticky Settings and Status

To configure the MAC Sticky settings, select the **General** tab in **Port Security**.

Configure the following settings.

#### Enable

Setting	Description	Factory Default
Enabled	Enable port security.	Enabled
Disabled	Disable port security.	

#### Port Security Mode


Setting	Description	Factory Default
MAC Sticky	Specify MAC Sticky as the port security mode.	Static Port Lock
Static Port Lock	Specify Static Port Lock as the port security mode.	





Select **MAC Sticky** and click **Apply**.



## NOTE

When you change the Port Security Mode, the settings in the table will be deleted.

Click the  icon on the port you want to edit.

	Port	Enable	Address Limit	Secure Action	Current Address
	1/1	Disabled	1	Packet Drop	0
	1/2	Disabled	1	Packet Drop	0
	1/3	Disabled	1	Packet Drop	0
	1/4	Disabled	1	Packet Drop	0

Configure the following settings.

### Edit Port 1/1 Setting

MAC Sticky  
Disabled ▼

---

Address Limit \*  
1 i

1 - 1013

Secure Action  
Packet Drop ▼

Cancel Apply

### MAC Sticky

Setting	Description	Factory Default
Enabled	Enable Static Port Lock for this port.	Disabled
Disabled	Disable Static Port Lock for this port.	

### Address Limit

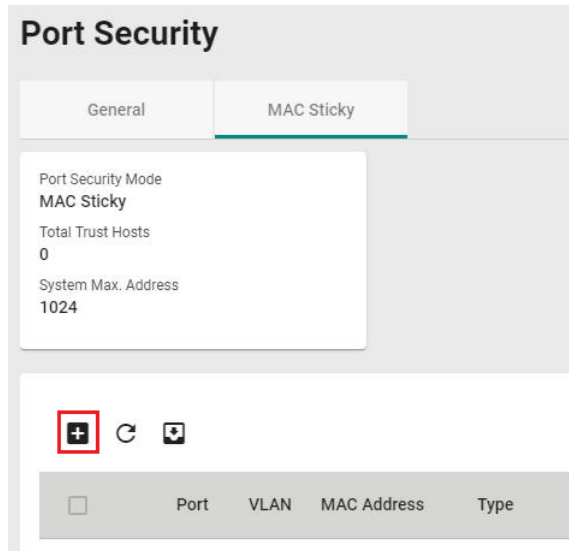
Setting	Description	Factory Default
1 to 997	Specify the maximum numbers of the learned MAC address.	1

### Secure Action

Setting	Description	Factory Default
Port Shutdown	Enable port shutdown when a violation occurs.	Packet Drop
Packet Drop	Drop the packets when a violation occurs.	

When finished, click **Apply** to save your changes.

Next, click the **MAC Sticky** tab, and then click the **+** icon to add the MAC Sticky entries.



Configure the following settings.

### Create Entry

Port \* ▼

---

VLAN ID \*

---

MAC Address \* i

---

Cancel Create

**Port**

Setting	Description	Factory Default
Select the port from the drop-down list	Select the port(s) that will be used with the MAC Sticky function.	None

**VLAN ID**

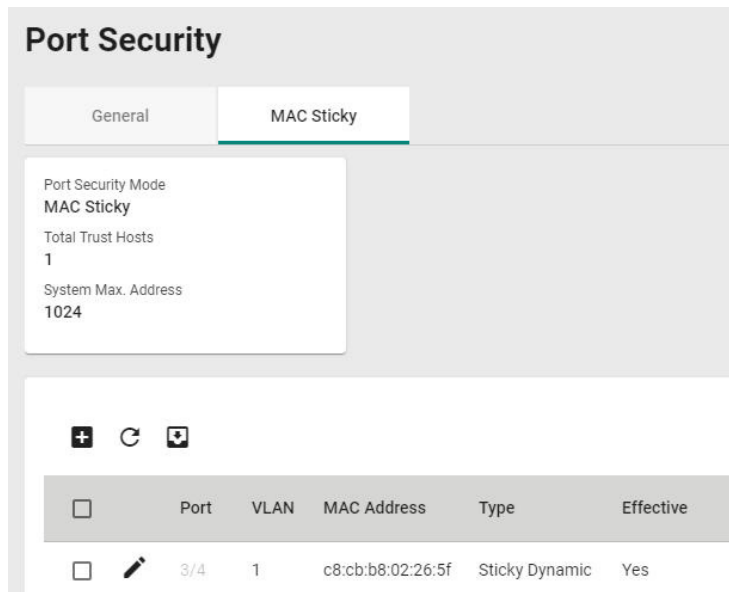
Setting	Description	Factory Default
Input the VLAN ID	Specify the VLAN ID that will be used with MAC Sticky.	None

**MAC Address**

Setting	Description	Factory Default
Input the MAC address that will be used	Specify the MAC Address of the device that will be used as the reliable source for network access.	None

When finished, click **Create**.

You can view the MAC Sticky settings in the figure below.

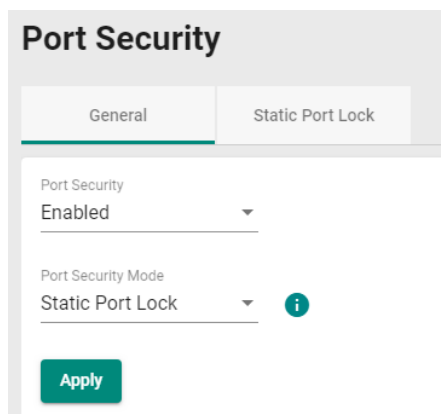


## Static Port Lock Overview

To provide a port-based security function, Moxa’s switches have implemented Static Port Lock function; the main idea is to allow configured devices, 128 at most, to access the network through a specific port. Packets sent from unknown devices or from configured devices with mismatching ports will be dropped. In other words, only the packets from the devices pre-configured with the specific MAC addresses can be sent to the specific port to ensure a secured network data transmission scenario.

## Static Port Lock Settings and Status

To configure these setting, first click the **Port Security** tab and then click **General**.



Configure the following settings.

### Enable


Setting	Description	Factory Default
Enabled	Enable port security.	Enabled
Disabled	Disable port security.	

### Port Security Mode

Setting	Description	Factory Default
MAC Sticky	Select MAC Sticky as the port security mode.	Static Port Lock
Static Port Lock	Select Static Port Lock as the port security mode.	

Select **Static Port Lock** and click **Apply**.



Select the  icon on the port you want to edit.

	Port	Enable	Manual Configured Address
	1/1	Disabled	0
	1/2	Disabled	0
	1/3	Disabled	0
	1/4	Disabled	0

Configure the following settings.

### Edit Port 1/1 Setting


Static Port Lock  
Disabled ▼

Cancel Apply

**Enable**

Setting	Description	Factory Default
Enabled	Enable Static Port Lock.	Disabled
Disabled	Disable Static Port Lock.	

When finished, click **Apply** to save your changes.

Next, click the **Static Port Lock** tab and then the  icon to perform further settings.

## Port Security


General


Static Port Lock


Port Security Mode  
**Static Port Lock**

Total Trust Hosts  
0

System Max. Address  
1024







<input type="checkbox"/>	Port	VLAN	MAC Address	Type

Configure the following settings.

### Create Entry

Port \* ▼

---

VLAN ID \*

---

MAC Address \* i

---

Cancel
Create

**Port**

Setting	Description	Factory Default
Select the port from the drop-down list	Specify the port(s) that will be used with Static Port Lock.	None

**VLAN ID**

Setting	Description	Factory Default
Input the VLAN ID	Specify the VLAN ID that will use Static Port Lock.	None

**MAC Address**

Setting	Description	Factory Default
Input the MAC address that will be used	Specify the MAC Address of the device that will be used as the reliable source for network access.	None

When finished, click **Create**.

You can view the **Static Port Lock** setting status from the following figure.


+
↺
+





	Port	VLAN	MAC Address	Type	Effective
<input type="checkbox"/>	1/1	1	00:01:02:03:04:05	Lock Configured	No

Max 1024

## Traffic Storm Control

A traffic storm can happen when packets flood the network; this causes excessive traffic and slows down the network performance. To counter this, Traffic Storm Control provides an efficient design to prevent the network from flooding caused by a broadcast, multicast, or unicast traffic storm on a physical network layer. The feature can handle packets from both ingress and egress data.

First click **Traffic Storm Control** on the menu, and then click the  icon on the specific port you want to configure.

Traffic Storm Control					
Port	Broadcast	DLF	Priority	Threshold (fps)	
 1/1	Enabled	Disabled	Disabled	12700	
 1/2	Enabled	Disabled	Disabled	12700	
 1/3	Enabled	Disabled	Disabled	12700	
 1/4	Enabled	Disabled	Disabled	12700	

Configure the following settings.

### Edit Port 1/1 Settings

Broadcast \*  
Enabled ▼

Multicast \*  
Disabled ▼

DLF \*  
Disabled ▼

Threshold \*  
12700 i  
625 - 14881000 fps

Copy Configurations ... i

CANCEL APPLY

There are three methods that can be used for traffic storm control: Broadcast, Multicast, and Destination Lookup Failure (DLF).

#### **Broadcast**

Setting	Description	Factory Default
Enabled	Enable Broadcast when a traffic storm occurs.	Disabled
Disabled	Disable Broadcast when a traffic storm occurs.	

### Multicast

Setting	Description	Factory Default
Enabled	Enable multicast when a traffic storm occurs.	Disabled
Disabled	Disable multicast when a traffic storm occurs.	

### DLF

Setting	Description	Factory Default
Enabled	Enable DLF when a traffic storm occurs.	Disabled
Disabled	Disable DLF when a traffic storm occurs.	

### Threshold (fps)


Setting	Description	Factory Default
625 to 14881000	Define the threshold for a traffic storm.	12700

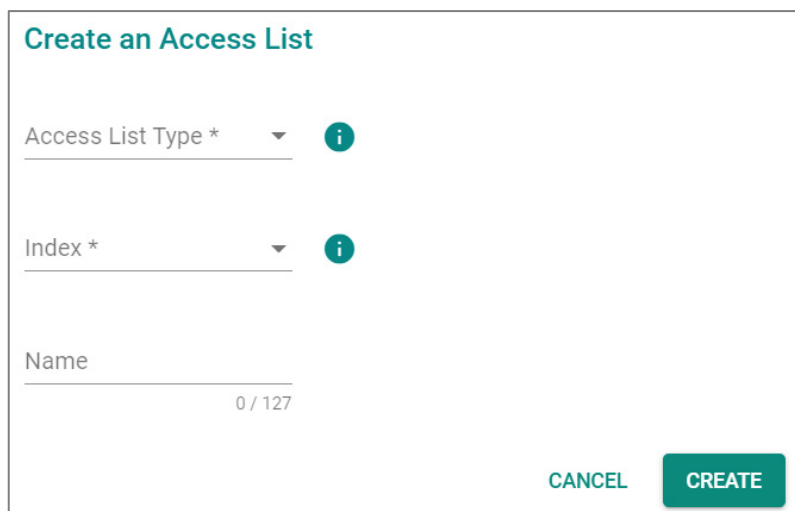
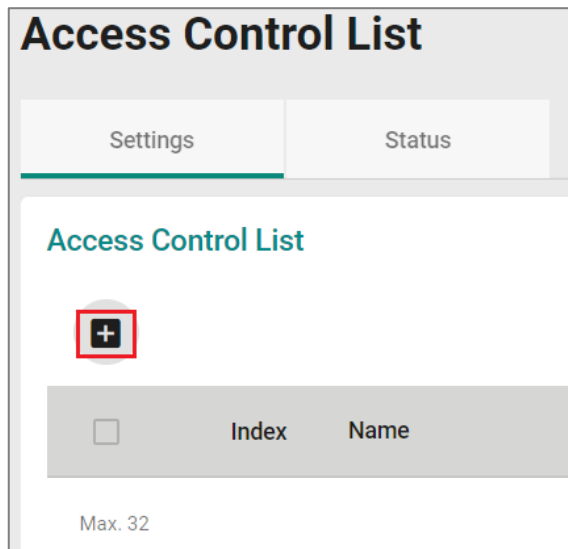
### Copy Config to Ports

Setting	Description	Factory Default
Select the port(s) from the drop-down list	Select the port(s) you want to have the same configurations for.	None

When finished, click **APPLY** to save your changes.

## Access Control List

Click **Access Control List** on the function menu and then click  to perform further configurations.



Configure the following settings.

#### Access List Type

Setting	Description	Factory Default
IP-based	Specify IP-based as the access list type.	None
MAC-based	Specify MAC-based as the access list type.	

#### Index (For IP-based type)

Setting	Description	Factory Default
Select from IP-1 to IP-16	Select from the drop-down list for index.	None

#### Index (For MAC-based type)

Setting	Description	Factory Default
Select from MAC-1 to MAC-16	Select from the drop-down list for index.	None

#### Name

Setting	Description	Factory Default
0 to 127 characters	Provide a name for this access list.	None

## IP-based ACL Table Configurations

Configure the following settings for IP-based access list.

**ACL Table of IP-1** ▼

Active Interface Type \*

Port-based ▼

---

Active Ingress Ports ▼ ⓘ

---

Active Egress Ports ▼ ⓘ

---

**APPLY**

#### Active Interface Type

Setting	Description	Factory Default
Port-based	Specify Port-based as the active interface type.	None
VLAN-based	Specify VLAN-based as the active interface type.	

#### Active Ingress Ports (For Port-based type)

Setting	Description	Factory Default
Select the port(s) from the drop-down list	Select the port(s) as the active ingress port(s).	None

#### Active Egress Ports (For Port-based type)

Setting	Description	Factory Default
Select the port(s) from the drop-down list	Select the port(s) as the active egress port(s).	None

#### Active Ingress VLAN (For VLAN-based type)

Setting	Description	Factory Default
Select the port(s) from the drop-down list	Select the port(s) as the active ingress VLAN.	None

### Active Egress VLAN (For VLAN-based type)

Setting	Description	Factory Default
Select the port(s) from the drop-down list	Select the port(s) as the active egress VLAN.	None

When finished, click **APPLY** to save your changes.



## NOTE

Each port can only be mapped to either an ingress port or an egress port - not both.

## IP-based Rule Index Settings

Click the **+** icon for Rule Index settings.



### Create Rule Index 1 Settings of IP-1

Rule Index 1 \*  
Enabled

Rule Type \*  
-

Protocol  
Any

Source IP Address  
Any

Source IP Mask  
-

Destination IP Address  
Any

Destination IP Mask  
-

DSCP  
Any

0 - 63

CANCEL CREATE

Configure the following settings.

### Rule Index 1

Setting	Description	Factory Default
Enabled	Enable Rule Index 1 settings.	Enabled
Disabled	Disable Rule Index 1 settings.	

### Rule Type

Setting	Description	Factory Default
Permit	Permit the rule type.	None
Deny	Deny the rule type.	

### Protocol

Setting	Description	Factory Default
Select the port(s) from the drop-down list	Select the protocol used for this rule index.	Any

**ICMP Type (For ICMP protocol only)**

Setting	Description	Factory Default
0 to 255	Select the ICMP type value.	Any

**ICMP Code (For ICMP protocol only)**

Setting	Description	Factory Default
0 to 15	Select the ICMP code value.	Any

**IGMP Type (For IGMP protocol only)**

Setting	Description	Factory Default
0 to 255	Select the IGMP type value.	Any

**Protocol Number (For User defined protocol only)**

Setting	Description	Factory Default
0 to 255	Select the protocol number.	None

**Source IP Address**

Setting	Description	Factory Default
IP address	Provide the IP address as the source IP address.	Any

**Source IP Mask**

Setting	Description	Factory Default
Select the port(s) from the drop-down list	Select the source IP mask from the list.	None

**Source Port**

Setting	Description	Factory Default
Select the port(s) by using the up/down arrow	Select the source port.	Any

**Destination IP Address**

Setting	Description	Factory Default
IP address	Provide the IP address as the destination IP address.	Any

**Destination IP Mask**

Setting	Description	Factory Default
Select the port(s) from the drop-down list	Select the destination IP mask from the list.	None

**Destination Port**

Setting	Description	Factory Default
Select the port(s) by using the up/down arrow	Select the destination port.	Any

**DSCP**

Setting	Description	Factory Default
0 to 63	Specify the DSCP value.	Any

**Action-Redirect Enable**

Setting	Description	Factory Default
Enabled	Enable the redirection function.	Disabled
Disabled	Disabled the redirection function.	

**DSCP Remark**

Setting	Description	Factory Default
0 to 63	Specify the DSCP remark value.	Disabled

When finished, click **CREATE** to complete.

Note that the following system packets are not included in the ACL operation.

Item	Destination/Source Port Number
DHCP Server	67
DHCP Client	68
Moxa Service	40404

## MAC-based ACL Table Configurations

Configure the following settings for MAC-based access list.

**ACL Table of MAC-1** ▼

Active Interface Type \*

Port-based ▼

---

Active Ingress Ports ▼ ⓘ

---

Active Egress Ports ▼ ⓘ

---

**APPLY**

### Active Interface Type

Setting	Description	Factory Default
Port-based	Specify Port-based as the active interface type.	None
VLAN-based	Specify VLAN-based as the active interface type.	

### Active Ingress Ports (For Port-based type)

Setting	Description	Factory Default
Select the port(s) from the drop-down list	Select the port(s) as the active ingress port(s).	None

### Active Egress Ports (For Port-based type)

Setting	Description	Factory Default
Select the port(s) from the drop-down list	Select the port(s) as the active egress port(s).	None

### Active Ingress VLAN (For VLAN-based type)

Setting	Description	Factory Default
Select the port(s) from the drop-down list	Select the port(s) as the active ingress VLAN.	None

### Active Egress VLAN (For VLAN-based type)

Setting	Description	Factory Default
Select the port(s) from the drop-down list	Select the port(s) as the active egress VLAN.	None

When finished, click **APPLY** to save your changes.




## NOTE

Each port can only be mapped to either an ingress port or an egress port - not both.



## MAC-based Rule Index Settings

Click the  icon for Rule Index settings.



### Create Rule Index 1 Settings of MAC-1

Rule Index 1 \*  
Enabled ▼

Rule Type \*  
▼

EtherType  
Any ▼

Source MAC Address  
Any Source MAC Mask ▼

Destination MAC Address  
Any Destination MAC Ma... ▼

VLAN ID  
Any  
1 - 4094

CoS  
Any  
0 - 7

CANCEL
CREATE

Configure the following settings.

### Rule Index 1

Setting	Description	Factory Default
Enabled	Enable Rule Index 1 settings.	Enabled
Disabled	Disable Rule Index 1 settings.	

### Rule Type

Setting	Description	Factory Default
Permit	Permit the rule type.	None
Deny	Deny the rule type.	

### EtherType

Setting	Description	Factory Default
GOOSE	Select GOOSE as the Ethernet type.	Any
SMV	Select SMV as the Ethernet type.	
User defined	Select User defined as the Ethernet type.	

### EtherType Value (For User defined type only)

Setting	Description	Factory Default
In hex digit	Provide the Ethernet type value for the user defined type.	0x

### Source MAC Address

Setting	Description	Factory Default
MAC address	Provide the MAC address as the source MAC address.	Any

### Source MAC Mask

Setting	Description	Factory Default
Select the port(s) from the drop-down list	Select the source MAC mask from the list.	None

### Destination MAC Address

Setting	Description	Factory Default
MAC address	Provide the MAC address as the destination MAC address.	Any

### Destination MAC Mask

Setting	Description	Factory Default
Select the port(s) from the drop-down list	Select the destination MAC mask from the list.	None

### VLAN ID

Setting	Description	Factory Default
Select the VLAN ID by using the up/down arrows	Select the VLAN ID.	Any

### CoS

Setting	Description	Factory Default
Select the Cos value by using the up/down arrows	Specify the DSCP value.	Any

When finished, click **CREATE** to complete.

Note that the following system packets are not included in the ACL operation.

Item	MAC Address
IEEE reserved Multicast MAC address	01:80:C2:00:00:XX

Item	Ether Type
ARP	0x0806
LACP	0x8809
Jumbo Frame	0x8870
EAP over LAN	0x888E
LLDP	0x88CC

## Access Control List Status

Click **Status** tab to view the Access Control List status.

### Access Control List

Settings    **Status**

#### ACL Summary

Number of activate ACL (Max. 16)  
1

#### Access Control List

Index	Name	Activated	Activate Direction
MAC-1	test	Inactivated	--
IP-1	test	Activated	Both

## Loop Protection

Click **Loop Protection** on the function menu.

### Settings

Click **Settings** tab for further configurations.

### Loop Protection

Settings    Status

Loop Protection \*  
Disabled

Detect Interval \*  
10  
1 - 30 sec.

**APPLY**

Configure the following settings.

#### Loop Protection

Setting	Description	Factory Default
Enabled	Enable Loop Protection function.	Disabled
Disabled	Disable Loop Protection function.	

### Detect Interval

Setting	Description	Factory Default
1 to 30	Specify the detect interval value.	10


When finished, click **APPLY** to complete.





## Status

Click **Status** tab to view the Loop Protection status.

### Loop Protection

Settings    **Status**



Ports	Loop Status	Port Status	Peer Port
 1/1	Normal	--	--
 1/2	Normal	--	--
 1/3	Normal	--	--
 1/4	Normal	--	--

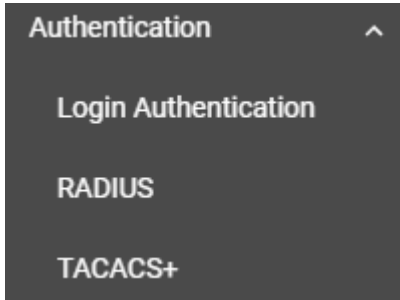
## Authentication

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

There are five combinations available for users to choose from:

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

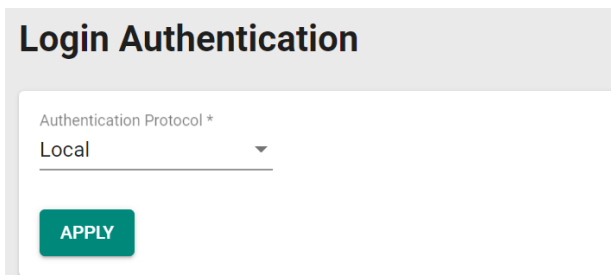
This section includes the configurations for **Login Authentication**, **RADIUS**, and **TACACS+**.



## Login Authentication

This section allows users to select the login authentication protocol.

Select **Login Authentication**.

A configuration page titled 'Login Authentication'. It features a dropdown menu labeled 'Authentication Protocol \*' with 'Local' selected. Below the dropdown is a green 'APPLY' button.

Configure the following settings.

### **Authentication Protocol**

Setting	Description	Factory Default
Local	Select Local as the authentication protocol.	Local
RADIUS	Select RADIUS as the authentication protocol.	
TACACS+	Select TACACS+ as the authentication protocol.	
RADIUS, Local	Select RADIUS and Local as the authentication protocol.	
TACACS+, Local	Select TACACS+ and Local as the authentication protocol.	

When finished, click **APPLY** to save your changes.

## RADIUS

Click **RADIUS** on the menu and configure the following settings.

### RADIUS Server

Server Address 1 \* UDP Port \*

0.0.0.0 1812

---

1 - 65535

Share Key

---

0 / 64

Auth Type \*

CHAP ▼

---

Timeout \*

5

---

5 - 180 sec.

Retry \*

1

---

0 - 5 times

Server Address 2 \* UDP Port \*

0.0.0.0 1812

---

1 - 65535

Share Key

---

0 / 64

Auth Type \*

CHAP ▼

---

Timeout \*

5

---

5 - 180 sec.

Retry \*

1

---

0 - 5 times

**APPLY**

### Server Address 1

Setting	Description	Factory Default
Input the server address	Specify the 1st server address as the authentication database.	0.0.0.0

### UDP Port

Setting	Description	Factory Default
Input the port number	Specify the UDP port.	1812

### Share Key

Setting	Description	Factory Default
Input the key	Input the share key for 1st server authentication verification.	None

**Authentication Type**

Setting	Description	Factory Default
PAP	PAP is the authentication type.	CHAP
CHAP	CHAP is the authentication type.	
MS-CHAPv1	MS-CHAPv1 is the authentication type.	

**Timeout (sec.)**

Setting	Description	Factory Default
5 to 180	When waiting for a response from the server, set the amount of time before timeout.	5

**Retry (sec.)**

Setting	Description	Factory Default
0 to 5	Define the retry interval when trying to reconnect to a server.	1

**Server Address 2**

Setting	Description	Factory Default
Input the server address	Specify the 2nd server address as the authentication database.	0.0.0.0

**UDP Port**

Setting	Description	Factory Default
Input the port number	Specify the UDP port.	1812

**Share Key**

Setting	Description	Factory Default
Input the key	Specify the share key for 2nd server authentication verification.	None

**Authentication Type**

Setting	Description	Factory Default
PAP	PAP is the authentication type.	CHAP
CHAP	CHAP is the authentication type.	
MS-CHAPv1	MS-CHAPv1 is the authentication type.	

**Timeout (sec.)**

Setting	Description	Factory Default
5 to 180	When waiting for a response from the server, set the amount of time before the device is timed out.	5

**Retry (sec.)**

Setting	Description	Factory Default
0 to 5	Set the retry interval when trying to reconnect to a server.	1

When finished, click **APPLY** to save your changes.





**NOTE**

The RADIUS service will be operated via the 1st server; if it fails, it will run on the 2nd server.

## TACACS+

Click **TACACS+** on the menu and then configure the following settings.

### TACACS+ Server

Server Address 1 *	TCP Port *
0.0.0.0	49
	1 - 65535
Share Key	 
	0 / 64
Auth Type *	
CHAP	▼
Timeout *	
5	
5 - 180	sec.
Retry *	
1	
0 - 5	times
Server Address 2 *	TCP Port *
0.0.0.0	49
	1 - 65535
Share Key	 
	0 / 64
Auth Type *	
CHAP	▼
Timeout *	
5	
5 - 180	sec.
Retry *	
1	
0 - 5	times

**APPLY**

#### Server Address 1

Setting	Description	Factory Default
Input the server address	Specify the 1st server address as the authentication database.	0.0.0.0

#### TCP Port

Setting	Description	Factory Default
Input the port number	Specify the UDP port.	49

#### Share Key

Setting	Description	Factory Default
Input the key	Specify the share key for 1st server authentication verification.	None



### Authentication Type

Setting	Description	Factory Default
ASCII	ASCII is the authentication type.	CHAP
PAP	PAP is the authentication type.	
CHAP	CHAP is the authentication type.	

### Timeout (sec.)

Setting	Description	Factory Default
Input the value	When waiting for a response from the server, set the amount of time before the device is timed out.	5

### Retry

Setting	Description	Factory Default
Input the value	Set the retry interval when trying to reconnect to a server.	1

### Server Address 2

Setting	Description	Factory Default
Input the server address	Specify the 2nd server address as the authentication database.	0.0.0.0

### TCP Port

Setting	Description	Factory Default
Input the port number	Specify the UDP port.	49

### Share Key

Setting	Description	Factory Default
Input the key	Specify the share key for 2nd server authentication verification.	None

### Authentication Type

Setting	Description	Factory Default
ASCII	ASCII is the authentication type.	CHAP
PAP	PAP is the authentication type.	
CHAP	CHAP is the authentication type.	

### Timeout (sec.)

Setting	Description	Factory Default
Input the value	When waiting for a response from the server, set the amount of time before the device is timed out.	5

### Retry

Setting	Description	Factory Default
Input the value	Set the retry interval when trying to reconnect to a server.	1

When finished, click **APPLY** to save your changes.

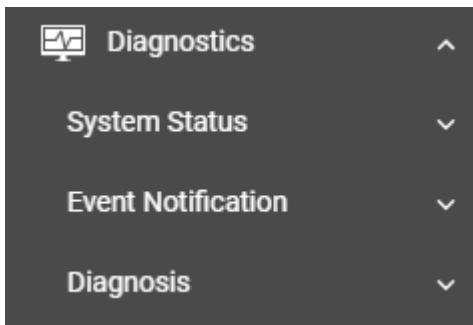


## NOTE

The TACACS+ service will be operated via the 1st server; if it fails, it will run on the 2nd server. In addition, users that are created with the TACACS+ server come with Admin privilege.

# Diagnostics

This section describes the diagnostics functions of Moxa's switch. Click **Diagnostics** on the function menu.




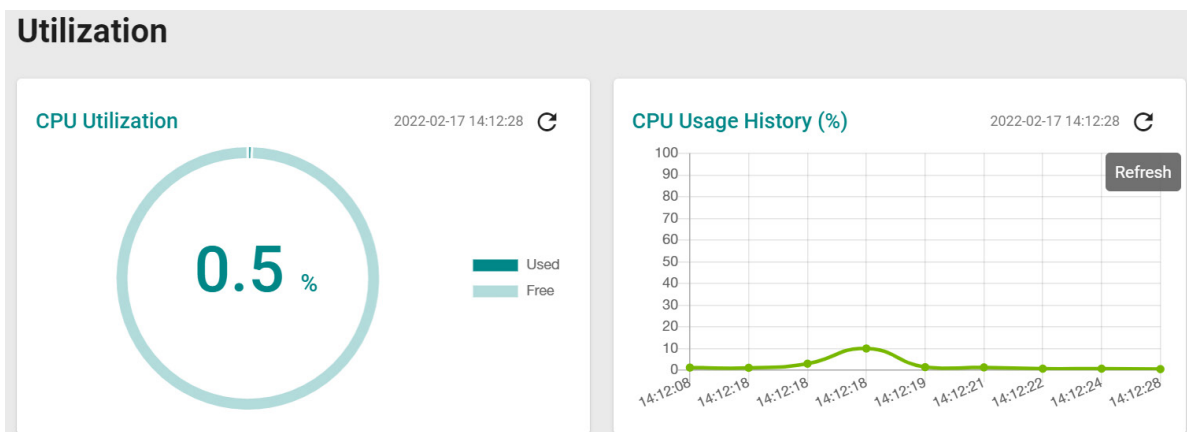
## System Status

This section allows users to view the current system status including **Resource Utilization**, **Statistics**, **Module Information**, and **Intelligent Temp. Control**.



## Utilization

Click **Utilization** on the function menu to view the current utilization status including CPU utilization, memory history, power consumption, and power history. All of the information is displayed via graphics, making it easier for users to view the system status. In addition, a  icon is available on the upper right corner of each figure, which allows users to view the latest status for each function.

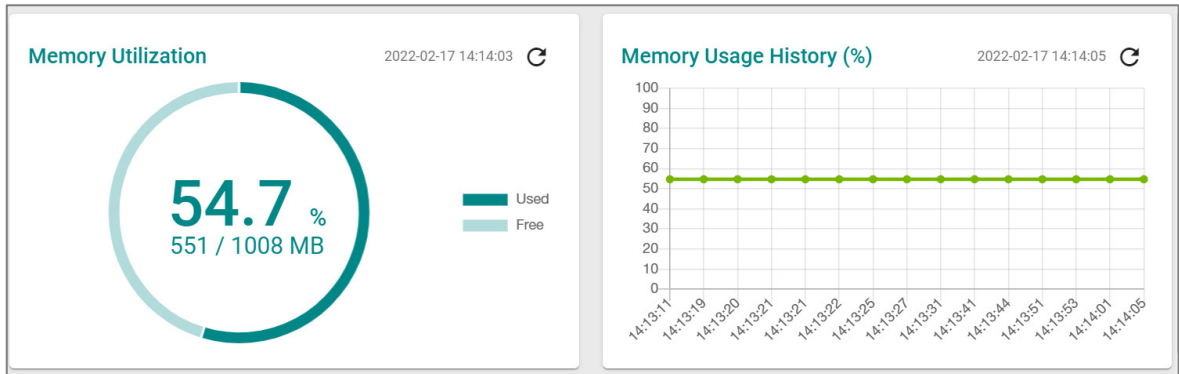


### CPU Utilization

Setting	Description	Factory Default
Read-only	Displays the current utilization of the CPU.	None

### CPU Usage History

Setting	Description	Factory Default
Read-only	Displays the CPU usage history trend in a chart.	None

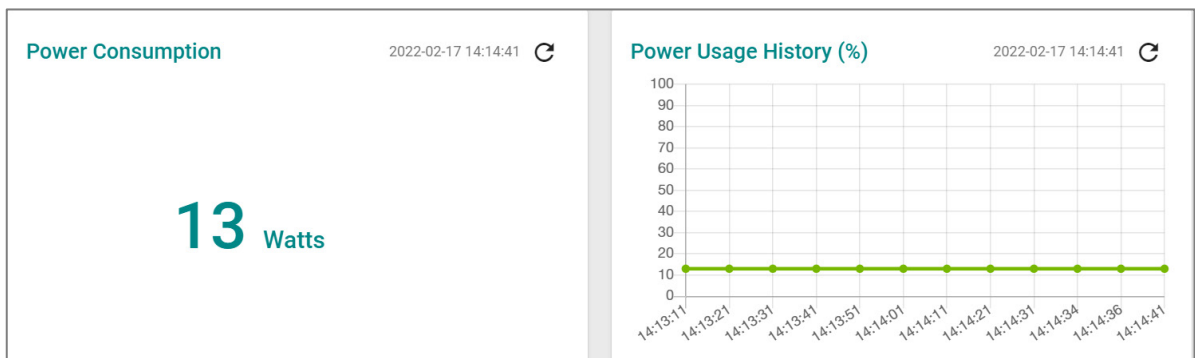


### Memory Utilization

Setting	Description	Factory Default
Read-only	Displays the memory status.	None

### Memory Usage History

Setting	Description	Factory Default
Read-only	Displays the history of the memory usage.	None



### Power Consumption (watt)

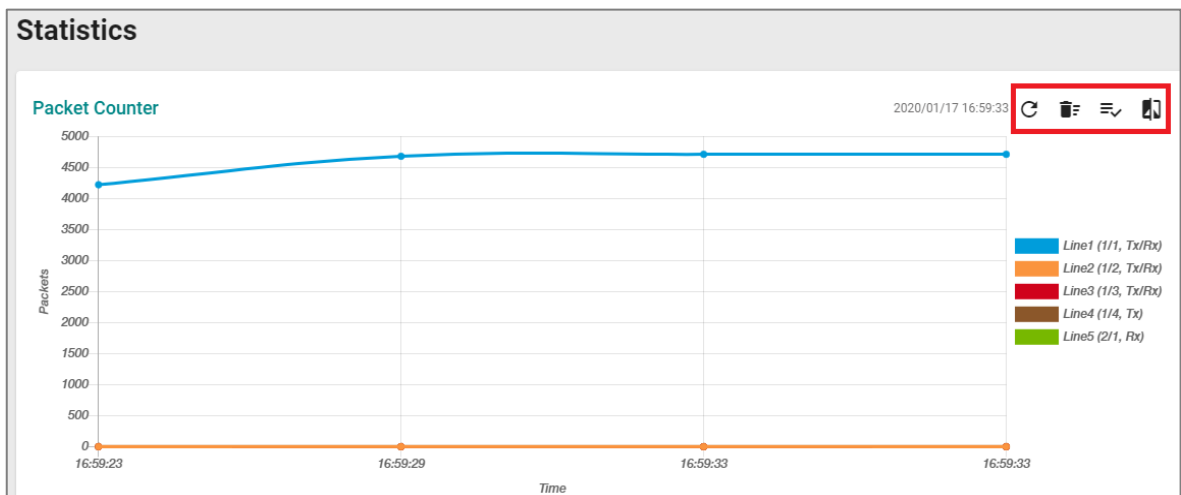
Setting	Description	Factory Default
Read-only	Displays the power consumption status.	None

### Power Usage History






Setting	Description	Factory Default
Read-only	Displays the history of the power usage.	None

## Statistics





Click **Statistics** on the function menu. The first figure shows the packet counter status.



The status of the different ports will be shown in different colors. A maximum of five ports will have their information displayed.

	Line1 (1/1, Tx/Rx)
	Line2 (1/2, Tx/Rx)
	Line3 (1/3, Tx/Rx)
	Line4 (1/4, Tx)
	Line5 (2/1, Rx)

There are four icons on the right upper corner of the page. The table below provides a description for each one.

Item	Name	Description
	Refresh	All statistical data will be refreshed.
	Reset Statistics Graph	The packet counter will be cleared and the graphs will be reset.
	Display Setting	All selected setting items will be shown here.
	Data Comparison	Select the data you want to compare.

### Refreshing the Statistics

Click the **Refresh** icon and all statistical data will be refreshed immediately.

### Resetting Statistics Graph

Click the **Reset** icon and select **CLEAR** to clear the packet counter and reset the graph.

### Reset Statistics Graph

Are you sure to clear all graph data?

CANCEL
CLEAR

## Display Setting

Click the **Display Setting** icon and all settings will be displayed. You can select the display mode from the drop-down list.

**Display Settings**

Display Mode \*  
 Packet Counter ▼

---

Line 1 Monitoring Port \*      Line 1 Sniffer \*  
 1/1 ▼                              Tx/Rx ▼

Line 2 Monitoring Port \*      Line 2 Sniffer \*  
 1/2 ▼                              Tx/Rx ▼

Line 3 Monitoring Port \*      Line 3 Sniffer \*  
 1/3 ▼                              Tx/Rx ▼

Line 4 Monitoring Port \*      Line 4 Sniffer \*  
 1/4 ▼                              Tx ▼

Line 5 Monitoring Port \*      Line 5 Sniffer \*  
 2/1 ▼                              Rx ▼

CANCEL
APPLY

The Monitoring Port is the port you want to view or monitor. The sniffer port is the port that you can choose to view its receiving or transmission status or both.

### Display Mode

Setting	Description	Factory Default
Packet Counter	The packet statistics will be displayed.	Packet Counter
Bandwidth Utilization	The bandwidth statistics will be displayed.	

Click **APPLY** to complete.

## Comparing Data

Click the **Data Comparison** icon and then select the items from the relevant fields.

**Data Comparison**

Benchmark Line \*      Benchmark Line - Time \*  
 ▼                              ▼

---

Comparison Line \*      Comparison Line - Time \*  
 ▼                              ▼

CLOSE

Click **CLOSE** to complete.

The data comparison figure will be shown. Click **CLOSE** to finish.

### Data Comparison

Benchmark Line \*  
1/1, Tx/Rx

Benchmark Line - Time \*  
14:15:18

---

Comparison Line \*  
1/2, Tx/Rx

Comparison Line - Time \*  
14:15:18

Tx Total Octets	0	↓ ↑	▼
Tx Total Packets	0	↓ ↑	▼
Tx Unicast Packets	0	↓ ↑	▼
Tx Multicast Packets	0	↓ ↑	▼
Tx Broadcast Packets	0	↓ ↑	▼

CLOSE

The detailed packet transmission activity for each port can be seen in the table below.

🔍 🔍 🗑️ 🔄 🔍 Search

Port	Tx Total Octets	Tx Total Packets	Tx Unicast Packets	Tx Multicast Packets	Tx Broadcast Packets	Rx Total Octets	Rx Total Packets	Rx Unicast Packets	Rx Multicast Packets
1/1	10877827	7891	7826	64	1	649940	5501	3706	1482
1/2	0	0	0	0	0	0	0	0	0
1/3	0	0	0	0	0	0	0	0	0
1/4	0	0	0	0	0	0	0	0	0

Collision Packets	Late Collision Packets	Excessive Collision Packets	CRC Align Error Packets	Drop Packets	Undersize	Oversize Packets	Fragment Packets	Jabber Packets
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	0	0	0	0	0	0	0	0

**Port:** port number

**Tx Total Octets:** Number of octets transmitted including bad packets and FCS octets. Framing bits are not included.

**Tx Total Packets:** Number of packets transmitted.

**Tx Unicast Packets:** Number of Unicast packets transmitted.

**Tx Broadcast Packets:** Number of good Broadcast packets transmitted. Multicast packets are not included.

**Rx Total Octets:** Number of octets received, including bad packets and FCS octets. Framing bits are not included.

**Rx Unicast Packets:** Number of Unicast packets received.

**Rx Multicast Packets:** Number of Multicast packets received.

**Rx Broadcast Packets:** Number of good Broadcast packets received. Multicast packets are not included.

**Rx Pause Packets:** Number of pause packets received.

**Collision Packets:** Number of collisions received. If Jumbo Frames are enabled, the threshold of Jabber Frames is raised to the maximum size of Jumbo Frames.

**Late Collision Packets:** Number of late collision packets.

**Excessive Collision Packets:** Number of excessive collision packets.

**CRC Align Error Packets:** Number of CRC and Align errors that have occurred.

**Drop Packets:** Number of packets that were dropped.

**Undersize:** Number of undersized packets (less than 64 octets) received.

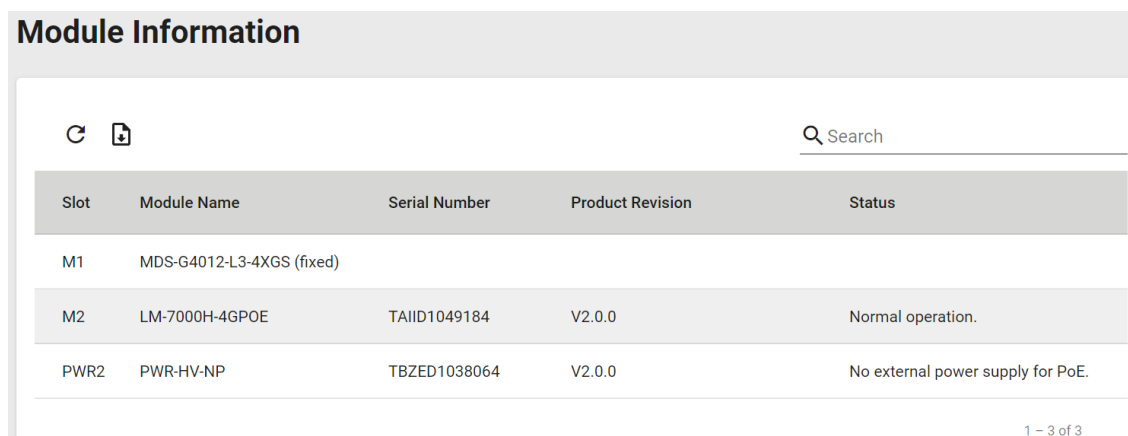
**Oversize Packets:** Number of oversized packets (over 1518 octets) received.

**Fragment Packets:** Number of fragments (packets with less than 64 octets, excluding framing bits, but including FCS octets) received.

**Jabber Packets:** Number of received packets that were longer than 1632 octets. This number excludes frame bits, but includes FCS octets that had either a bad FCS (Frame Check Sequence) with an integral number of octets (FCS Error) or a bad FCS with a non-integral octet (Alignment Error) number.

## Module Information

Click **Module Information** on the function menu to view the current module information of the switch.



The screenshot shows a web interface titled "Module Information". At the top left, there are icons for refresh and download. At the top right, there is a search bar labeled "Search". Below these is a table with the following columns: Slot, Module Name, Serial Number, Product Revision, and Status. The table contains three rows of data. At the bottom right of the table area, it says "1 - 3 of 3".

Slot	Module Name	Serial Number	Product Revision	Status
M1	MDS-G4012-L3-4XGS (fixed)			
M2	LM-7000H-4GPOE	TAIID1049184	V2.0.0	Normal operation.
PWR2	PWR-HV-NP	TBZED1038064	V2.0.0	No external power supply for PoE.

For example, in the figure above, the MDS-G4012-L3 switch is installed in Slot M1 and there is an LM-7000H-4GPOE module installed in Slot M2. In addition, a power module has been installed in Slot PWR2.



### ATTENTION

When a different type of module has been inserted into the switch, we suggest you re-configure the settings, or use reset to default settings. When the same module is inserted into the slot, users do not need to re-configure the settings or use reset to default settings.

# Intelligent Temperature Control

## Intelligent Temperature Control Overview

Electronics overheating for prolonged periods may face negative impacts to functionality and device availability. To prevent or minimize overheating, system temperature can be monitored through intelligent temperature control. In addition to monitoring, the can automatically adjust fan speed based on input from built-in thermal sensors, or trigger temperature alarms and protection features.

Smart temperature controls have the following feature sets:

- **Smart fan:** The fan system provides adequate airflow for cooling. Fan speed will be adjusted automatically based on temperature data from thermal sensors.
- **Smart power:** when the component temperature has overheated, power cut-off feature can be triggered to suspend device's operation to not only cool down the device but also protect components for further damage.

## How intelligent temperature control works

To decrease the hurt from working under inappropriate temperature environment, there are several build-in thermal sensors which offers the temperature parameters to monitor the operating thermal condition of the critical parts. Inside temperature of the device can be affected either by environment temperature changing or by malfunctioning of the device components. By detecting temperature parameters, device can send alarm to notify that the device temperature is high and even trigger corresponding actions.

## System temperature

System temperature represents the average temperature of the device while operating. To monitor the thermal condition of the device, user can set the temperature alarm threshold to notify the central management once the working temperature is higher than expected temperature.

## Fan system

Fan system support **N+M** redundancy. **N** means the number of primary working fan and **M** means the number of standby fans. When the device powers on, all of fan will operate at full speed until the temperature information from all thermal sensors have been collected. Based on build-in algorithm, fan system will adjust all the speed of operating fan to the same duty cycle 0,10,30,50,70 or 100%. Fan speed is in RPM as the unit, and it can be monitored remotely. System will monitor the fan speed and triggered alarm if detecting unexpected speed while enabling the warning notification.

## Power Cut-off

Power Cut-off cuts off network connectivity to reduce power consumption (and corresponding heat production) when temperatures reach a certain threshold. This feature does not turn off the switch, only some of the networking components for the purpose of preventing damage.

If the feature is enabled, when one of critical components has overheated for over 1 min, the system will trigger the power cut-off feature to protect the component from further damage by unexpected high temperature.

When the feature is triggered, switch will trigger the event notification and shut down the in-band ports, and then enter power cut-off status.

During the power cut-off status, few features are still functional for access to check the log and monitor the thermal condition.

- User still can access system information from OOB interface by SSH/Telnet/Web/SNMP
- Keep smart fan control.

After entering the power cut-off status, it should be rebooted manually to release the status and recover.

## Auto Reboot in Power Cut-off

In some cases, it might be difficult to manually reboot the device to release the power cut-off status. Auto Reboot in Power Cut-off feature can help to release after 12 hours of Power Cut-off status.



## Intelligent Temperature control Settings

This section describes how to set up the temperature alarm and enable the features.

Click **Intelligent Temp. Control** on the menu.

Click the **Settings** tab for the settings. You can configure the following parameters to enable the features or set up system temperature alarm.

To apply the settings, configure the following parameters.

### Power Cut-off

Setting	Description	Factory Default
Enabled	Shuts down in-band ports upon detection of overheating of a critical component for 1 minute.	Disabled
Disabled	Disable power cut-off.	

### Auto Reboot in Power Cut-off

Setting	Description	Factory Default
Enabled	Reboot on triggering of power cut-off	Disabled
Disabled	Disable Auto Reboot.	

### System Temperature Alarm

Setting	Description	Factory Default
25 to 70	Specify the alarm threshold temperature in Celsius.	70.00
77 to 158	Specify the alarm threshold temperature in Fahrenheit.	158.00

## Status

Click the Status tab to view the detailed status of system temperature and fan modules.

### Fan modules



Fan Module	Speed (rpm)	Duty Cycle (%)
1	5219	0
2	5150	0
3	5102	0
4	5290	0
5	5063	0
6	5217	0
7	5176	0
8	5259	0

### PWR Fan



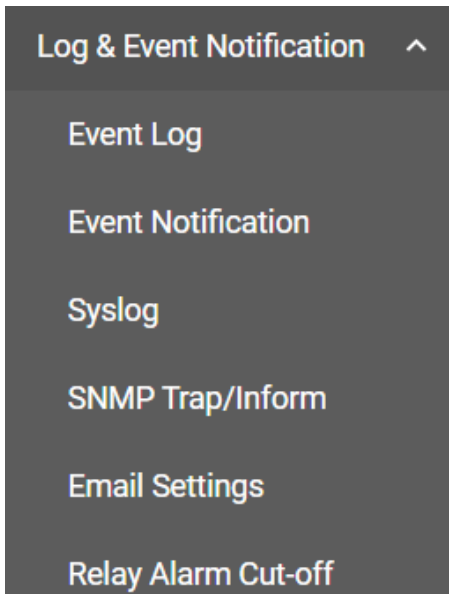
PWR Fan	Speed (rpm)
1	--
2	7968

Refer to the following table for detailed description of each item.

Item	Description
Fan Module	The number of the fan modules on this device.
PWR Fan	The number of the PWR fans on this device.
Speed (rpm)	Shows the speed of the fan in RPM.
Duty Cycle (%)	Show the percentage of the fan runtime for one cycle.

# Log & Event Notification

This section includes the information for **Event Log**, **Event Notification**, **Syslog**, **SNMP Trap/Inform**, **Email Settings**, and **Relay Alarm Cut-off**.



## Event Log

To check event logs, click the **Event Log** tab.

The screenshot shows the "Event Log" interface. At the top, there are three tabs: "Event Log" (selected), "Oversize-Action", and "Backup". Below the tabs are three icons: a refresh icon, a trash icon, and a download icon. On the right side, there is a search bar with a magnifying glass icon and the text "Search". The main area contains a table with the following data:

Index	Bootup Number	Severity	Timestamp	Uptime	Message
1	21	Notice	2018-12-21 19:15:28	0d0h22m2s	Configuration [Web] changed by admin.
2	21	Notice	2018-12-21 19:15:13	0d0h21m47s	Configuration [Web] changed by admin.
3	21	Notice	2018-12-21 18:55:50	0d0h2m24s	[Account:admin] successfully logged in via local.
4	21	Critical	2018-12-21 18:54:18	0d0h0m52s	System has performed a cold start.
5	21	Notice	2018-12-21 18:54:01	0d0h0m35s	Interface vlan1 up.
6	21	Notice	2018-12-21 18:54:01	0d0h0m35s	Port 2/1 link up.
7	21	Warning	2018-12-21 18:53:57	0d0h0m31s	The PTP sync status has changed from DISABLED to FREERUN.
8	20	Notice	2018-12-21 21:23:34	0d2h30m8s	Interface vlan1 down.

## Editing Oversize Action

To edit the event log oversize-action, click the **Oversize-Action** tab.

Configure the following settings when the event log file is full.

### ***Oversize-Action***

Setting	Description	Factory Default
Overwrite the oldest event log	Overwrite the oldest event log.	Overwrite the oldest event log
Stop recording event log	Disable Port Mirror for this port.	

### ***Capacity Warning***

Setting	Description	Factory Default
Enabled	Enable capacity warning event log.	Disabled
Disabled	Disable capacity warning event log.	

### ***Warning Threshold (%)***

Setting	Description	Factory Default
50 to 100	Set the warning threshold as a percentage.	80

Click **APPLY** to save your changes.

## Backing Up Event Logs

Click the **Backup** tab first.

There are four ways to back up your event log files: from a local location of your computer, by remote SFTP server, by remote TFTP server, or by a USB tool.

### Local

Select **Local** from the drop-down list under **Method**. Click **BACKUP**, which will save the event log files to your local computer.

### TFTP Server

Select **TFTP** from the drop-down list under **Method**.

#### Server IP Address

Setting	Description	Factory Default
Input the IP address of the TFTP server	Users can input the IP address of the TFTP server.	None

#### File Name

Setting	Description	Factory Default
Input the backup file name (supports up to 54 characters, including the .ini file extension).	Users can input the file name to back up the event log files.	None

When finished, click **BACKUP** to back up the event log files.

### SFTP Server

Select **SFTP** from the drop-down list of **Method**.

### Server IP Address

Setting	Description	Factory Default
Input the IP address of the SFTP server	Input the IP address of the SFTP server where the event log files will be saved.	None

### File Name

Setting	Description	Factory Default
Input the backup file name (support up to 54 characters, including the .ini file extension).	Input the file name of the event log files	None

### Account

Setting	Description	Factory Default
Input the account of the SFTP server	An account must be provided to authorize the SFTP server for secure connection.	None

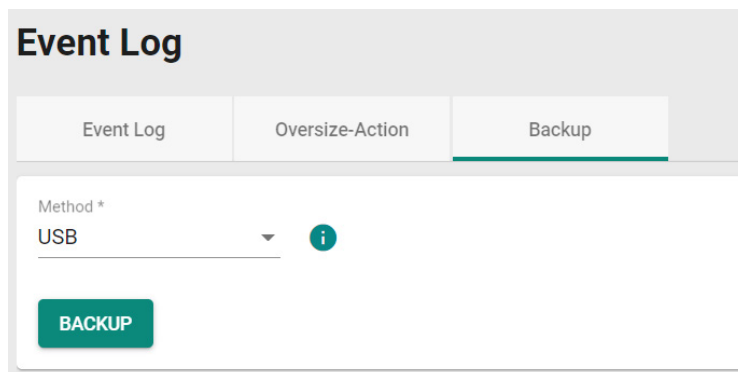
### Password

Setting	Description	Factory Default
Input the passwords for the SFTP server	The password has to be specified in order to authorize the SFTP Server for secure connection.	None

When finished, click **BACKUP** to back up the event log files.

## USB

Select **USB** from the drop-down list under **Method**.



The screenshot shows a web interface for configuring event logs. At the top, there are three tabs: 'Event Log', 'Oversize-Action', and 'Backup'. The 'Event Log' tab is active. Below the tabs, there is a 'Method \*' dropdown menu with 'USB' selected. To the right of the dropdown is an information icon (i). At the bottom of the configuration area, there is a green 'BACKUP' button.

Insert a Moxa's ABC-02 USB-based configuration tool onto the USB port of the switch, click **BACKUP** to back up the event log files.



## Note


If you have difficulty using the ABC-02 configuration tool, check if **USB Function** has been enabled in **Hardware Interfaces** section.

## Auto Backup of Event Logs

To enable automatic backup, select **Enabled** from the drop-down list. Click **APPLY** to back up the event log files automatically.

### Auto Backup of Event Logs



Automatically Back Up \*






Enabled 

**APPLY**

## Event Notification

There are two functions within Event Notification: **System and Function**, and **Port**.

In the **Event Notification** menu, click the **System and Function** tab, and then click the  icon on the specific event you want to configure. For example, select the  icon for warm start when the switch reboots.

Event Notification					
System and Function		Port			
Group	Event Name	Enabled	Severity	Registered Action	
	General	Warm start	Enabled	Notice	Trap, Email
	General	Password changed	Enabled	Notice	Trap, Email
	General	Login success	Enabled	Notice	Trap, Email
	General	Configuration changed	Enabled	Notice	Trap, Email
	General	Configuration imported	Enabled	Notice	Trap, Email

Configure the following settings.

### Edit Event Notification

Event Name  
Cold start  
.....

Enabled \*  
Enabled ▼

Registered Action  
Trap, Email ▼

CANCEL
APPLY

**Enable**



Setting	Description	Factory Default
Enabled	Enable Event Notification for this event.	Enabled
Disabled	Disable Event Notification for this event.	

**Registered Action**

Setting	Description	Factory Default
Trap	Send SNMP Trap for event notifications.	Trap/Email
Email	Send an email for event notifications.	
MGMT Relay	Trigger MGMT Relay for event notifications.	
PWR1 Relay	Trigger PWR1 Relay for event notifications.	
PWR2 Relay	Trigger PWR2 Relay for event notifications.	

When finished, click **APPLY** to save your changes.






In addition, use the same method to edit other events, such as login lockout, warm start, password changed, etc.

Next, in the **Event Notification** menu, click the **Port** tab, and then click the  icon on the specific port status on Event Name. For example, select the  icon for event notifications when the port status is on.

### Event Notification

System and Function

Port

	Event Name	Enable	Severity	Registered Action
	Port On	Enabled	Notice	Trap, Email
	Port Off	Enabled	Notice	Trap, Email
	Port shutdown by Port Security	Enabled	Warning	Trap, Email
	Port shutdown by Rate Limit	Enabled	Warning	Trap, Email
	Port recovery by Rate Limit	Enabled	Warning	Trap, Email



Configure the following settings.

### Edit Event Notification

Event Name  
Port On  
.....

Enabled \*  
Enabled ▼

Registered Action  
Trap, Email ▼

Registered Port  
All Ports ▼

CANCEL
APPLY

#### Event Name

Setting	Description	Factory Default
Event name	Show the event name of the port. (read only)	Event name of each port

#### Enable

Setting	Description	Factory Default
Enabled	Enable Event Notification for this event.	Enabled
Disabled	Disable Event Notification for this event.	

#### Registered Action

Setting	Description	Factory Default
Trap	Send SNMP Trap for event notifications.	Trap/Email
Email	Send an email for event notifications.	
MGMT Relay	Trigger MGMT Relay for event notifications.	
PWR1 Relay	Trigger PWR1 Relay for event notifications.	
PWR2 Relay	Trigger PWR2 Relay for event notifications.	

#### Registered Port

Setting	Description	Factory Default
Select port(s) from the drop-down list	Specify the port(s) that use the registered action.	All Ports

When finished, click **APPLY** to save your changes.

In addition, use the same method to edit other events such as, port status is off, port shutdown by port security, and port recovery by rate limit, etc.

Check the following table for the severity degree of each event.

Event Name	Severity
802.1X Auth Failed	Warning
ABC-02 is inserted or unplugged	Notice
ABC-03 is inserted or unplugged	Notice
Account log out	Notice
Account removed	Notice
Account settings changed	Notice
Announce message with different interval	Warning
Announce timeout	Warning
Check if hardware revision is valid	Notice
Check if it is a known power module	Warning
Cold start	Critical

Event Name	Severity
Configuration changed	Notice
Configuration exported	Notice
Configuration imported	Notice
Coupling changed	Warning
DI off	Notice
DI on	Notice
Dual homing path changed	Warning
Event log export	Notice
Firmware upgrade failed	Warning
Firmware upgrade successful	Notice
Grand Master changed	Warning
Hardware revision is not allowed	Error
Interface link down	Notice
Interface link up	Notice
LLDP table changed	Info
Log capacity threshold	Warning
Login failed	Warning
Login lockout	Warning
Login successful	Notice
Low input voltage	Warning
Master changed	Warning
Master mismatch	Warning
module change	Notice
Module Initialized Fail	Error
Module inserted	Notice
Module removed	Notice
MSTP new port role	Warning
MSTP root changed	Warning
MSTP topology changed	Warning
OSPF DR router adjacency changed	Notice
OSPF interface DR changed	Notice
OSPF interface ISM became DR	Notice
Over power budget limit	Warning
Packet dropped by Port Security	Warning
Password changed	Notice
PD no response	Error
PD over-current	Error
PD power off	Notice
PD power on	Notice
Port Link Down	Notice
Port Link Up	Notice
Port recovery by Rate Limit	Warning
Port shutdown by Loop	Critical
Port shutdown by Port Security	Warning
Port shutdown by Rate Limit	Warning
Port state change	Info
Power detection failure	Warning
Power module inserted	Notice
Power module removed	Notice
Power Off->On	Notice
Power On->Off	Notice
PTP message with the wrong domain number	Warning
Redundant port health check failed	Error
Relay Override message	Notice
Relay Triggered message	Notice
RMON failing alarm	Warning
RMON raising alarm	Warning
RSTP invalid BPDU	Warning

Event Name	Severity
RSTP migration	Warning
RSTP new port role	Warning
RSTP root changed	Warning
RSTP topology changed	Warning
Send message failed	Warning
SSH Key generated	Notice
SSL certification changed	Notice
Sync status changed	Warning
Topology changed (RSTP)	Warning
Topology changed (Turbo Ring)	Warning
Topology changed (MSTP)	Warning
Unknown module	Warning
VRRP Master changed	Warning
Warm start	Notice
When the trust host moves, it will send a log to Moxa log handler.	Warning

# Syslog

## General Settings

Click **Syslog** on the function menu and configure the following settings.

### Syslog

- General
- Authentication

Syslog \*  
Disabled

Syslog Server 1 \*      Authentication \*  
Disabled      Disabled

Address 1      UDP Port  
514  
1 - 65535

Syslog Server 2 \*      Authentication \*  
Disabled      Disabled

Address 2      UDP Port  
514  
1 - 65535

Syslog Server 3 \*      Authentication \*  
Disabled      Disabled

Address 3      UDP Port  
514  
1 - 65535

**APPLY**

### Logging Enable

Setting	Description	Factory Default
Enabled	Enable logging.	Disabled
Disabled	Disable logging.	

### Syslog Server 1

Setting	Description	Factory Default
Enabled	Enable the 1st log server.	Disabled
Disabled	Disable the 1st log server.	

### Address 1

Setting	Description	Factory Default
IP Address	Input the IP address of the Syslog 1st server that is used by your network.	None

### UDP Port

Setting	Description	Factory Default
1 to 65535	Input the UDP port number.	514

### Syslog Server 2

Setting	Description	Factory Default
Enabled	Enable the 2nd syslog server.	Disabled
Disabled	Disable the 2nd syslog server.	

### Address 2

Setting	Description	Factory Default
IP Address	Input the IP address of Syslog 2nd server that is used by your network.	None

### UDP Port

Setting	Description	Factory Default
1 to 65535	Input the UDP port number.	514

### Syslog Server 3

Setting	Description	Factory Default
Enabled	Enable the 3rd syslog server.	Disabled
Disabled	Disable the 3rd syslog server.	

### Address 3

Setting	Description	Factory Default
IP Address	Input the IP address of the Syslog 3rd server that is used by your network.	None

### UDP Port


Setting	Description	Factory Default
1 to 65535	Input the UDP port number.	514

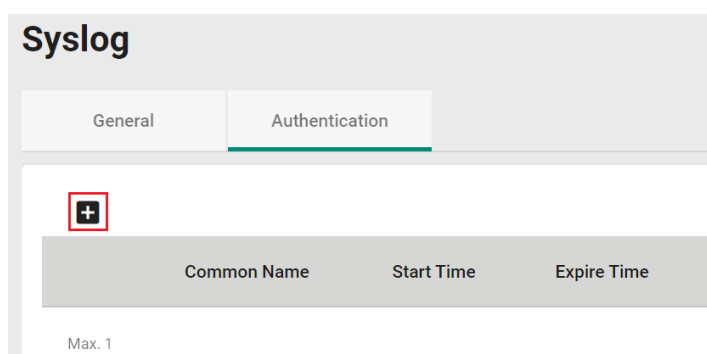
When finished, click **APPLY** to save your changes.



## NOTE


If the syslog server cannot receive the previous logs, it is possible that the receiving port of the syslog server is not ready. We suggest you enable the Linkup Delay function to delay the log delivery time.


Click **Authentication** tab and the  icon the function menu.




Configure the following settings.


### Add Certificate and Key

Client Certificate \* 


Client Key \* 

CA Key \* 

#### Client Certificate

Setting	Description	Factory Default
Click the  icon and select the file from your computer.	Import the client certificate file.	None

#### Client Key

Setting	Description	Factory Default
Click the  icon and select the file from your computer.	Import the client key file.	None


#### CA Key

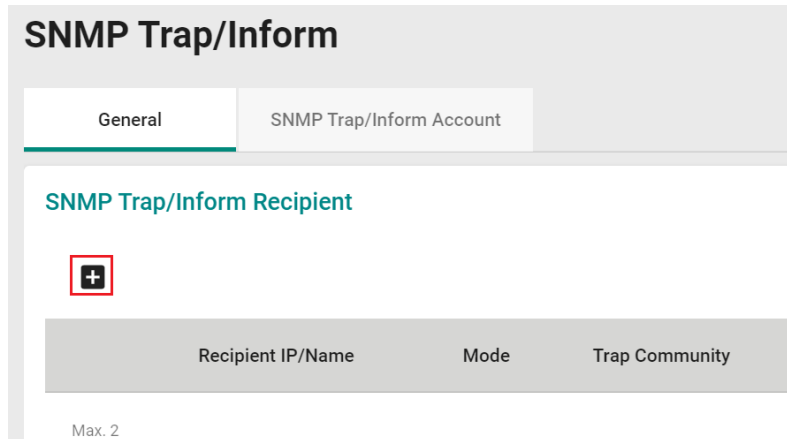
Setting	Description	Factory Default
Click the  icon and select the file from your computer.	Import the CA key file.	None

When finished, click **CREATE** to save your changes.

# SNMP Trap/Inform

## SNMP Trap Host Settings

SNMP Trap allows an SNMP agent to notify the NMS of a significant event. The switch supports two SNMP modes: **Trap** mode and **Inform** mode. Click **SNMP Trap/Inform** on the menu, and then select the  icon on the page.



Configure the following settings.

### Create Host Settings

Recipient IP/Name \*  
0 / 32

Mode \*  
▼

Trap Community \*  
At least 4 characters 0 / 32

### Recipient IP/Name

Setting	Description	Factory Default
Input a recipient IP or name, (max. 32 characters)	Specify the name of the primary trap server used by your network.	None

### Mode


Setting	Description	Factory Default
Trap V1	Set the trap version to Trap V1.	None
Trap V2c	Set the trap version to Trap v2c.	
Inform V2c	Set the inform version to Inform V2c.	
Trap V3	Set the trap version to Trap V3.	
Inform V3	Set the inform version to Inform V3.	

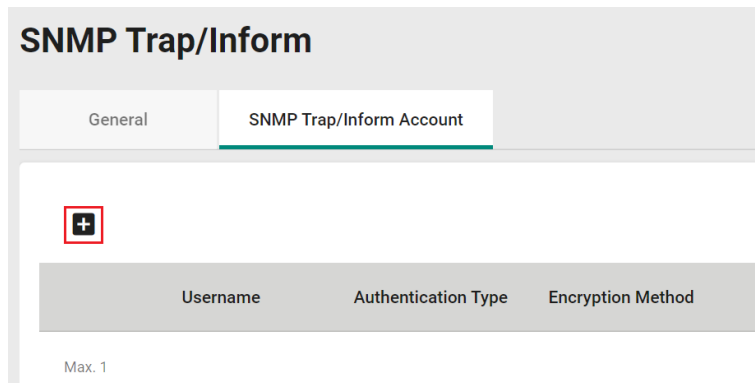
### Trap Community

Setting	Description	Factory Default
At least 4 characters, (max. 30 characters)	Specify the community string that will be used for authentication.	None

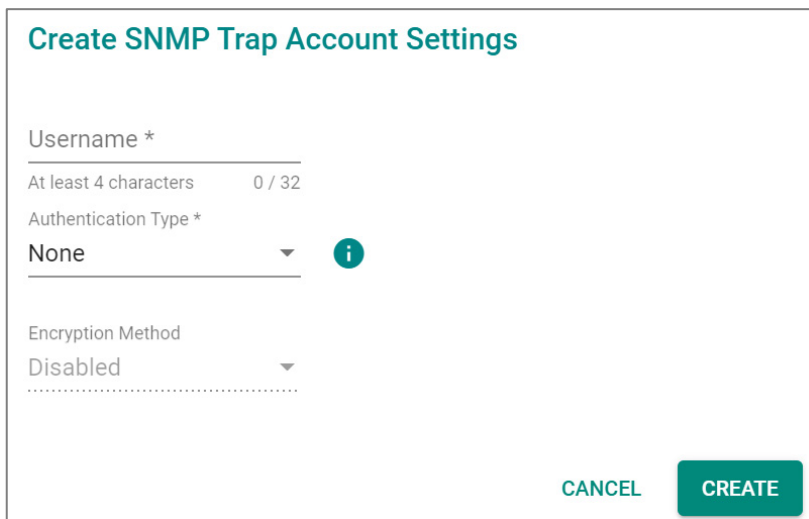
When finished, click **CREATE**.

## SNMP Trap Account Settings

Click **SNMP Trap/Inform** on the menu, and then click **SNMP Trap/Inform Account** tab. Next click the  icon on the page.



Configure the following settings.



### **Username**

Setting	Description	Factory Default
At least 4 characters, (max. 30 characters)	Input a username.	None

### **Authentication type**

Setting	Description	Factory Default
None	No authentication type will be used.	None
MD5	MD5 is the authentication type.	
SHA	SHA is the authentication type.	



### Authentication Password

Setting	Description	Factory Default
8 to 64 characters	Input the authentication password.	None

### Encryption Method

Setting	Description	Factory Default
Disabled	Disable the encryption method.	None
DES	DES is the encryption method.	
AES	AES is the encryption method.	

### Encryption Key

Setting	Description	Factory Default
8 to 64 characters	Enable data encryption.	None

When finished, click **CREATE**.

## SNMP Inform Settings

First select **SNMP Trap/Inform** on the menu and then click **General**. On the bottom of the page, find the following figure for the settings.

**SNMP Inform Settings**

Inform Retry \*  
3  
1 - 99 times

Inform Timeout \*  
10  
1 - 300 sec.

**APPLY**

Configure the following settings.

### Inform Retry

Setting	Description	Factory Default
1 to 99	Input the retry value.	3

### Inform Timeout

Setting	Description	Factory Default
1 to 300	Input the timeout value.	10

When finished, click **APPLY** to save your changes.

## Email Settings

Select **Email Settings** on the function menu and configure the following settings.

### Email Settings

Mail Server \*  
0.0.0.0

TCP Port \*  
25  
1 - 65535

Username Password

0 / 60 0 / 60

TLS Enable \*  
Disabled ▼

Sender Address  
admin@localhost.com  
19 / 63

1st Recipient Email Ad... 2nd Recipient Email Ad... 3rd Recipient Email Ad...

0 / 63 0 / 63 0 / 63

4th Recipient Email Ad... 5th Recipient Email Ad...

0 / 63 0 / 63

**APPLY**

### Mail Server

Setting	Description	Factory Default
IP address or URL	The IP Address or URL of the email server.	0.0.0.0

### TCP Port

Setting	Description	Factory Default
1 to 65535	The TCP port number of your email server.	25

### Username

Setting	Description	Factory Default
Max. 60 characters	Your email account name.	None

### Password

Setting	Description	Factory Default
Max. 60 characters	Your email account password.	None

### TLS Enable

Setting	Description	Factory Default
Enabled	Enable TLS (Transport Layer Security).	Disabled
Disabled	Disable TLS (Transport Layer Security).	

### Sender Address

Setting	Description	Factory Default
Max. 60 characters	The sender's email address.	admin@localhost.com

### 1st to 5th Email Addresses

Setting	Description	Factory Default
Max. 63 characters	You can set up to five email addresses to receive alert emails from the Moxa switch.	None

When finished, click **APPLY** to save your changes.

## Relay Output Overview

A relay is an electrically operated switch that often uses an electromagnet to mechanically operate a switch. Relays are used to control a circuit by a separate low-power signal, or where several circuits must be controlled by one signal. This is typically safe when the problem or malfunction occurs in a remote device.

Moxa's switches offer three sets of relay outputs, one on the mainboard and two on the power modules, providing the secured protection of the remote switch and secure data communication. In addition, email notifications can also be sent to inform system administrators to perform further checks and maintenance.

## Relay Output Settings and Status

To select Relay Output as the event notifications, click **Relay Output** on the function menu.

### Relay Alarm Cut-off

MGMT Relay

PWR1 Relay

PWR2 Relay

**APPLY**

### Relay Output

Setting	Description	Factory Default
MGMT Relay	Trigger MGMT Relay for event notifications.	None
PWR1 Relay	Trigger PWR1 Relay for event notifications.	
PWR2 Relay	Trigger PWR2 Relay for event notifications.	

When finished, click **APPLY** to save your changes.

Go to the **Event Log** section, you can view the relay alarms you have selected to be cut off.

### Event Log

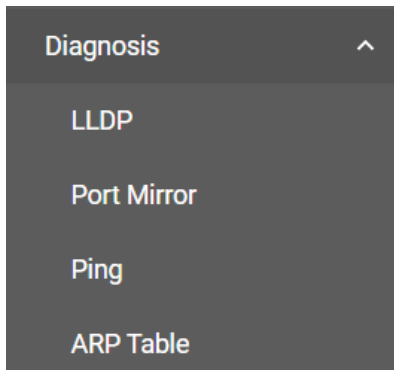
Event Log    Oversize-Action    Backup

🔄 🗑️ 📄

Index	Bootup Number	Severity	Timestamp	Uptime	Message
1	23	Notice	2018-12-21 18:56:56	0d0h3m30s	PWR1 Relay relay alarm has been cut off.
2	23	Notice	2018-12-21 18:56:55	0d0h3m30s	PWR2 Relay relay alarm has been cut off.
3	23	Notice	2018-12-21 18:56:55	0d0h3m30s	MGMT Relay relay alarm has been cut off.

## Diagnosis

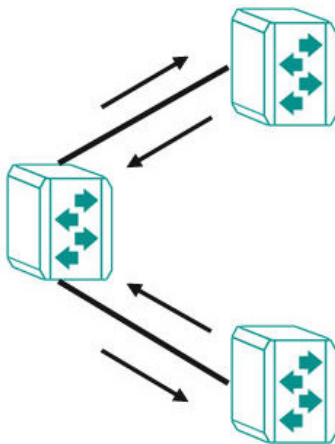
This section explains the configurations for system diagnoses such as **LLDP**, **Port Mirror**, **Ping**, and **ARP Table**.



### LLDP Overview

LLDP is an OSI Layer 2 protocol defined by IEEE 802.11AB. LLDP standardizes the self-identification advertisement method, and allows each networking device, such as a Moxa managed switch, to periodically send its system and configuration information to its neighbors. Because of this, all LLDP devices are kept informed of each other's status and configurations. 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.



## LLDP Settings and Status

Click **LLDP** on the menu and then select the **Setting** tab to configure the following settings.

### LLDP

Settings

Status

Enable\*  
Enabled ▼

LLDP Version\*  
2005 ▼

Transmit Interval\*  
30

5 - 32768 sec.

Notification Interval\*  
5

5 - 3600 sec.

Tx Delay\*  
2

1 - 8192 sec.

Reinitialization Delay\*  
2

1 - 10 sec.

Holdtime Multiplier\*  
4

2 - 10 times

Chassis ID Subtype\*  
MAC-Address ▼

APPLY

### Enable

Setting	Description	Factory Default
Enabled	Enable LLDP.	Disabled
Disabled	Disable LLDP.	

### LLDP Version

Setting	Description	Factory Default
Show the LLDP version	Show the LLDP version automatically.	2005

### Transmit Interval (sec.)

Setting	Description	Factory Default
5 to 32768	Set the transmit interval of LLDP messages	30

### Notification Interval (sec.)

Setting	Description	Factory Default
5 to 3600	Specify the notification interval.	5

### Tx Delay (sec.)

Setting	Description	Factory Default
1 to 8192	Specify the Tx delay interval.	2

### Reinitialization Delay (sec.)

Setting	Description	Factory Default
1 to 10	Specify the LLDP reinitialization delay interval.	2


### Holdtime Multiplier





Setting	Description	Factory Default
2 to 10	Specify the holdtime multiplier value.	4

### Chassis ID Subtype

Setting	Description	Factory Default
Chassis-Component	Select Chassis-Component as Chassis ID subtype.	Mac-Address
If-Alias	Select If-Alias as Chassis ID subtype.	
Port-Component	Select Port-Component as Chassis ID subtype.	
MAC-Address	Select MAC-Address as Chassis ID subtype.	
Network-Address	Select Network-Address as Chassis ID subtype.	
If-Name	Select If-Name as Chassis ID subtype.	
Local	Select Local as Chassis ID subtype.	

When finished, click **APPLY** to save your changes.

Each port for the LLDP settings can also be configured. Select the  icon for the port you want to configure.

Port	Port Status
 1/1	Tx and Rx
 1/2	Tx and Rx
 1/3	Tx and Rx
 1/4	Tx and Rx

Configure the following settings.

#### Edit Port 1/1 Settings

Port Status \*  
Tx and Rx ▼

Subtype \*  
If-Alias ▼

TLV \*  
Basic ▼


**Transmit TLVs**

Port Description

System Name

System Description

System Capability

Copy Configurations ... ▼ 

CANCEL APPLY

### Port Status

Setting	Description	Factory Default
Tx Only	Set Tx as the port status.	Tx and Rx
Rx Only	Set Rx as the port status.	
Tx and Rx	Set both Tx and Rx as the port status.	

### Subtype

Setting	Description	Factory Default
If-Alias	Select If-Alias as the subtype.	If-Alias
Port-Component	Select Port-Component as the subtype.	
MAC-Addr	Select MAC-Address as the subtype.	
If-Name	Select If-Name as the subtype.	
Local	Select Local as the subtype.	

### TLV

Setting	Description	Factory Default
Basic	Set TLV as Basic.	Basic
802.1	Set TLV as 802.1.	
802.3	Set TLV as 802.3.	

### Transmit TLVs

Setting	Description	Factory Default
Port Description	Add a port description for the TLV.	Port Description System Name
System Name	Add a system name for the TLV.	
System Description	Add a system description for the TLV.	
System Capability	Add a system capability for the TLV.	

### Copy Configurations to Port

Setting	Description	Factory Default
Select the port from the list	Copy the same configurations to other port(s).	None

When finished, click **APPLY** to save your changes.

To view the LLDP status, click the **Status** tab on the LLDP page, and the status of all LLDP will be shown on the page.

## LLDP

Settings Status

### Local Information

LLDP  
Enabled

LLDP Version  
v1(2005)

Chassis ID Subtype  
MAC-Address

Chassis ID  
00:e0:55:00:00:00

### Local Timer

Transmit Interval  
30 (sec.)

Notification Interval  
5 (sec.)

Tx Delay  
2 (sec.)

Reinitialization Delay  
2 (sec.)

Holdtime Multiplier  
4 (times)

### Remote Table Statistics

Last Change Time (ms)  
4072700

Inserts  
4

Drops  
0

Delete  
3

Ageouts  
0

Refer to the following table for the detailed description of each item.

Local Information	
Enable	Show if LLDP has been enabled or disabled.
LLDP Version	Show the LLDP version.
Chassis ID Subtype	Show the chassis ID subtype.
Chassis ID	Show the chassis ID.

Local Timer	
Transmit Interval (sec.)	The interval between regular LLDP packet transmissions.
Notification Interval (sec.)	The interval that notifications will be sent.
Tx Delay (sec.)	The delay period between successive LLDP frame transmissions initiated by changes.
Reinitialization Delay (sec.)	The interval an LLDP port waits before re-initializing an LLDP packet transmission.
Holdtime Multiplier	The amount of time that the receiving device holds an LLDP packet before discarding it.

Remote Table Statistics	
Last Change Time (ms.)	The last time the remote table changed.
Inserts	How many inserts have occurred.
Drop	How many drops have occurred.
Delete	How many deletes have occurred.
Ageouts	How many ageouts have occurred.

To view the LLDP status for a specific port, click the detailed information icon on the port. All information will be shown on the right side of the page.

The screenshot displays a network management interface with a table of ports and a detailed information panel on the right. The table has columns for Port, Tx Status, Rx Status, Neighbor Port ID, Neighbor Chassis ID, and Port Description. The first row, representing port 1/1, has a detailed information icon highlighted with a red box. The detailed information panel on the right is also outlined in red and contains the following sections:

- Port Local Interface**
  - Port ID SubType: Chassis-Component
  - Port ID: Eth1/1
  - Port Description: Ethernet Interface Port 01
- Extended 802.1 TLV**
  - Port VLAN ID: 1
  - VLAN ID / Name: 1 /
- Extended 802.3 TLV**
  - Link Aggregation Status: Disabled
  - Aggregated Port ID: 0
  - Maximum Frame Size: 1518



# Port Mirror

## Port Mirror Overview

The **Port Mirror** 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.

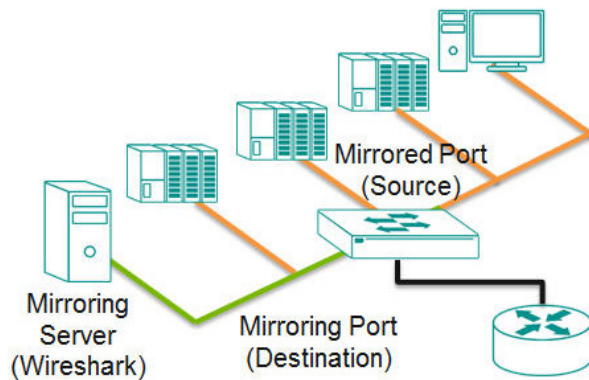
The Port Mirror function includes two features:

**SPAN (Switched Port Analyzer):** Mirroring data of monitored ports to multiple terminal ports on the same switch. Five sessions are allowed to be configured in a switch.

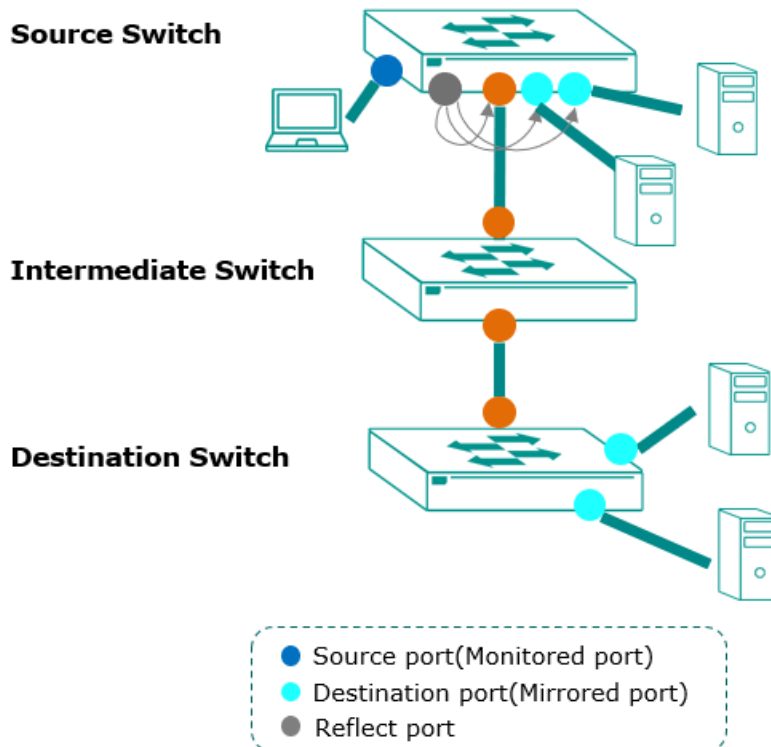
**RSPAN (Remote Switched Port Analyzer):** Mirroring data of monitored ports on one switch to multiple terminal ports on the other switches. Two sessions are allowed to be configured in a switch.

## How Port Mirror Works

**SPAN** can be configured to copy packets from various ports to a single port or multiple ports, so that users can check if there are problems occurring in these ports. For example, the following figure demonstrates how the packets transmitted in the four mirrored ports (marked in orange) are copied (mirrored) to a single mirroring port (marked in green). These packets will be sent to a monitoring computer and then software is used to check if there is something wrong with these packets. It is a useful function to troubleshoot or debug a network data transmission issue.



**RSPAN** can be configured to copy packets from various ports in one or more source switches through intermediate switches to a single or multiple port(s) to destination switches. The PC or monitor server can be connected to destination ports in the destination switch to receive the copy of the original monitored traffic. For example, the following figure demonstrates how the packets transmitted in mirrored ports (marked in blue) are copied (mirrored) through an intermediate switch to two mirroring ports (marked in green).

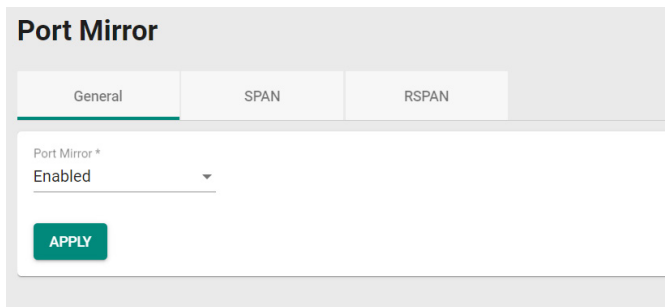


- Users can set source ports in one or more RSPAN source switches. Enable reflect port for multiple designated ports, or disable reflect port for a single designated port.
- Users can configure RSPAN VLAN for monitored traffic to be labeled with a RSPAN VLAN tag and send to an RSPAN destination switch via trunk ports.
- Users can connect a PC that has the server monitoring feature for the ports that are set to be the destination ports to receive the monitored traffic.
- The monitor traffic will be stripped off RSPAN VLAN tag and then the PC or monitor server will receive a copy of the original monitored traffic.

## Port Mirror Settings

The Port Mirror function includes SPAN and RSPAN which share the same global settings.

Click **Port Mirror** on the menu and then configure the settings.




The screenshot shows the 'Port Mirror' configuration page with the 'General' tab selected. The 'Port Mirror' dropdown menu is set to 'Enabled'. An 'APPLY' button is visible at the bottom left.

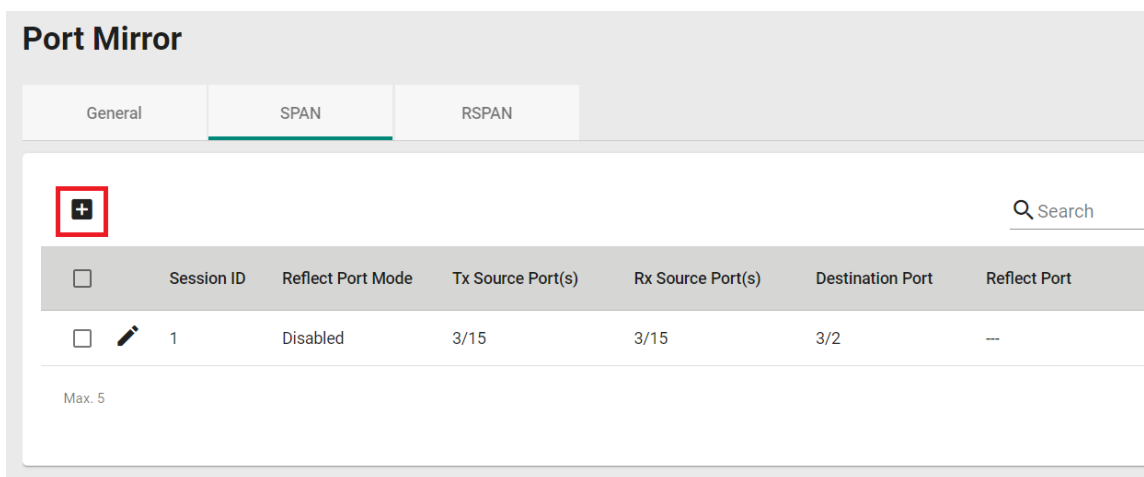
### Port Mirror

Setting	Description	Factory Default
Enabled	Enable Port Mirror.	Enabled
Disabled	Disable Port Mirror.	

When finished, click **APPLY** to save your changes.

## Configure SPAN

To configure the SPAN settings, click the SPAN tab, and then click the  icon.



The screenshot shows the 'Port Mirror' configuration page with the 'SPAN' tab selected. A red box highlights a plus icon in the top left corner of the table area. The table below has columns for Session ID, Reflect Port Mode, Tx Source Port(s), Rx Source Port(s), Destination Port, and Reflect Port. A search bar is located in the top right corner.

<input type="checkbox"/>	Session ID	Reflect Port Mode	Tx Source Port(s)	Rx Source Port(s)	Destination Port	Reflect Port
<input type="checkbox"/>	1	Disabled	3/15	3/15	3/2	---

Max. 5

Configure the following settings.

### Create Session

Session ID \* ▼

---

Reflect Port Mode \* ▼

---

Tx Source Port(s) ▼      Rx Source Port(s) ▼

---

Destination Port \* ▼

---

Either the TX or RX source ports need to be selected.

CANCEL
CREATE

#### **Session ID**

Setting	Description	Factory Default
Select from the drop-down list	Select the session ID from the dropdown list (1 to 5). SPAN and RSPAN share 7 sessions, SPAN uses 1 to 5, and RSPAN uses 6 and 7.	None

#### **Reflect Port Mode**

Setting	Description	Factory Default
Enable	Enable Reflect Port Mode and configure the Reflect Port for mirroring packets to multiple destination ports.	None
Disable	Disable the Reflect Port Mode for mirroring packets to a single destination port.	

#### **Tx Source Port**

Setting	Description	Factory Default
Select the port from the list	Select this option to monitor only those data packets being sent out through the switch's port.	None

#### **Rx Source Port**

Setting	Description	Factory Default
Select the port from the list	Select this option to monitor only those data packets coming into the switch's port.	None

#### **Reflect Port**

Setting	Description	Factory Default
Select the port from the list	Specify the port as the destination port.	None

#### **Destination Port**

Setting	Description	Factory Default
Select the destination port from the list	Specify this port as the Reflect Port after enabling Reflect Port Mode for mirroring packets to multiple destination ports. This port is specifically reserved for Reflect Port use, please do not configure for other use.	None

When finished, click **CREATE** to save your changes.

The following steps demonstrate how to copy packets from one or more source port(s) (monitored ports) to a single destination port (mirror port):

1. Select Session ID from drop list (1 to 5)
2. Disable Reflect Port Mode
3. Select the monitored packet source port(s), you can select either Tx source port(s) or Rx source port(s), or both.
  - If Tx source port(s) is selected, the egress traffic on the port(s) will be mirrored to the destination port.
  - If the Rx source port(s) is selected, the ingress traffic on the port(s) will be mirrored to the destination port.
4. Select the destination port, which is required to be access port.



## NOTE

The duplication of source port(s) configured in different sessions is not allowed. The duplication of source port(s) and destination ports in different sessions is not allowed.

The following steps demonstrate how to copy packets from one or more source port(s) (monitored ports) to multiple destination ports:

1. Select Session ID from drop list (1~5)
2. Enable Reflect Port Mode
3. Select the monitored packet source port(s), you can select either Tx source port(s) or Rx source port(s), or both. The source port(s) must be the access port(s).
  - If Tx source port(s) is selected, the egress traffic on the port(s) will be mirrored to the reflect port.
  - If the Rx source port(s) is selected, the ingress traffic on the port(s) will be mirrored to the reflect port.
4. Select the reflect port, which is required to be an access port. The port is specifically reserved for Reflect Port use, please do not configure for other use.
5. Go to the VLAN page, configure the port(s) required to receive the packets from source ports as the member port of the same VLAN ID as reflect port.



## NOTE

The duplication of source port(s) configured in different sessions is not allowed. The duplication of source port(s), reflect port, and destination ports in different sessions is not allowed.

## Configure RSPAN

To configure the RSPAN settings, click RSPAN.

Configure the following settings. Users need to decide the switch role for RSPAN first, the switch roles are Source switch, Intermediate switch, and Destination switch.

### RSPAN Intermediate Role

Setting	Description	Factory Default
Enable	Enable the RSPAN intermediate role if the switch role is intermediate role.	Disabled
Disable	Disable the RSPAN intermediate role if the switch role is the source or destination role.	

If you enable the RSPAN intermediate role, the existing RSPAN session in this switch will be deleted. Click **GOT IT** to continue.

**Enable RSPAN Intermediate Role**

If this setting is applied, all existing RSPAN Sessions will be deleted.


CANCEL
**GOT IT**

### RSPAN Intermediate 1st VLAN ID

Setting	Description	Factory Default
Select the port from the list	Specify the 1st VLAN ID as the RSPAN intermediate VLAN ID. The RSPAN intermediate VLAN ID cannot be the management VLAN ID.	None

### RSPAN Intermediate 2st VLAN ID

Setting	Description	Factory Default
Select the port from the list	Specify the 2st VLAN ID as the RSPAN intermediate VLAN ID. The RSPAN intermediate VLAN ID cannot be the management VLAN ID.	None

Next, click  icon to create the session.

### Create Session

Session ID \* ▼

---

Reflect Port Mode \* ▼

---

RSPAN Type \* ▼

---

RSPAN VLAN ID \* ▼

---

Tx Source Port(s) ▼      Rx Source Port(s) ▼

---

Designated Port \* ▼

---

Either the TX or RX source ports need to be selected.

CANCEL
CREATE

#### **Session ID**

Setting	Description	Factory Default
Select from the drop-down list	Select the session ID from the dropdown list (6 to 7). SPAN and RSPAN share 7 sessions, SPAN uses 1 to 5, and RSPAN uses 6 and 7.	None

#### **Reflect Port Mode**

Setting	Description	Factory Default
Enable	Enable Reflect Port Mode and configure Reflect Port for mirroring packets to multiple designated ports.	None
Disable	Disable Reflect Port Mode for mirroring packets to a single designated port.	

#### **RSPAN Type**

Setting	Description	Factory Default
Source	Specify the RSAPN type as Source if the switch role is RSPAN source switch.	None
Destination	Specify the RSAPN type as Destination if the switch role is the RSPAN destination switch.	

#### **RSPAN VLAN ID**

Setting	Description	Factory Default
Select the ID from the list	Select the VLAN ID as the RSPAN VLAN ID. The RSPAN VLAN ID cannot be the management VLAN ID.	None

#### **Tx Source Port**

Setting	Description	Factory Default
Select the port from the list	Select this option to monitor only those data packets being sent out through the switch's port.	None

### Rx Source Port

Setting	Description	Factory Default
Select the port from the list	Select this option to monitor only those data packets coming into the switch's port.	None

Specify this port as the Reflect Port after enabling Reflect Port Mode for mirroring packets to multiple designated ports. This port is specifically reserved for Reflect Port use, please do not configure for other use.

### Designated Port

Setting	Description	Factory Default
Select the port from the list	Specify this port as the designated port.	None

When finished, click **CREATE** to create the RSPAN session.

To configure RSPAN, users need to decide the switch role first. Here are two scenarios:

1. To copy packets from one or more source port(s) (monitored ports) to a single designated port (mirror port).
2. To copy packets from one or more source port(s) to multiple designated ports. The different configuration steps between the two scenarios are configuring the source switch. The other configuration steps for configuring the intermediate switch and destination switch are the same. The following are the configuration steps:

#### **To configure source switch for scenario 1: To copy packets to a single designated port (mirror port).**

1. Select Session ID from drop list (6 and 7). The session can be different between the source switch, intermediate switch, and destination switch for the same mirroring traffic.
2. Disable Reflect Port Mode
3. Select Source as RSPAN Type.
4. The RSPAN type cannot be duplicated in different RSPAN sessions.
5. Select RSPAN VLAN which cannot be the management VLAN. The VLAN cannot be duplicated in different RSPAN sessions. The RSPAN VLAN must be the same for any traffic that travels between the source switch, the intermediate switch, and the destination switch.
6. Select the monitored packet source port(s), you can select either Tx source port(s) or Rx source port(s), or both.
  - If Tx source port(s) is selected, the egress traffic on the port(s) will be mirrored to a designated port.
  - If the Rx source port(s) is selected, the ingress traffic on the port(s) will be mirrored to a designated port.
7. Select the designated port, which is required to be an access port.



### NOTE

The duplication of source port(s) configured in different sessions is not allowed. The duplication of source port(s) and designated port(s) in different sessions is not allowed.



**To configure source switch for scenario 2: To copy packets to multiple designated ports (mirror port):**

1. Select Session ID from drop list (6 and 7). The session can be different between source switch, intermediate switch and destination switch for the same mirroring traffic.
2. Enable Reflect Port Mode
3. Select Source as RSPAN Type
4. Select RSPAN VLAN, which cannot be the management VLAN. The VLAN cannot be duplicated in different RSPAN sessions. The RSPAN VLAN must be the same between source switch, intermediate switch to destination switch for the same mirroring traffic.
5. Select the monitored packet source port(s), you can select either Tx source port(s) or Rx source port(s), or both.
  - If Tx source port(s) is selected, the egress traffic on the port(s) will be mirrored to the reflect port.
  - If the Rx source port(s) is selected, the ingress traffic on the port(s) will be mirrored to the reflect port.
6. Select the reflect port, which is required to be trunk port. The port is reserved for reflect traffic to designated ports use, please do not configure for other use.
7. Go to the VLAN page, configure the ports required to receive the packets from source ports as the member port of the same VLAN ID as reflect port.



**NOTE**

The duplication of source port(s) configured in different sessions is not allowed. The duplication of source port(s), reflect port and destined port(s) and in different sessions is not allowed.

**To configure the intermediate switch:**

1. Enable the intermediate role for intermediate switch. RSPAN session can be created after enabling the intermediate role in the switch.
2. Select RSPAN VLAN ID which cannot be the management VLAN. The RSPAN VLAN must be the same for the traffic mirrored from source switch, intermediate switch to destination switch.

**To configure the destination switch:**

1. Select Session ID from drop list (6 and 7); the session can be different for the traffic mirrored from source switch, intermediate switch to destination switch.
2. Select Destination as RSPAN Type. The RSPAN type cannot be duplicated in different RSPAN sessions.
3. Select RSPAN VLAN, which cannot be the management VLAN. The VLAN cannot be duplicated in different RSPAN sessions. The RSPAN VLAN must be the same for the traffic mirrored from source switch, intermediate switch to destination switch.
4. Select the destination port(s) and the ports must be the access port.

## Ping

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

To use the Ping function, click **Ping** on the menu, and enter the IP address or domain name you want to ping. After clicking **Ping**, the result will be shown.

## Ping

IP Address/Name \*

PING

### ARP Table

To view the ARP Table, select **ARP Table** and the information will be displayed.

### ARP Table

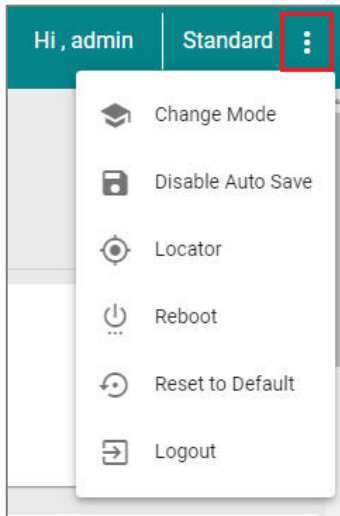
🔄 📄

Index	MAC Address	IP Address
1	28:d2:44:5e:8b:40	192.168.127.99

Max 2000

# Maintenance and Tools

This section explains how to maintain Moxa's switch and the tools that help users operate the switch. Click the icon on the upper right corner of the page.

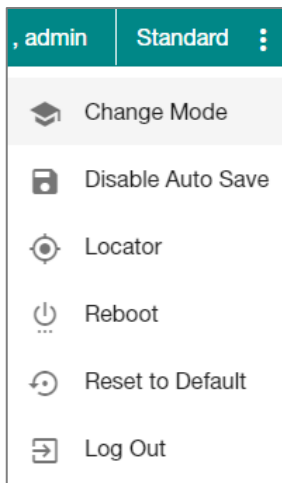


## Standard/Advanced Mode

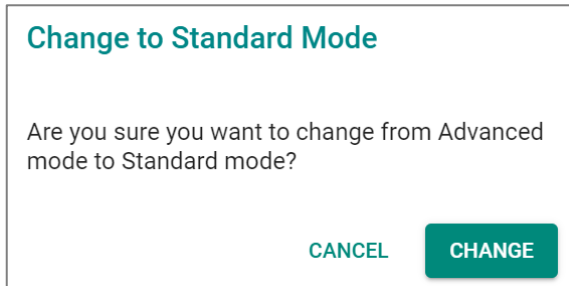
There are two configuration modes available for users: **Standard Mode** and **Advanced Mode**.

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

To switch to Advanced Mode, click the change mode icon on the upper right corner of the page, and then select **Change Mode**.



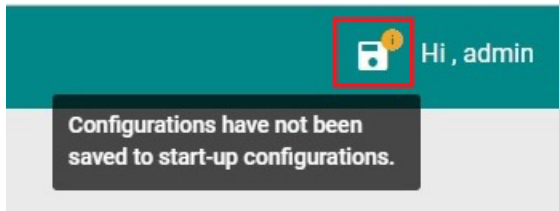
Click **CHANGE** to change to **Advanced Mode**.



Advanced Mode offers more detailed system configurations for specific functions. Use the same process if you want to return to Standard Mode.

## Disable Auto Save

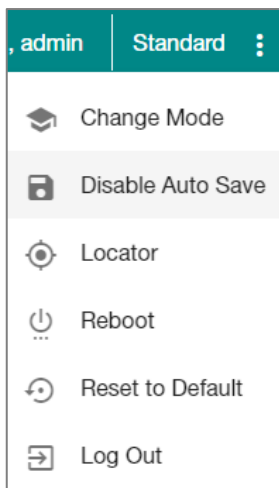
Auto Save allows users to save the settings to the start-up configurations; all parameters will be effective when applied immediately, even when the switch has restarted. When users select **Disable Auto Save**, all parameters will be temporarily stored in the running config (memory), and a disk icon will appear on the upper right corner of the page. Users need to save the running-configuration to the startup-configuration when changing any parameters or function after clicking **Apply**.



It is highly recommended that you always manually save all configurations by clicking Save Disk icon when **Disable Auto Save** is applied, or all information will have disappeared after the switch has restarted.

When **Disable Auto Save** is applied, only the configurations that are running will be saved; users can unplug the power or perform a warm start to recover the network before manually saving the configurations. When Auto Save is enabled, the start-up configurations will be saved in the switch.

To disable the **Auto Save** function, click **Disable Auto Save** in the menu.



Click **Disable**.

### Disable Auto Save Mode

Are you sure you want to disable auto save mode?

CANCEL **DISABLE**

## Locator

Users can trigger the device locator by clicking this icon. This will cause the LED indicators on the switch to flash for one minute. This helps users easily find the location of the switch in a field site.

, admin | Standard

- Change Mode
- Disable Auto Save
- Locator**
- Reboot
- Reset to Default
- Log Out

Click **Locate** to finish.

### Switch Locator

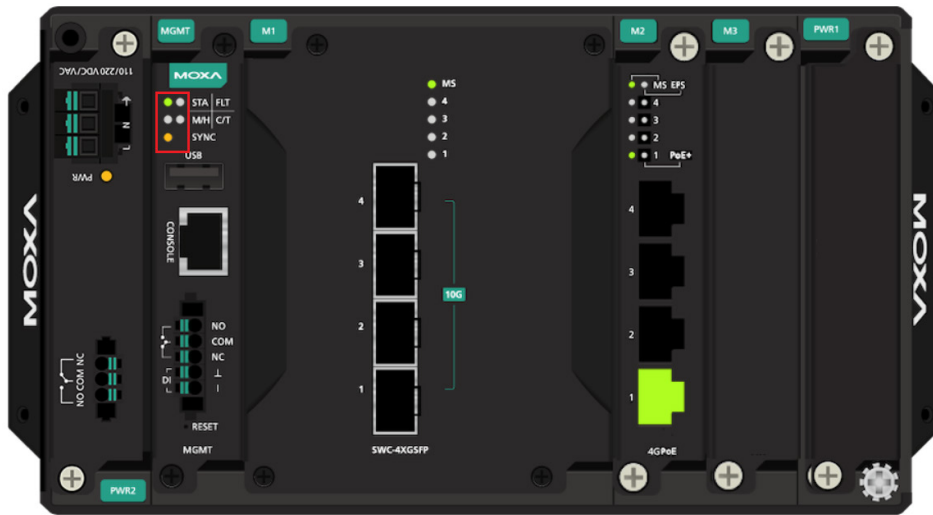
Duration \*  
60  ⓘ  
30 - 300 sec.

CANCEL **LOCATE**

### Duration (sec.)

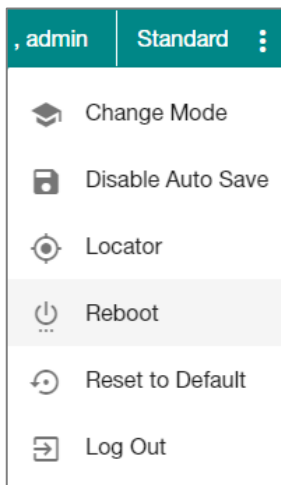
Setting	Description	Factory Default
30 to 300	Specify the length of time the indicators will remain flashing.	60

Click **Locate** to activate the switch locator. The LED indicators are located on the upper left corner of the switch as can be seen in the figure below.

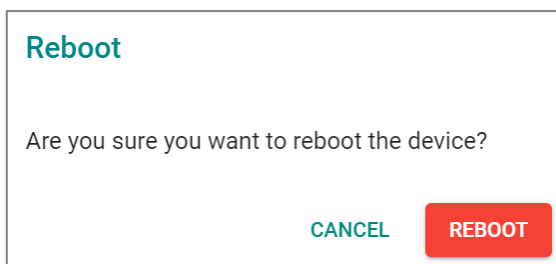


## Reboot

To reboot the device, select **Reboot**.

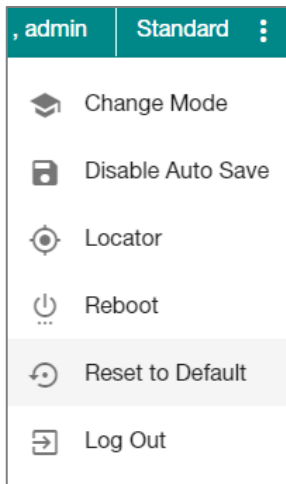


Click **REBOOT** to restart the device.

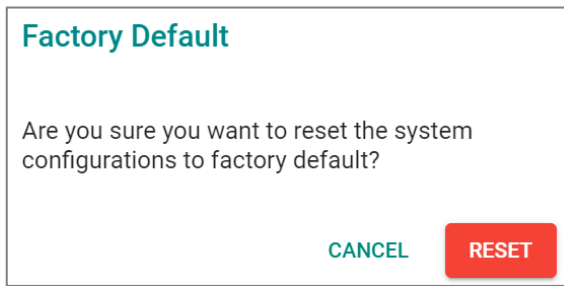


## Reset to Default

To reset the switch to the default status, select **Reset to Default**.

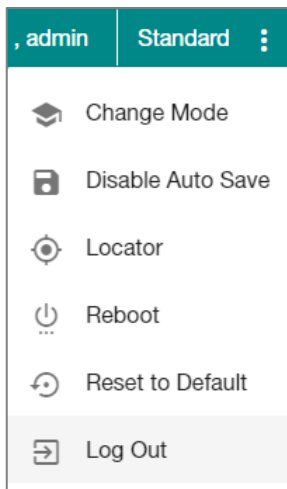


To return the switch to factory default settings, click **RESET**.

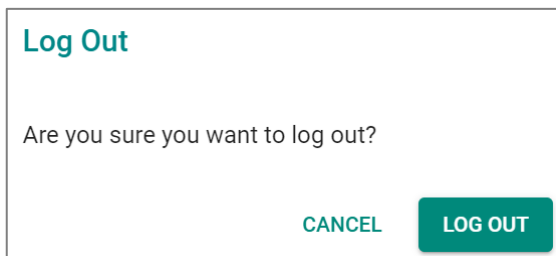


## Log Out of the Switch

To log out of the switch, select **Log Out**.



Click **LOG OUT** to log out of the switch.





# A. Account Privileges List

This appendix describes the read/write access privileges for different accounts on Moxa's Managed Ethernet Series switches.

## Account Privileges List

This appendix lists the privileges for different account roles.

Please note, **R** stands for **Read** and **W** stands for **Write**.

Function	Account Privilege		
	Admin	Supervisor	User
<b>System</b>			
Information Setting	R/W	R/W	R
Firmware Upgrade	Execute	No Access	No Access
Configuration Backup and Restore	Execute	Execute	No Access
Event log backup	Execute	Execute	Execute
User Account	R/W	No Access	No Access
Password Policy	R/W	No Access	No Access
IP Configuration	R/W	R/W	R
Time Zone	R/W	R/W	R
System Time	R/W	R/W	R
<b>Port</b>			
Port Setting	R/W	R/W	R
Linkup Delay	R/W	R/W	R
Link Aggregation (Port Channel)	R/W	R/W	R
PoE	R/W	R/W	R
<b>VLAN</b>			
IEEE 802.1Q	R/W	R/W	R
GARP	R/W	R/W	R
<b>MAC</b>			
Static Unicast	R/W	R/W	R
MAC Address Table	R/W	R/W	R
<b>QoS</b>			
Classification	R/W	R/W	R
Ingress Rate Limit	R/W	R/W	R
Scheduler	R/W	R/W	R
Egress Shaper	R/W	R/W	R
<b>Multicast</b>			
IGMP Snooping	R/W	R/W	R
Static Multicast	R/W	R/W	R
GMRP	R/W	R/W	R
<b>Layer 2 Redundancy</b>			
Spanning Tree	R/W	R/W	R
Turbo Ring v2	R/W	R/W	R
Dual Homing	R/W	R/W	R
<b>Network Management</b>			
SNMP	R/W	No Access	No Access
SNMP Trap/Inform	R/W	No Access	No Access
RMON1 (CLI only)	R/W	R/W	R

Function	Account Privilege		
	Admin	Supervisor	User
<b>Security</b>			
Management Interface	R/W	R/W	R
Login Policy	R/W	R	R
Trusted Access	R/W	R	R
SSH & SSL	Execute	Execute	No Access
IEEE802.1X	R/W	R/W	R
Port Security	R/W	R/W	R
Traffic Storm Control	R/W	R/W	R
<b>Authentication</b>			
RADIUS	R/W	No Access	No Access
TACACS+	R/W	No Access	No Access
Login Authentication	R/W	No Access	No Access
<b>Diagnostics</b>			
Event Notification	R/W	R/W	R
Relay Output	R/W	R/W	R
Email Notification	R/W	R	R
Syslog	R/W	R	R
Event Log	R/W	R/W	R
LLDP	R/W	R/W	R
Port Mirror	R/W	R/W	R
Ping	Execute	Execute	Execute
ARP Table	R/W	R/W	R
Utilization	R	R	R
Statistics	R	R	R
Module information	R	R	R
<b>Maintenance and Tool</b>			
Standard/Advance Mode	Execute	Execute	Execute
Disable Auto Save	R/W	R/W	R
Locator	R/W	R/W	Execute
Reboot	Execute	Execute	No Access
Reset to default	R/W	No Access	No Access

# B. Event Log Description

This appendix describes all of the information for the event logs. When an event occurs, it will be recorded in the event log files. Users can check the event log name and its event log description.

## Event Log Description

Event Name	Severity	Event Description
802.1X Auth Failed	Warning	802.1x authentication failed on port {{index}}/{{number}} with {{buffer}}
ABC-02 is inserted or unplugged	Notice	ABC-02 is {{inserted/unplugged}}.
ABC-03 is inserted or unplugged	Notice	ABC-03 is {{inserted/unplugged}}.
Account log out	Notice	[Account:{{user_name}}] logged out.
Account removed	Notice	[Account:{{user_name}}] has been removed by admin.
Account settings changed	Notice	Account settings of [Account:{{user_name}}] has been updated. Account settings of [Account:{{user_name}}] has been deleted. Account settings of [Account:{{user_name}}] has been created.
Announce message with different interval	Warning	An Announce message with a different interval has been received from port {{index}}/{{number}}
Announce timeout	Warning	PTP port {{index}}/{{number}} Announce receipt timer has timed out.
Check if hardware revision is valid	Notice	The hardware revision of Power Module {{index}} is not allowed.
Check if it is a known power module	Warning	To avoid potential overheating, Moxa does not recommend using a {{index}} power supply with this device.
Cold start	Critical	System has performed a cold start.
Configuration changed	Notice	Configuration {{modules}} changed by {{username}}.
Configuration exported	Notice	Configurations exported {{successful /failed}} by {{username}} via {{method}}.
Configuration imported	Notice	Configuration import {{successful /failed}} by {{username}} via {{method}}.
Coupling changed	Warning	Turbo Ring v2 coupling path status has changed.
DI off	Notice	Digital Input {{index}} has been turned off.
DI on	Notice	Digital Input {{index}} has been turned on.
Dual homing path changed	Warning	Dual Homing path has switched.
Event log export	Notice	Event Log export {{successful /failed}} by {{username}} via {{method}}.
Firmware upgrade failed	Warning	Firmware failed to upgrade.
Firmware upgrade successful	Notice	Firmware successfully upgraded
Grand Master changed	Warning	The PTP grandmaster has changed from {{mac addr}} to {{mac addr}}
Hardware revision is not allowed	Error	The hardware revision of Line Module %d is not allowed.
Interface link down	Notice	Interface{{number}} down.
Interface link up	Notice	Interface {{number}} up.
LLDP table changed	Info	LLDP remote table has changed.
Log capacity threshold	Warning	Number of event log entries {{logEntryNum}} has reached the threshold.

Event Name	Severity	Event Description
Login failed	Warning	[Account {{user_name}}] log in failed via {{interface}}.
Login lockout	Warning	[Account {{user_name}}] locked due to {{failed_times}} failed login attempts.
Login successful	Notice	[Account {{user_name}}] successfully logged in via {{interface}}.
Low input voltage	Warning	The input voltage of the power supply has dropped below 46 VDC. Please adjust the voltage to between 46 and 57 VDC to fit the PoE voltage requirement.
Master changed	Warning	Ring {{Index}} master has changed.
Master mismatch	Warning	Ring {{Index}} master setting does not match.
module change	Notice	M{{index}} module has changed.
Module Initialized Fail	Error	M{{index}} Module initialized has failed.
Module inserted	Notice	M{{Index}} Module inserted.
Module removed	Notice	M{{index}} Module removed.
MSTP new port role	Warning	MSTP (MST{{Index}}) port {{number}} role changed from {{role}} to {{role}}.
MSTP root changed	Warning	MSTP (MST{{Index}}) new root has been elected in topology.
MSTP topology changed	Warning	Topology (MST{{Index}}) has been changed by MSTP.
OSPF DR router adjacency changed	Notice	Interface {{ip addr}}/{{ip addr}}/{{ip addr}}/{{ip addr}} DR neighbor {{ip addr}}/{{ip addr}}/{{ip addr}}/{{ip addr}} adjacency changed.
OSPF interface DR changed	Notice	Interface {{ip addr}}/{{ip addr}}/{{ip addr}}/{{ip addr}} DR Change{{ip addr}}/{{ip addr}}/{{ip addr}}/{{ip addr}} to {{ip addr}}/{{ip addr}}/{{ip addr}}/{{ip addr}}.
OSPF interface ISM became DR	Notice	Interface {{ip addr}}/{{ip addr}}/{{ip addr}}/{{ip addr}} become DR.
Over power budget limit	Warning	The consumed power {{power_value}} of all the PDs have exceeded the maximum input power {{input_power_value}}.
Packet dropped by Port Security	Warning	Port {{index}}/{{number}} dropped packets due to violation of Port Security rule.
Password changed	Notice	Password of [Account: {{user_name}}] has been changed.
PD no response	Error	Port {{number}} device is not responding to the PD failure check. Please check the device status.
PD over-current	Error	Current of port {{number}} has exceeded the safety limit. Please check the device status.
PD power off	Notice	Port {{number}} PD power off.
PD power on	Notice	Port {{number}} PD power on.
Port Link Down	Notice	Port {{index}}/{{number}} link down. Port-channel {{Channel id}} link down.
Port Link Up	Notice	Port {{index}}/{{number}} link up. Port-channel {{Channel id}} link up.
Port recovery by Rate Limit	Warning	Port {{index}}/{{number}} has recovered by rate limit.
Port shutdown by Loop	Critical	Port {{index}}/{{number}} looping and shutdown.
Port shutdown by Port Security	Warning	Port {{index}}/{{number}} has shut down due to a violation of the Port Security rule.
Port shutdown by Rate Limit	Warning	Port {{index}}/{{number}} has excessive traffic and shutdown.
Port state change	Info	PTP port {{index}}/{{number}} has changed from {{state}} to {{state}}.
Power module insert	Notice	Power Module {{index}} has been inserted.
Power module remove	Notice	Power Module {{index}} has been removed.

Event Name	Severity	Event Description
Power Off->On	Notice	Power {{index}} has turned off.
Power On->Off	Notice	Power {{index}} has turned on.
PTP message with the wrong domain number	Warning	The PTP message with the wrong domain number was received from port {{index}}/{{number}}.
Redundant port health check failed	Error	Redundant port {{index}}/{{number}} health check fail.
Relay Override message	Notice	{{relay_name}} relay alarm has been cut off.
Relay Triggered message	Notice	{{MGMT/PWR1/PWR2}} alarm is on due to {{Event Name}}.
RMON failing alarm	Warning	{{user defined}}.
RMON raising alarm	Warning	{{user defined}}.
RSTP invalid BPDU	Warning	RSTP Port-Channel {{channel id}} received an invalid BPDU (type: {{type}}, value: {{value}}). RSTP port {{index}}/{{number}} received an invalid BPDU (type: {{type}}, value: {{value}}).
RSTP migration	Warning	Port-Channel {{channel id}} changed to {{rstp/stp}}. Port {{index}}/{{number}} changed to {{rstp/stp}}.
RSTP new port role	Warning	RSTP Port-Channel {{channel id}} role changed from {{role}} to {{role}}. RSTP port {{index}}/{{number}} role changed from {{role}} to {{role}}.
RSTP root changed	Warning	RSTP new root has been elected in topology.
RSTP topology changed	Warning	Topology has been changed by RSTP.
Send message fail	Warning	PTP port {{index}}/{{number}} failed to transmit {{Type}}.
SSH Key generated	Notice	SSH key has been regenerated.
SSL certification changed	Notice	SSL certificate has been changed. SSL certificate has been regenerated.
Sync status change	Warning	The PTP sync status has changed from {{PreSyncStatus}} to {{CurSyncStatus}}.
Topology changed (RSTP)	Warning	Topology has been changed by RSTP.
Topology changed (Turbo Ring)	Warning	Topology change has been detected on Ring {{RingIndex}} of Turbo Ring v2.
Unknown module	Warning	Module {{index}} Unknown Module Initialized Failed.
VRRP Master change	Warning	VRRP Interface {{number}} VrId {{vlanId}} state change to master.
Warm start	Notice	System has performed a warm start.
When the trust host moves, it will send a log to Moxa log handler.	Warning	A trust host, MAC is {{mac address}} with VLAN {{Vlan Id}}, moved from port {{index}}/{{number}} to port {{index}}/{{number}}.

## C. SNMP MIB File

---

This appendix contains the SNMP MIB file for the managed switch.

### Standard MIB Installation Order

If you need to import the MIB one-by-one, please install the MIBs in the following order.

1. RFC1213-MIB.mib
2. SNMP-FRAMEWORK-MIB.mib
3. SNMPv2-SMI.mib
4. SNMPv2-TC.mib
5. SNMPv2-CONF.mib
6. SNMPv2-MIB.mib
7. IANAifType-MIB.mib
8. IEEE8023-LAG-MIB.mib
9. IF-MIB.mib
10. EtherLike-MIB.mib
11. IEEE8021-PAE-MIB.mib
12. BRIDGE-MIB.mib
13. P-BRIDGE-MIB.mib
14. RFC1271-MIB.mib
15. RMON-MIB.mib
16. TOKEN-RING-RMON-MIB.mib
17. RMON2-MIB.mib
18. Q-BRIDGE-MIB.mib
19. INET-ADDRESS-MIB.mib
20. IEEE8021-TC-MIB.mib
21. IEEE8021-SPANNING-TREE-MIB.mib
22. IANA-ADDRESS-FAMILY-NUMBERS-MIB.mib
23. LLDP-MIB.mib
24. LLDP-EXT-DOT1-MIB.mib
25. LLDP-EXT-DOT3-MIB.mib

### MIB Tree

Refer to the following content for the MIB Tree structure.

```
iso(1)
|-std(0)-iso8802(8802)-ieee802dot1(1)-ieee802dot1mibs(1)
  |-ieee8021paeMIB(1): IEEE8021-PAE-MIB.mib
  |-ieee8021SpanningTreeMib(3): IEEE8021-SPANNING-TREE-MIB.mib
|-org(3)
  |-dod(6)-internet(1)
    |-mgmt(2)-mib-2(1): SNMPv2-MIB.mib
    |-system(1): RFC1213-MIB.mib
```

```

|-interface(2): RFC1213-MIB.mib
|-at(3): RFC1213-MIB.mib
|-snmp(11): RFC1213-MIB.mib
|-rmon(16): RMON-MIB.mib
|-dot1dBridge(17): BRIDGE-MIB.mib, P-BRIDGE-MIB.mib, Q-BRIDGE-MIB.mib
|-ifMIB(31): IF-MIB.mib
|-etherMIB(35): EtherLike-MIB.mib
|-private(4)-moxa(8691)
|-product(600): mxGeneralInfo.mib, mxProductInfo.mib,
|-general(602): mxGeneral.mib, mxDeviceIo.mib, mxDhcpSvr.mib, mxEmailC.mib,
mxEventLog.mib,
:mxGene.mib, mxLocator.mib, mxManagementIp.mib, mxPoe.mib,
mxPorte.mib,
: mxRelayC.mib, mxSnmp.mib, mxSwe.mib, mxSysLoginPolicySvr.mib,
: mxSyslogSvr.mib, mxSysPasswordPolicySvr.mib, mxSystemInfo.mib,
: mxSysTrustAccessSvr.mib, mxSysUtilSvr.mib, mxTimeSetting.mib,
: mxTimeZone.mib, mxTrapC.mib, mxUiServiceMgmt.mib
|-switching(603): mxSwitching.mib
|- portInterfacce : mxPort.mib, mxLa.mib
|- basicLayer2: mxLhc.mib, mxQos, mxVlan.mib
|- layer2Redundancy: mxRstp.mib, mxTrv2.mib, mxTurboChain.mib,
mxDualHoming.mib
|- layer2Security: mxStcl.mib, mxRlps.mib, mxPssp.mib, mxPsms.mib, mxDot1x.mib,
mxRadius.mib
|- layer2Diagnostic: mxLldp.mib, mxTcst.mib, mxPortMirror.mib, mxRmon.mib
|- layer3Diagnostic
|- layer2Multicast: mxIgmpSnp.mib
|- layer3Multicast
|-poe(608): mxPoe.mib
|-snmpV2(6)-snmpModules(3)
|-snmpFrameworkMIB(10): SNMP-FRAMEWORK.mib
|-ieee(111)-standards-association-numbers-series-standards(2)-lan-man-stds(802)-ieee802dot1(1)-
ieee802dot1mibs(1)-ieee8021SpanningTreeMib(3): IEEE8021-SPANNING-TREE-MIB.mib

```

# D. Security Guidelines

---

This appendix explains security practices for installing, operating, maintaining, and decommissioning the device. Moxa strongly recommends that our customers follow these guidelines to enhance network and equipment security.

## Installation

### Physical Installation

1. The device **MUST** be installed in an access controlled area, where only the necessary personnel have physical access to the device.
2. The device **MUST NOT** be directly connected to the Internet, which means switches **MUST** be installed within a security perimeter, which can be implemented by a firewall at the border since the device is not classified as zone/boundary equipment.
3. Please follow the instructions in the Quick Installation Guide, which is included in the package, to ensure you install the device correctly in your environment.
4. The device has anti-tamper labels on the enclosures. This allows an administrator to tell whether the device has been tampered with.
5. The ports that are not in use should be deactivated. Please refer to **[User Manual section Port Interface]** for detailed instructions.

### Account Management

Follow these best practices when setting up an account.

1. Each account should be assigned the correct privileges: Only allow the minimum number of people to have admin privilege so they can perform device configuration or modifications, while other users should only have read access privilege. The device supports both local account authentication and remote centralized mechanism, including Radius and TACACS+.
2. Change the default password, and strengthen the account password complexity by:
  - a. Enabling the "Password Policy" function.
  - b. Increasing the minimum password length to at least eight characters.
  - c. Defining a password policy to ensure that it contains at least an uppercase and lowercase letter, a digit, and a special character.
  - d. Setting user passwords to expire after a certain period of time.
3. Enforce regulations that ensure that only a trusted host can access the device. Please refer to **Trusted Access** for detailed instructions.



## Vulnerable Network Ports

1. For network security concerns, we strongly recommend that you change the port numbers, such as TCP port numbers for HTTP, HTTPS, Telnet, and SSH, for the protocols that are in use; ports that are not in use but are still reachable pose an unacceptable security risk and should be disabled. Refer to the **Management Interface** section for detailed instructions.
2. In order to avoid eavesdroppers from snooping confidential information, users should adopt encryption-based communication protocols, such as HTTPS instead of HTTP, SSH instead of Telnet, SFTP instead of TFTP, SNMPv3 instead of SNMPv1/v2c, etc. In addition, the maximum number of sessions should be kept to an absolute minimum. Please refer to **Management Interface** for detailed instructions.
3. Users should re-generate SSL certificate and SSH key for the device before commissioning HTTPS or SSH applications. Please refer to **SSH & SSL** for detailed instructions.

## Operation

1. In order to ensure that communications are properly protected, use a strong cryptographic algorithm for key exchange or encryption protocols for HTTPS/SSH applications. The device follows the NIST SP800-52 and SP800-131 standards, and supports TLS v1.2 and v1.3 with the following cipher suites:

TLS V1.2				
Cipher suite name	Key exchange	Authentication	Encryption	Hash function
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256	ECDHE	RSA	CHACHA20-POLY1305	SHA256
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	ECDHE	ECDSA	AES128	SHA256
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDHE	RSA	AES128	SHA256
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDHE	RSA	AES256	SHA384
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	Ephemeral DH	RSA	AES128	SHA256
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	Ephemeral DH	RSA	AES256	SHA384
TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256	Ephemeral DH	RSA	CHACHA20-POLY1305	SHA256
TLS_ECDHE-RSA_WITH_AES256-SHA384	ECDHE	RSA	AES256	SHA384
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	ECDHE	RSA	AES128	SHA256
TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256	ECDHE	ECDSA	CHACHA20-POLY1305	SHA256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDHE	RSA	AES256	SHA384
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384	ECDHE	ECDSA	AES256	SHA384
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	ECDHE	ECDSA	AES128	SHA256

TLS V1.3				
Cipher suite name	Key exchange	Encryption	Mode	Hash function
TLS_AES_256_GCM_SHA384	any	AES256	GCM	SHA384
TLS_CHACHA20_POLY1305_SHA256	any	CHACHA20-POLY1305	N/A	SHA256
TLS_AES_128_GCM_SHA256	any	AES128	GCM	SHA256

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

Browser	Version
Microsoft Edge	All
Microsoft Internet Explorer	v11 or above
Mozilla Firefox	v27 or above
Google Chrome	v38 or above
Apple Safari	v7 or above

Reference: <https://support.globalsign.com/ssl/general-ssl/tls-protocol-compatibility#Browsers>

3. The device supports event logs and syslog for SIEM integration:
- Event log: Due to limited storage capacity, the event log can only accommodate a maximum of 10,000 entries. Administrators can set a warning for a pre-defined threshold. We recommend that users regularly back up system event logs. Please refer to **Event Log** for detailed instructions.
  - Syslog: the device supports syslog, and advanced secure TLS-based syslog for centralized SIEM integration. Please refer to **Syslog** for detailed instructions.
4. The device can provide information for control system inventory:
- SNMPv1, v2c, v3: We recommend administrators use SNMPv3 with authentication and encryption to manage the network.
  - Telnet/SSH: We recommend that administrators use SSH with authentication and encryption to retrieve device properties.
  - HTTP/HTTPS: We recommend that administrators use HTTPS with a certificate that has been granted by a Certificate Authority to configure the device.
  - MMS: We recommend administrators enable MMS security mode to enhance protection.
5. Denial of Service protection: To avoid disruption of normal operation of the switch, administrators should configure the QoS function. The device supports ingress rate limit and egress shaper. Administrators can decide how to deal with excess data flow and configure the device accordingly. This process will regulate the resulted data rate per port. Refer to **QoS** for more information.
6. Time synchronization with authentication: Time synchronization is crucial for process control. To prevent malicious attacks whereby the settings are changed without permission, authentication must be in place between the NTP server and client. The device supports NTP with a pre-shared key. Please refer to **NTP** Server for detailed instructions.
7. Periodically regenerate the SSH and SSL certificates: Even though the device supports RSA 2048-bit and SHA-256 to ensure sufficient complexity, we strongly recommend that users frequently renew their SSH key and SSL certificate in case the key is compromised. Please refer to **SSH & SSL** for detailed instructions.
8. Below is the list of the protocol port numbers used for external interfaces.

**Protocol: TCP**

Service Type	Port Number
SSH	22
Telnet	23
HTTP	80
HTTPS	443

**Protocol: UDP**

Service Type	Port Number
DHCP	67
NTP	123
SNMP	161
Moxa Service	40404

9. Disable **Hardware Interfaces** that are not in use.

## Maintenance

1. Perform firmware upgrades frequently to enhance features, deploy security patches, or fix bugs.
2. Frequently back up the system configurations: In order to properly protect the system configuration files from being tampered with, the device supports password encryption and signature authentication for backup files.
3. Examine event logs frequently to detect any anomalies.
4. To report vulnerabilities of Moxa products, please submit your findings on the following web page:  
<https://www.moxa.com/en/support/product-support/security-advisory/report-a-vulnerability>.

## Decommission

To avoid disclosing sensitive information such as account password and certificate, please reset the system settings to factory default before decommissioning the device or sending it back to Moxa RMA service.