Moxa Industrial Smart Ethernet Switch User Manual

Version 3.1, May 2025

www.moxa.com/products

Models covered by this manual:
SDS-3006 Series
SDS-G3006 Series
SDS-3008 Series
SDS-G3008 Series
SDS-3010 Series
SDS-G3010 Series
SDS-3016 Series
SDS-G3016 Series

Moxa Industrial Smart Ethernet Switch User Manual

Copyright Notice

Trademarks

Disclaimer

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

Technical Support Contact Information

www.moxa.com/support

Table of Contents

1. About this Manual

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

Read the following two chapters to learn how to use your Moxa smart switch:

- **Chapter 2: Quick Start Guide**
  In chapter 2, we explain how to configure your smart switch the first time you use it, and give an overview of the management function icons that are accessible from the switch's browser-based UI. The easy-to-recognize icons that appear on the UI dashboard effectively reduce deployment time, simplify maintenance, and enhance manageability.
- **Chapter 3: Management Functions**
  In chapter 3, we explain in detail how to access, configure, and use the various management functions supported by your Moxa smart switch. All of the functions can be easily accessed and configured through a web browser.

2. Quick Start Guide

The Moxa industrial smart Ethernet switch has a browser-based UI with easy-to-recognize icons on the UI dashboard to effectively reduce deployment time, simplify maintenance, and enhance manageability. Read this chapter before using your Moxa smart switch for the first time.

Connecting to the Switch for the First Time

To connect to your Moxa smart switch for the first time, use a standard Ethernet cable to connect your computer's Ethernet port to any of the switch's Ethernet ports. You will need to know the switch's factory default settings, which are shown in the following table:

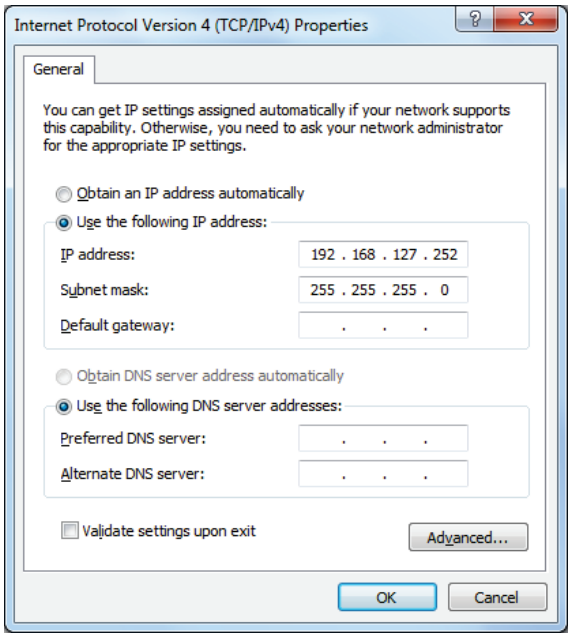
Smart Switch Factory Default Settings

Configuration Item	Default Setting
IP Address	192.168.127.253
Subnet Mask	255.255.255.0
Usernames	admin, user
Password	moxa
Management VLAN	1

Step 1: Configure your computer's network settings

To establish a connection between your computer and the Moxa smart switch, the smart switch and computer must be connected to the same logical subnet.

For example, for a Windows computer, open the **Internet Protocol Version 4 (TCP/IPv4) Properties** page, set subnet mask to 255.255.255.0, and the IP address to 192.168.127.252.



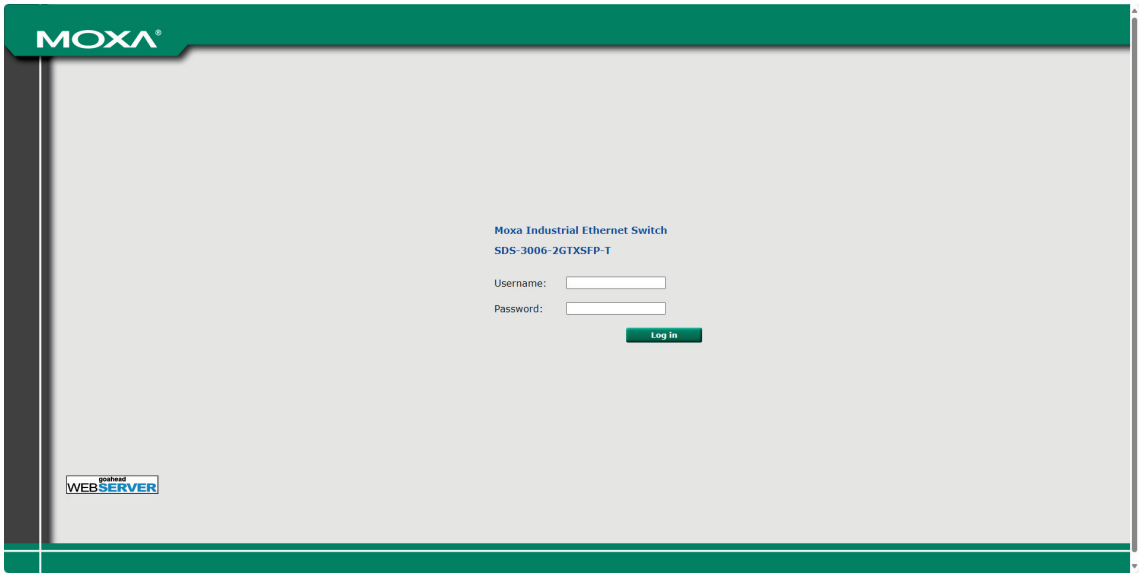
Step 2: Configure the resolution of your computer screen

For best results, set the resolution of your PC's display to 1024 x 768 pixels.

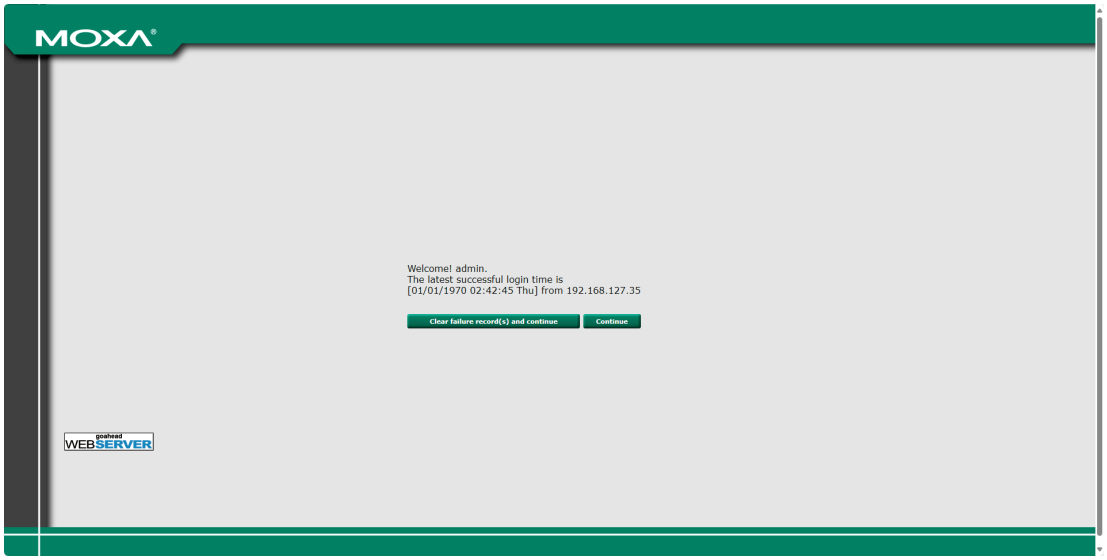
Step 3: Connect to the smart switch's browser-based UI

1. Open your computer's web browser and enter the IP address (default: 192.168.127.253) of the connected smart switch in the Address or URL field at the top of the browser window.

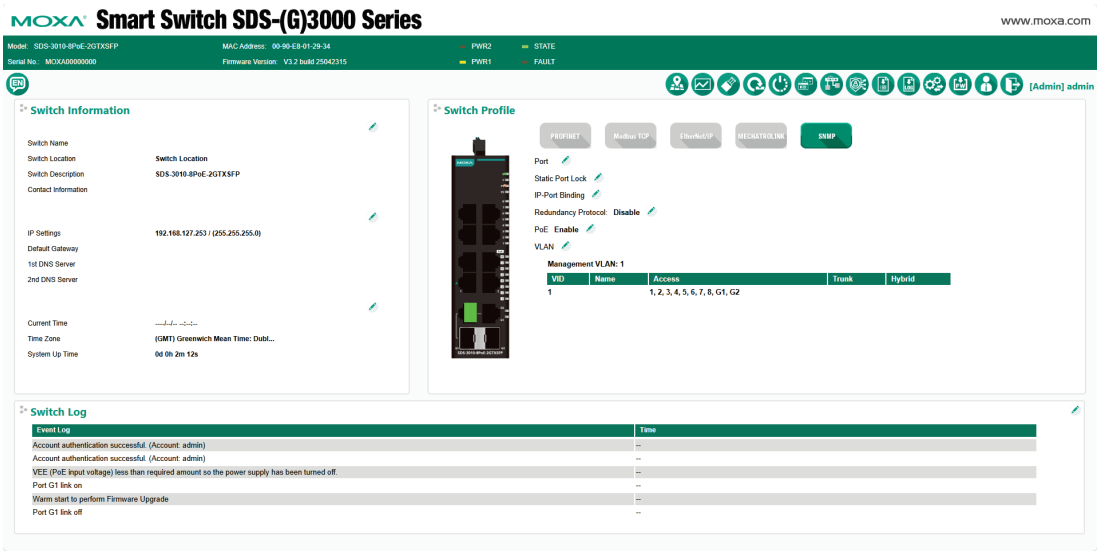
2. When the smart switch's web console opens, type in the Username (default: admin) and Password (default: moxa) and then click the Login button to log in.



3. Click **Continue** on the welcome page to proceed.



4. After logging in, you may need to wait a few moments for the web console to appear.

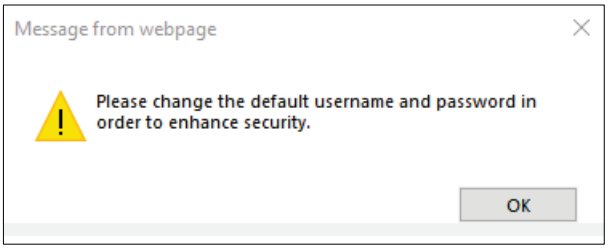


Important Reminders

Change the Default Password

> **IMPORTANT**
>
> Be sure to ***change the password*** of your Moxa smart switch the first time you use the switch.

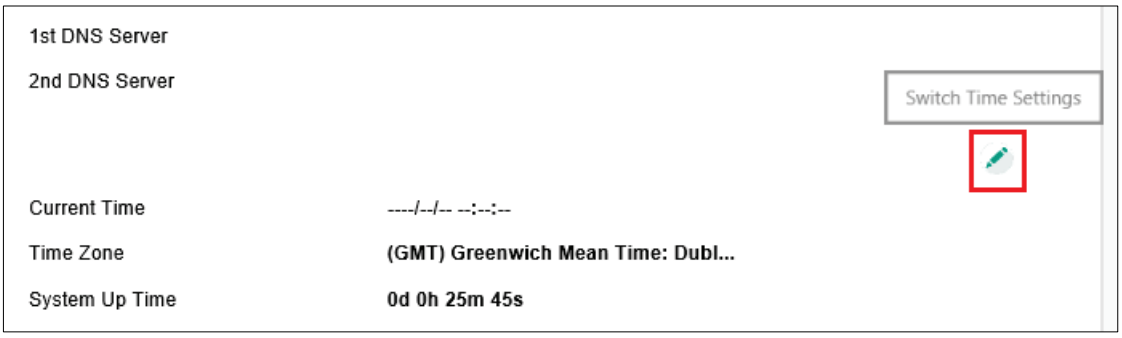
To reduce the chance that hackers will access your smart switch and your network, be sure to change the factory default password (moxa) the first time you use the switch. If the password has not been changed, the following popup window will appear each time you log in:



See the User Account Instructions section in chapter 3 to learn how to change the password.

Configure the Smart Switch's Date and Time Settings

Configure the switch's internal date and time settings the first time you log in to your Moxa smart switch. Setting the correct date and time is important because the switch's log and trap functions use a date/time stamp.



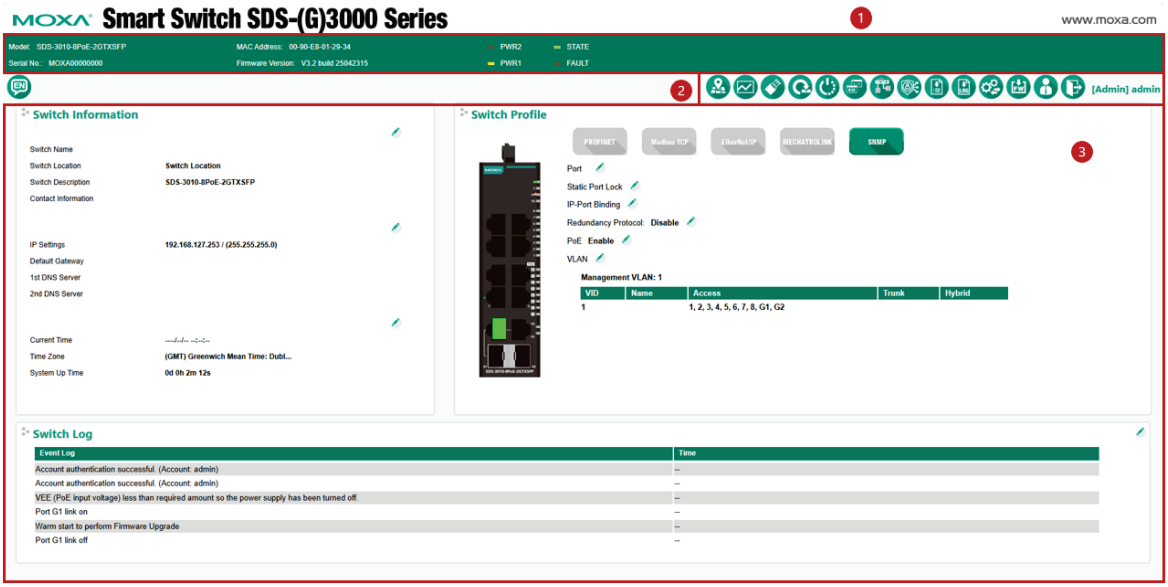
See the Date and Time Information section in the chapter 3 for details.

UI Dashboard

The dashboard of the Moxa smart switch's browser-based UI consists of three parts:

1. **Switch Information Bar:** Displays basic switch information, including the model name, MAC address, serial number, and firmware version.
2. **Management Bar:** The clickable icons (referred to below as "management buttons" or simply "buttons") displayed on the Management Bar can be used to perform various management functions. For a detailed explanation of each button, refer to the Management Bar Icons and Functionality section later in this chapter.
3. **Configuration Panels:** The configuration panels section includes three panels: Switch Information, Switch Profile, and Switch Log. Click any of the pencil icons to configure the items nearest the icon. For a detailed explanation of each configuration item, refer to **Chapter 3:** Management Functions.

Pencil Icon



Management Bar Buttons and Functionality

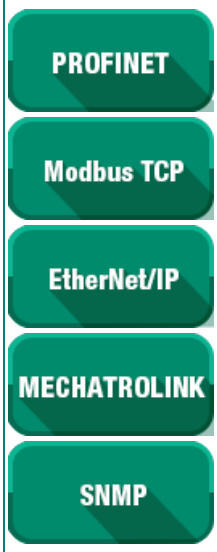
The icons on the Moxa smart switch's management bar can be used to perform a variety of management-type operations. The name of each button and the button's functionality are detailed below:

Icon	Function	Description
	**Multi-Language**	Click the Multi-Language button to select the language on the UI display. The smart switch supports English, Traditional Chinese, Simplified Chinese, Japanese, German, and French.
	**Switch Locator**	Click the **Switch Locator** button to locate the switch you are currently connected to. When the button is clicked, the STATE and FAULT LEDs on the switch will blink green and red, respectively, twice per second for a period of 30 seconds.
	**Statistics**	Click the **Statistics** button to view the system status, such as bandwidth utilization, packet counter, data transmission packets, or transmission error.
	**Fiber Check**	Click the **Fiber Check** button to diagnose the link status of fiber connectors. The displayed parameters include wavelength, temperature, voltage, Tx power, and Rx power. In the threshold settings, manually set the upper and lower bounds of each parameter according to specific application needs. For a detailed explanation of each setting, see the Fiber Check Instructions section later this chapter.
	**Factory Default**	Click the **Factory Default** button to restore the smart switch settings to factory default values. A popup window will appear asking you to click **OK** to proceed with the reset action, or **Cancel** to cancel the request. A factory reset button is also located on the top panel of the switch itself. Refer to the **Quick Installation Guide**, which can be downloaded from Moxa's website, for instructions on how to use the reset button.
	**Restart System**	Click the **Restart System** button to initiate a "warm restart" of the Moxa smart switch's operating system. A popup window will appear asking you to click **OK** to proceed with the reset action, or **Cancel** to cancel the request.
	**Management Interface**	Click the **Management Interface** button to update the TCP Port numbers for various web protocols, the maximum number of users who can be logged in simultaneously to various protocols, and the auto logout time setting. These settings can be used to better control network security. For a detailed explanation of each setting, see the Management Interface Instructions section later this chapter.
	**Port Mirror**	Click the **Port Mirror** button to configure a monitored port, sniffer mode, and mirror port. The mirror port can be configured to transmit the same data being transmitted to and/or from the monitored port, allowing the network administrator to "sniff" the observed port to keep an eye on network activity. For a detailed explanation of each setting, see the Port Mirror Instructions section later in this chapter. **NOTE:** Only sniffed traffic will be transmitted through the mirror port. **NOTE:** When the port mirror function is activated, the gray ports on the Port Mirror Button will change to blue.

Icon	Function	Description
	**Trusted Access**	Click the **Trusted Access** button to add or remove IP addresses that are allowed access to the switch. This IP address-based filtering method to control access helps ensure safe data transmissions. For a detailed explanation of each setting, see the Trusted Access Instructions section later this chapter. **NOTE:** In order to avoid being disconnected after enabling this function, please first add the current IP subnet to the Trusted Access list.
	**Inventory Report Download**	Click the **Inventory Report Download** button to download a text file that summarizes information related to the switch. The text file can be used to improve device management and for archiving. The text file will be named as follows: "[Switch Name]_inventory_report.txt". For an overview of the content that will be downloaded, see the Inventory Report Download section later in this chapter.
	**Log File Backup**	Click the **Log File Backup** button to back up the smart switch's log files. When the Log File Backup dialog window opens, select one of three backup methods: to a local drive, to a remote TFTP server, or save to Moxa Auto Backup Configurator (ABC-02). You may also select the "Automatically back up the event log to prevent it from being overwritten" option at the bottom of the dialog window. For a detailed explanation of the settings, see the Log File Backup Instructions section later in this chapter. **NOTE:** Moxa industrial smart Ethernet switches can store a maximum of 1000 event log entries. When the limit of 1000 entries is reached, the switch will overwrite and delete the oldest saved event log.
	**Configuration Backup and Restore**	Click the **Configuration Backup and Restore** button to enable your Moxa smart switch's configuration backup and restore function. When the settings window opens, select one of three backup and restore options: using a local computer, using a remote TFTP server, or using a Moxa Auto Backup Configurator (ABC-02). You may also require the configuration file to be encrypted, and configure the configuration backup and restore function to automatically load configurations from and back up configurations to an ABC-02 device attached to the switch. For a detailed explanation of the settings, see the Configuration Backup and Restore Instructions section later in this chapter. **NOTE:** When encryption is enabled, you must set a password, and use the password when restoring the configuration from a backup file.
	**Firmware Upgrade**	Click the **Firmware Upgrade** button to upgrade the firmware through either a local drive, remote TFTP server, or Auto Backup Configurator (ABC-02). For a detailed description of this function, see the Firmware Upgrade Instructions section later in this chapter.
	**User Account**	Click the **User Account** button to create, manage, or remove accounts and corresponding settings. For a detailed description of this setting, see the User Account Instructions section later in this chapter. **NOTE:** The active username and the user's corresponding access right are displayed to the right of the Management Bar buttons. For example: **[Admin] admin**

Icon	Function	Description
	**Logout**	Click the **Logout** button to manually log out of the switch's web console. Note that you can use the Management Interface function described above to configure the switch to automatically log out of the web console if the connection with the user is idle for a preset time period.

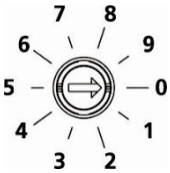
Configuration Panel Icons and Functionality

Icon	Function	Description
	**Edit**	Click any of the **Edit** buttons in the Switch Configuration Information section to edit the settings of items located near the edit icon.
	**Industrial Protocols and SNMP Profiles**	The Moxa smart switch supports three industrial protocols: PROFINET, EtherNet/IP, Modbus TCP, and MECHATROLINK-4; and one management protocol: SNMP. When activated, PROFINET, Modbus TCP, EtherNet/IP, MECHATROLINK-4, and/or SNMP statuses are transmitted to, and instructions are received from, devices connected to the switch. Such information can be displayed on a SCADA HMI or NMS system. If the industrial protocol is active, the protocol button will be green (as shown at the left). If the protocol is inactive, the protocol button will be gray. Click the industrial protocol button once to change the protocol from active to inactive and vice versa. **NOTE:** If you need to integrate the smart switch with an EtherNet/IP network for I/O operations, then IGMP Snooping and IGMP Query may be needed; when you click the EtherNet/IP button, the smart switch enables IGMP Snooping and IGMP Query automatically. **NOTE:** To configure additional SNMP settings, left click the SNMP button to enter the SNMP settings page. The SNMP button will always show in green disregarding if SNMP is enabled or disabled. **NOTE:** When clicking the MECHATROLINK button, the switch will disable GVRP and LLDP, and apply certain required VLAN configuration settings.

Rotary DIP Switch

The SDS-(G)3000 switches are classified as smart Ethernet switches. The rotary DIP switches located on the bottom panel of the SDS-(G)3000 facilitate one-step configuration to enable Industrial Protocol and DHCP client in only a few seconds without having to use a web browser.

The Rotary DIP switch has ten options that can be selected by pointing the arrow in that direction. The default setting 0 represents no DIP switch function is enabled and follows the configuration in the web interface. Options 1 to 7 can be used for PROFINET, Modbus, Ethernet/IP, MECHATROLINK-4 profiles, and DHCP clients. The options 8 to 9 are reserved for future use. Please reboot the device after changing the rotary DIP switch settings to enable the function.



NOTE

We strongly recommend using a 2.0 mm flathead screwdriver to rotate the DIP switch.

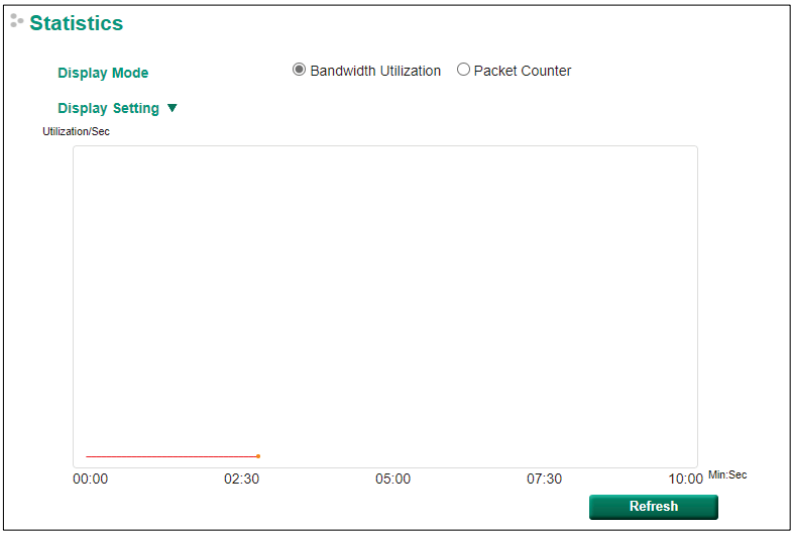
Rotary DIP Switch Settings for IA Profile:

Indicator	Mode
0	No function enabled via DIP switch (default)
1	PROFINET profile enabled
2	PROFINET profile and DHCP Client enabled
3	Ethernet/IP profile enabled
4	Ethernet/IP profile and DHCP Client enabled
5	Modbus TCP profile enabled
6	Modbus TCP profile and DHCP client enabled
7	MECHATROLINK-4 profile enabled
8-9	Reserved (currently performs the same behavior as indicator 0)

Detailed Descriptions of Management Bar Buttons

Statistics Instructions

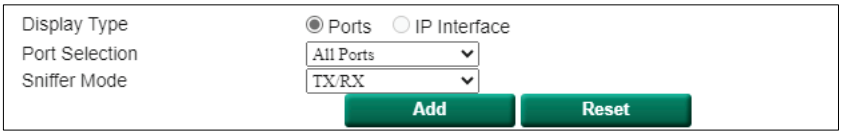
The following screenshot gives an overview of the statistics settings page, including details of each parameter.



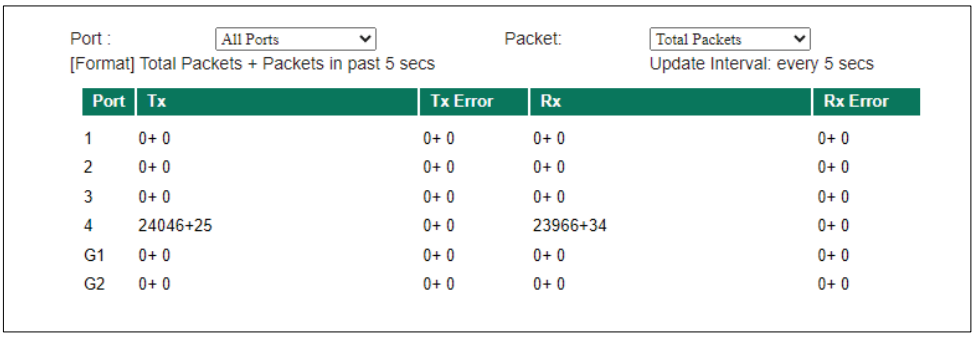
Display Mode

Setting	Description	Factory Default
Bandwidth Utilization	Shows the bandwidth statistics.	Bandwidth Utilization
Packet Counter	Shows the packet counter statistics.	

Display Setting



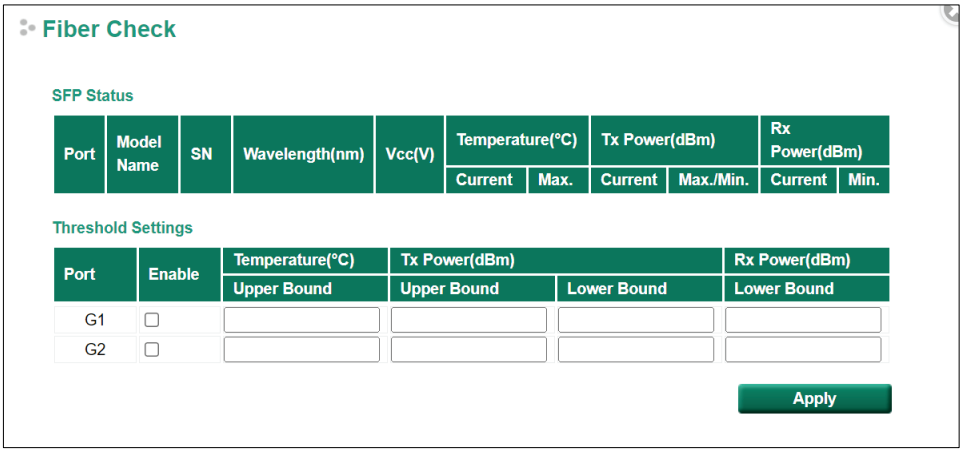
From the **Port Selection** field, you can select the ports to include in the statistics graph. In **Sniffer Mode**, you can choose to view the ports' reception or transmission status, or both.



The port table below the statistics graph shows detailed packet information for specified ports. Select the port to include from the **Port** field. Select the specific types of packets that need to be monitored from the **Packet** field. There are four types of packets: **Total Packets**, **TX Packets**, **RX Packets**, and **Error Packets**. TX packets are packets sent out from the switch, RX packets are packets received from connected devices, and error packets are packets that did not pass TCP/IP's error checking algorithm. The **Total Packets** option displays the combined number of TX, RX, and TX Error, RX Error Packet activity.

Fiber Check Instructions

Optical fiber is commonly used for long-distance data transmissions. This makes it is very costly to troubleshoot fiber cables and fiber transceivers at remote sites when issues occur. **Fiber Check** makes it easier for users to determine if the fiber modules are working properly and be notified when the threshold has been exceeded from the central site. The following screenshot gives an overview of the fiber settings page, including details of each parameter.



SFP Status

Setting	Description
Port	The switch port number with a fiber connection.
Model Name	The name of the Moxa SFP type fiber model.
SN	The serial number of the fiber module.
Wavelength (nm)	The wavelength of the fiber connection.
Vcc (V)	The voltage supply to the fiber connection.
Temperature (°C) – Current	The current temperate of the fiber connection.
Temperature (°C) – Max.	The maximum temperature threshold for the fiber connection.
Tx power (dBm) – Current	The current amount of light being transmitted through the fiber optic cable.
Tx power (dBm) – Max.	The maximum threshold of light being transmitted through the fiber optic cable.
Tx power (dBm) - Min.	The minimum threshold of light being transmitted through the fiber optic cable.
Rx power (dBm) – Current	The current amount of light being received from the fiber optic cable.

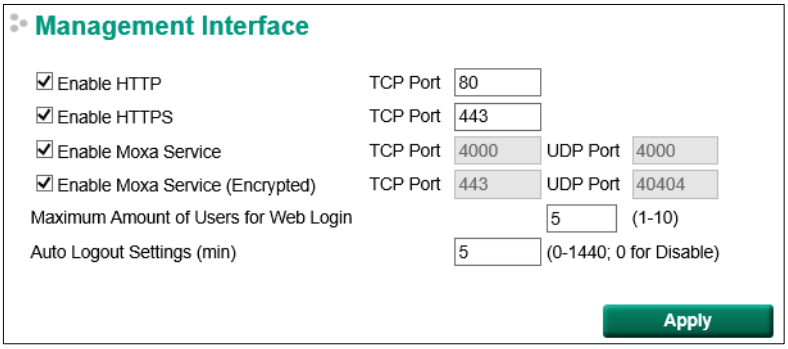
Setting	Description
Rx power (dBm) – Min.	The minimum threshold of light being received from the fiber optic cable.

Threshold Settings

Port	Description
Port	The switch port number with a fiber connection.
Enable	Check to apply the threshold specified values to the corresponding port.
Temperature (°C) – Upper Bound	Specify the maximum temperature threshold of the fiber connection.
Tx Power(dBm) – Upper Bound	Specify the maximum threshold of light being transmitted into the fiber optic cable.
Tx Power(dBm) – Lower Bound	Specify the minimum threshold of light being transmitted into the fiber optic cable.
Rx Power(dBm) – Lower Bound	Specify the minimum threshold of light being received from the fiber optic cable.

Management Interface Instructions

The following screenshot gives an overview of the management interface settings page, including details of each parameter.



Enable HTTP

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

Enable HTTPS

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

Enable Moxa Service

Setting	Description	Factory Default
Select/Deselect	Select the checkbox to enable Moxa Service. **NOTE:** Moxa Service only applies to the Moxa network management software suite.	TCP Port: 4000 UDP Port: 4000

Enable Moxa Service (Encrypted)

Setting	Description	Factory Default
Select/Deselect	Select the checkbox to enable Moxa Service (Encrypted). **NOTE:** Moxa Service (Encrypted) only applies to the Moxa network management software suite.	TCP Port: 443 UDP Port: 40404

Maximum Number of Users for Web Log in

Setting	Description	Factory Default
Integer (1 to 10)	Sets the maximum number of users who can log in to the web configuration simultaneously.	5

Auto Logout Setting (min)

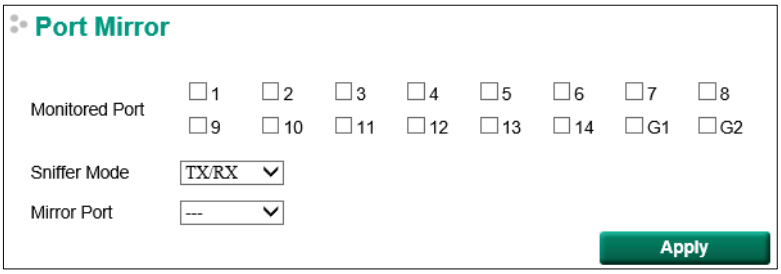
Setting	Description	Factory Default
Integer (0 to 1440)	Sets the web auto logout period. (Enter 0 to disable this function.)	5

NOTE

Press **Apply** once all settings have been properly set to activate the function.

Port Mirror Instructions

The following screenshot gives an overview of the port mirror settings page and details of each parameter.



Port Mirror

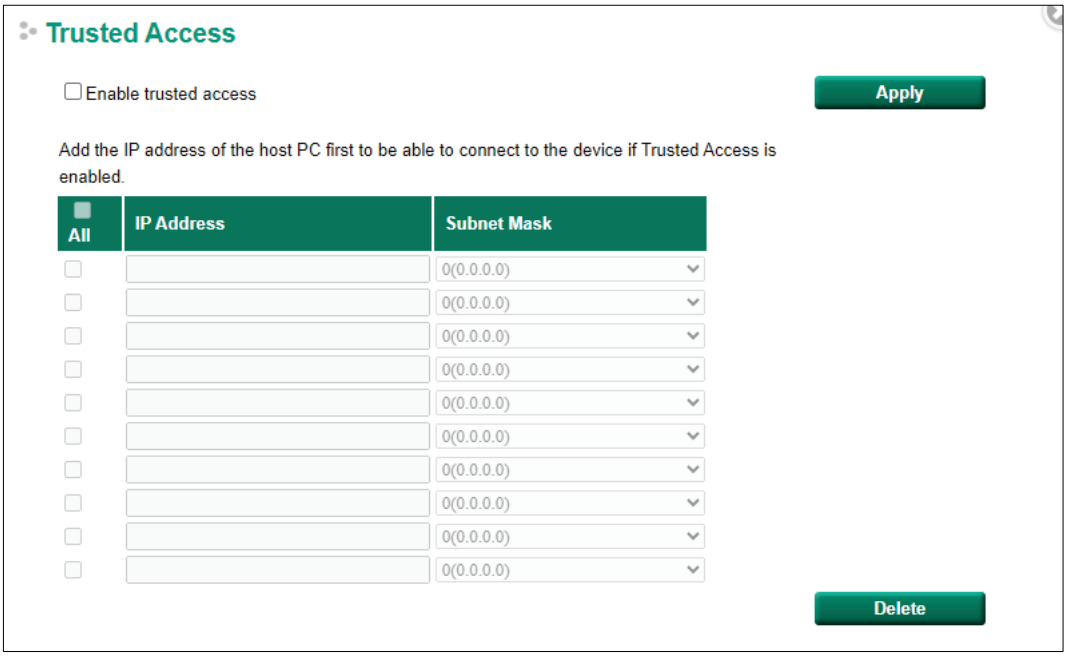
Setting	Description
Monitored Port	Select which ports will be monitored.
Sniffer Mode	Select one of the following three watch direction options: • **RX:** Select this option to monitor only those data packets coming into the Moxa switch's port. • **TX:** Select this option to monitor only those data packets being sent out through the Moxa switch's port. • **TX/RX:** Select this option to monitor data packets both coming into, and being sent out through, the Moxa switch's port.
Mirror Port	Select the number of ports that will be used to monitor the activity of the monitored port.

NOTE

Press **Apply** once all settings have been properly set to activate the function.

Trusted Access Instructions

The following screenshot gives an overview of the Trusted Access settings page, including details of each parameter.



You can add or remove IP addresses from the Trusted Access list to manage access to the Moxa switch. If trusted access is enabled, only addresses in the list will be allowed to access to the Moxa switch. Each IP address and netmask entry can be tailored for different situations:

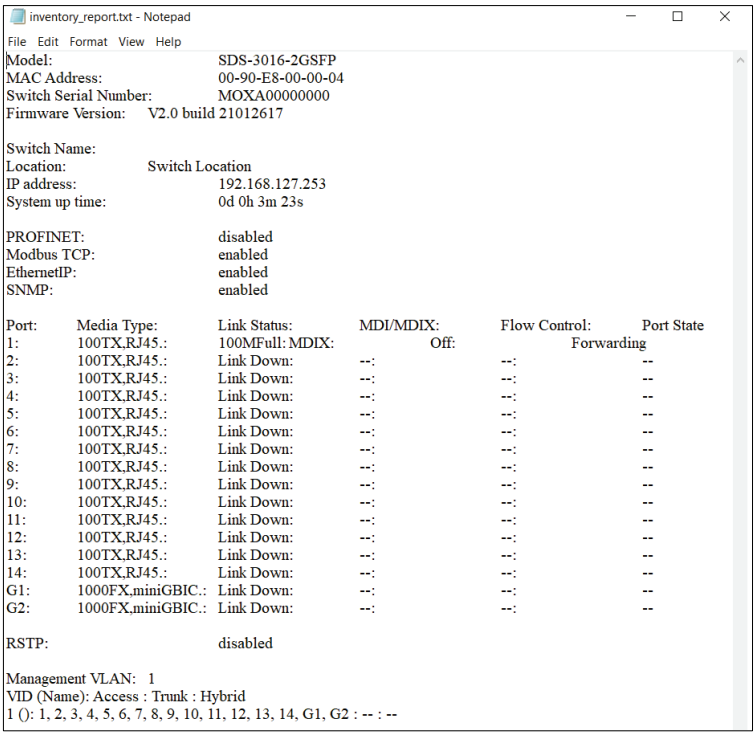
- **Grant access to a single host with a specific IP address**: Specify an IP address (e.g. 192.168.1.1) subnet 255.255.255.255 to only allow the associated IP address to access the switch.
- **Grant access to any host on a specific subnet**: Specify an IP address (e.g. 192.168.1.0) subnet 255.255.255.0 to allow all IP addresses within the 255.255.255.x subnet to access the switch.
- **Grant access to any host**: Disable trusted access to give unrestricted access to any host connecting to the switch.

NOTE

Make sure the current IP and subnet are already added to the Trusted Access list before enabling Trusted Access. If not, the connection will be terminated once Trusted Access is enabled and you may not be able to access the switch anymore.

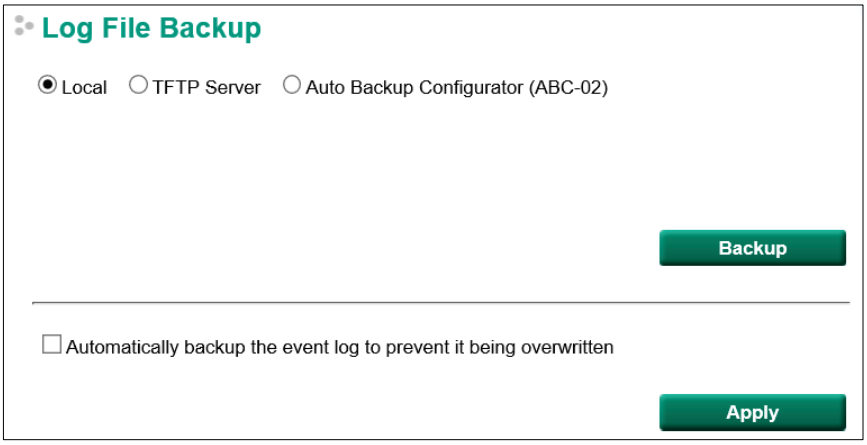
Inventory Report Download

This text file will be downloaded and saved with the following filename:
[Switch Name]_inventory_report.txt.
Information like factory and switch Information will be summarized in a systematic way in this file. Users can also import this text file into Microsoft Excel. Here is example:



Log File Backup Instructions

The log file backup settings page has two main sections. The first section can be used to manually select the destination to which the log file will be saved, and the second part can be used to activate the automatic backup of the event log to prevent it from being overwritten.



Log File Backup Method

Setting	Description	Factory Default
Local	Select **Local** and click the **Backup** button to back up the log file to a local drive.	Local
TFTP Server	Select **TFTP Server**, enter the Server IP and File Name, and then click the **Backup** button to back up the log file.	
Auto Backup Configurator (ABC-02)	Select **Auto Backup Configurator (ABC-02)** and then click **Backup** to save the configuration file to a connected ABC-02. The file will be saved in the ABC-02's **Moxa** folder with filename and extension as **Sys.log**.	

NOTE: Select the proper method and press **Backup** to start the backup.

Automatically Backup the Event Log

Setting	Description	Factory Default
Automatically backup the event log to prevent it from being overwritten	This function is designed to maintain a long-term record of the switch's log files. Moxa Ethernet switches are capable of saving 1000 event log entries. When the 1000-entry storage limit is reached, the switch over write the oldest saved event log. The ABC-02 can be used to back up these event logs. When the number of switch log entries reaches 1000, the oldest 100 log entries will first be copied from the switch to the ABC-02 before they are over written. Enable the **Automatically backup the event log to prevent it being overwritten** option, and then click **Apply**. After that, when the ABC-02 is plugged into the switch, the event logs will always be saved to the ABC-02 automatically when the number of switch log entries reaches 1000. Each backup action saves the oldest 100 logs to the ABC-02 in one file, with the filename generated by the current system time as **MMDDHHmm.log**. The file is saved to the **His_log** folder. **NOTE:** MM=month, DD=day, HH=hour, mm=minutes, from the system time.	unchecked

NOTE

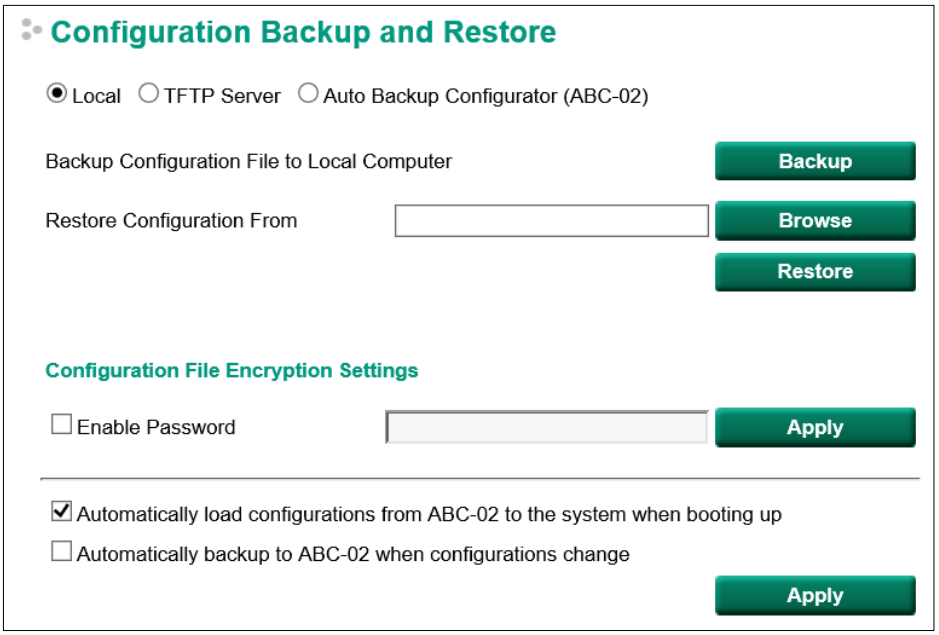
Press **Apply** once to activate the automatic backup function. Be sure an ABC-02 has been attached to the Moxa industrial smart Ethernet switch's USB storage port before activating the function.

The following information is included in the log file:

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

Configuration Backup and Restore Instructions

The configuration backup and restore settings page has three main sections. The first section is used to manually select the destination for backing up and restoring the configuration, the second section is used to set the password for encrypting the downloaded configuration files, and the third section is used to activate automatically restoring the configuration file from an attached ABC-02 when the switch is booted up and backing up the configuration automatically to the attached ABC-02 whenever there is any change.



Configuration Backup and Restore

Setting	Description	Factory Default
Local	1. Select **Local** and click the **Backup** button to back up the configuration file (the file will be named **Sys.ini**) to a local drive. 2. Click **Browse** to search for a configuration on a local disk, and then click the Restore button.	Local
TFTP Server	1. Select **TFTP Server** and enter the TFTP server's IP address. 3. Input the backup/restore file name (supports up to 54 characters, including the .ini file extension) and then click the **Backup/Restore** button.	
Auto Backup Configurator (ABC-02)	1. Click **Backup** to save the configuration file to the ABC-02. The file will be saved in the ABC-02's **Moxa** folder as a *.ini file (e.g., **Sys.ini**). 4. Click **Browse** to select the configuration file, and then click **Restore** to start loading the configuration into the switch. **NOTE:** Two files will be saved to the ABC-02-USB's **Moxa** folder: **Sys.ini** and **MAC.ini**. The purpose of saving the two files is to identify which file will be used when **Auto load configuration from ABC to system when boot up** is activated. **MAC.ini** is named using the last 6 digits of the switch's MAC address, without spaces.	

NOTE

Select the method you would like to use and then press **Backup** to start the backup operation.

Configuration File Encryption Setting

Setting	Description	Factory Default
Enable Password	1. In order to back up an encrypted configuration file from a smart switch, select the checkbox and type in a password to enable encrypting the configuration file when it is downloaded. 5. When loading the encrypted configuration file into a smart switch, first enable the function and type in the corresponding password to decrypt the configuration file while it is being loaded.	unchecked

Automatically Load and Restore the Configuration

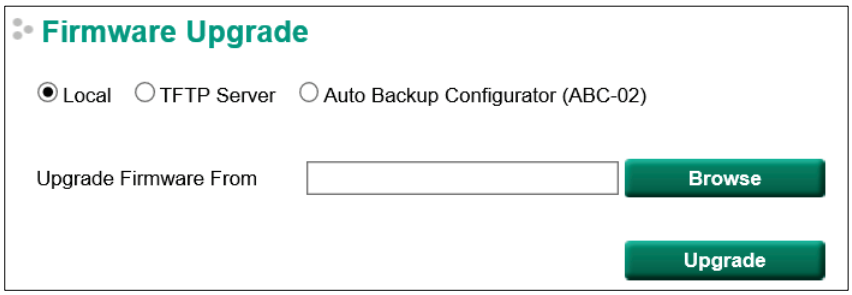
Setting	Description	Factory Default
Automatically load configurations from the ABC-02 to the system when booting up	1. Enable this function by selecting the **Automatically load configurations from ABC-02 to the system when booting up** checkbox and then click **Apply**. 6. Power off your switch first, and then plug in the ABC-02. When you power on your switch, the system will detect the configuration file on the ABC-02 automatically. The switch will recognize the file name, with the following sequence priority: • First priority: **MAC.ini** • Second priority: **Sys.ini** If no matching configuration file is found, the fault LED light will turn on, and the switch will boot up normally. **NOTE:** The MAC.ini configuration file should be named using the last 6 digits of the switch's MAC address, without spaces.	Checked
Automatically backup to ABC-02 when configurations change	1. Enable this function by checking the **Automatically backup to ABC-02 when configurations change** checkbox and then click **Apply**. 7. Attach a Moxa ABC-02 for backing up the switch configuration files automatically. Once the current configuration is modified, the switch will back up the modified configuration to the **/His_ini** folder on the ABC-02. The file name will be the system date/time **(MMDDHHmm.ini)**. **NOTE:** MM=month, DD=day, HH=hour, mm=minutes, from the system time.	unchecked

Firmware Upgrade Instructions

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

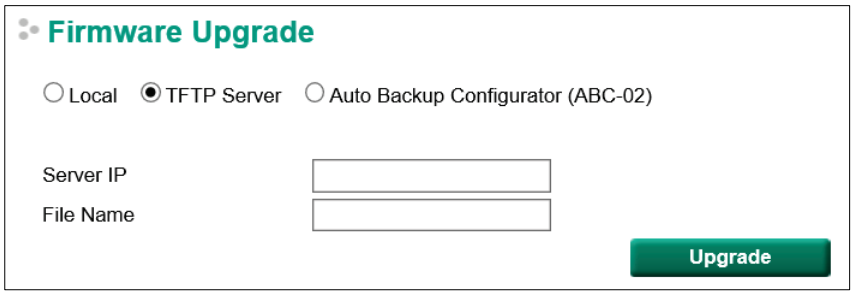
Local

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



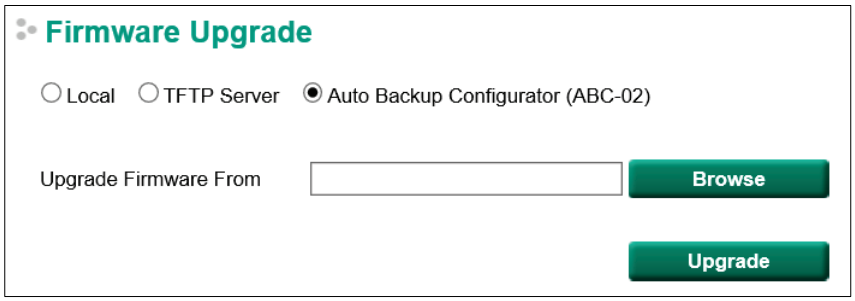
TFTP Server

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



Auto Backup Configurator (ABC-02)

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



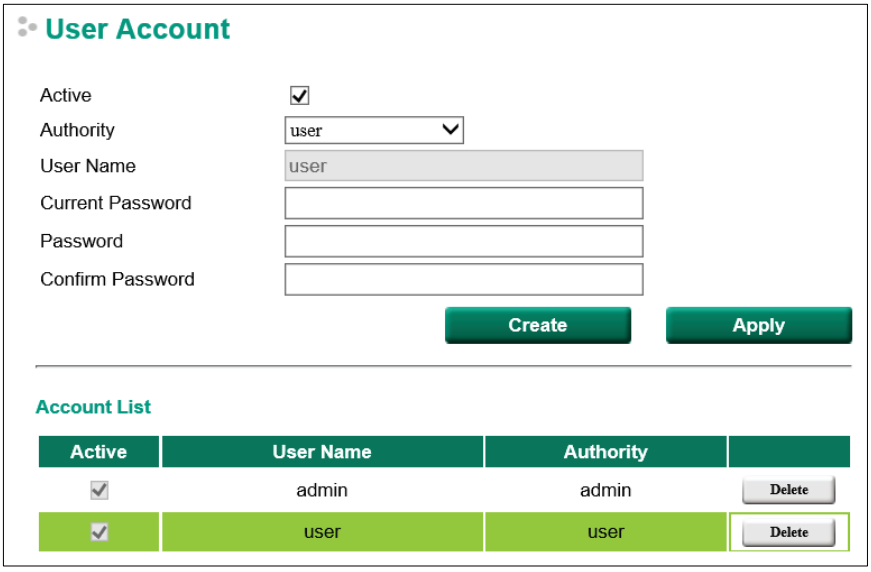
User Account Instructions

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

NOTE

1. In order to maintain a higher level of security, we strongly suggest that you change the password after first logging in.
2. By default, there will be an "admin" user account with **admin** privilege and a "user" user account with **user** privilege. The accounts can be deleted or disabled but at least one account with admin privilege activated must be maintained at all times.
3. You can create up to a maximum of 10 accounts.

The **User Account** settings page is divided into a top section and a bottom section. To modify the settings of a particular account, click the username for the account in the bottom section to highlight the line associated with the account, and then change the settings for the account in the top section of the page.



Creating a New Account

Type in the user name and password, assign an authority to the new account, and then click **Create**.

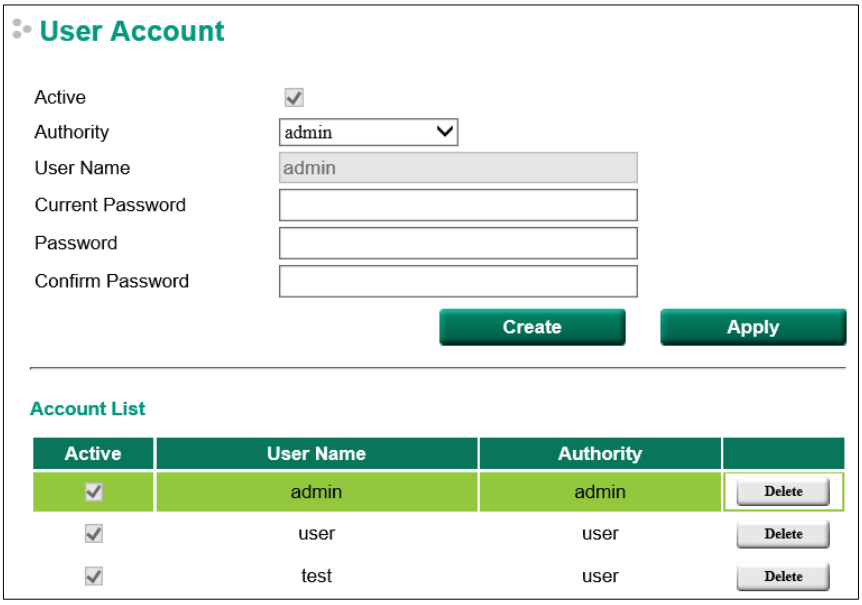
Setting	Description	Factory Default
Active	Check the **Active** checkbox to activate the account; uncheck the checkbox to deactivate the account.	checked
Authority	Select **admin** to assign read/write access to this account; the user will be able to configure all parameters. Select **user** to assign read-only access to this account; the user will only be able to view configuration parameters.	admin
User Name (Max. of 30 characters)	User Name	None
Password	Password for the user account (between 4 and 16 characters)	None
Confirm Password	Re-type in the password to further confirm the setting.	None

NOTE

The naming rule stipulated by SNMPv3 and industrial protocols requires passwords to be more than 8 characters in length; spaces are not allowed.

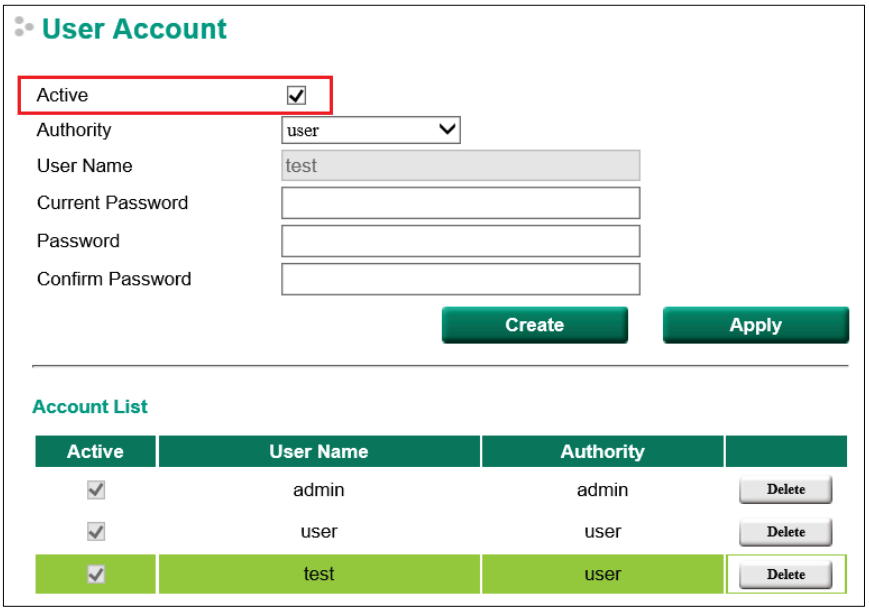
Modifying an Existing Account

Select an existing account from the Account List table, modify the account details (authority, user name, password, etc.), and then click **Apply** to save the changes.



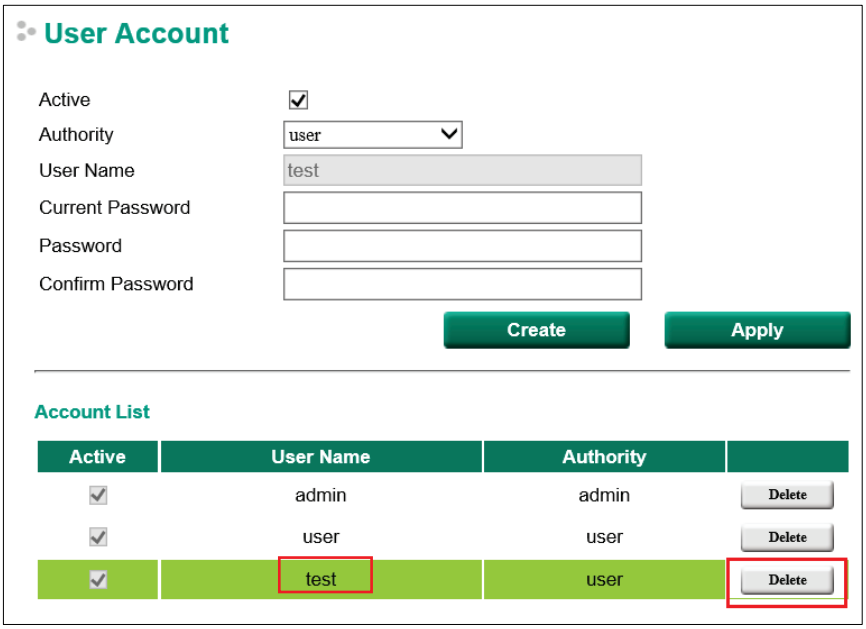
Activate or Deactivate an Existing Account

Select an existing account from the Account List table, check or uncheck the **Active** check box, and then click **Apply** to save the changes.

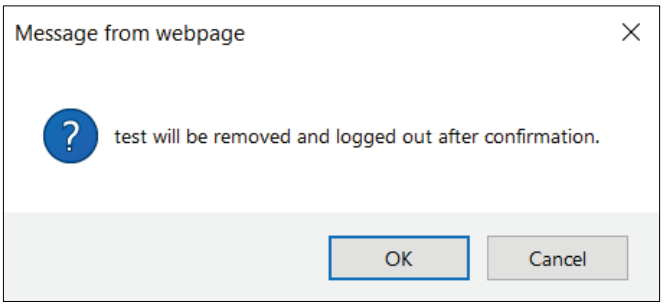


Deleting an Existing Account

Click **Delete** to delete the account.



A warning message will appear, click **OK** to delete the account.



3. Management Functions

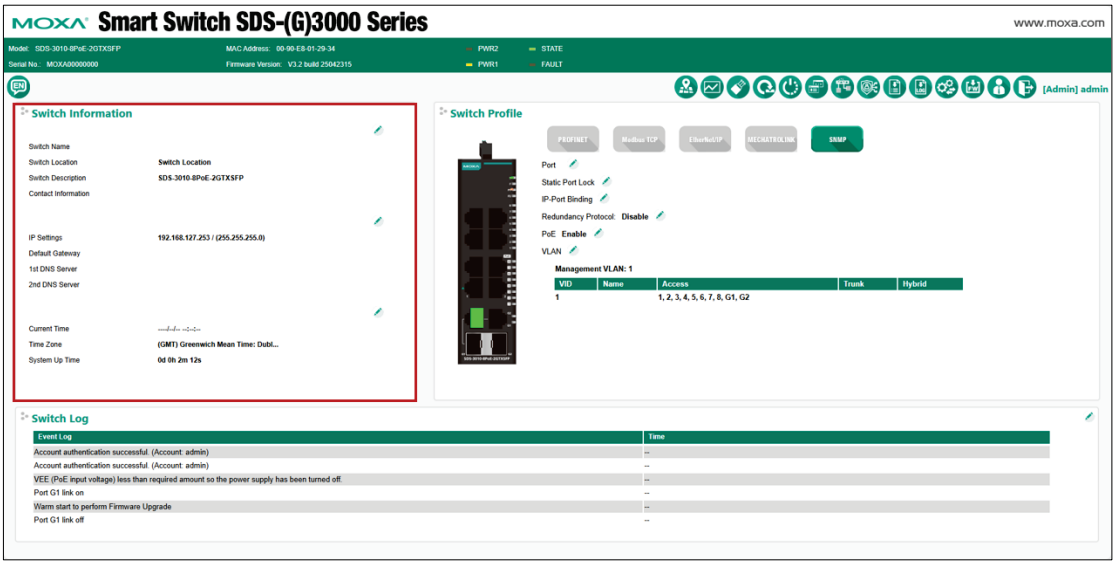
In this chapter, we explain in detail the management functions supported by Moxa's industrial smart Ethernet switch. The configuration and operating results are summarized on the switch's configuration information dashboard for quick reference. You can also use the "edit" icon to edit and adjust the settings to fit the needs of your application or network.

Switch Information

Switch Information is listed on the left side of the switch's configuration information dashboard. The following settings are shown:

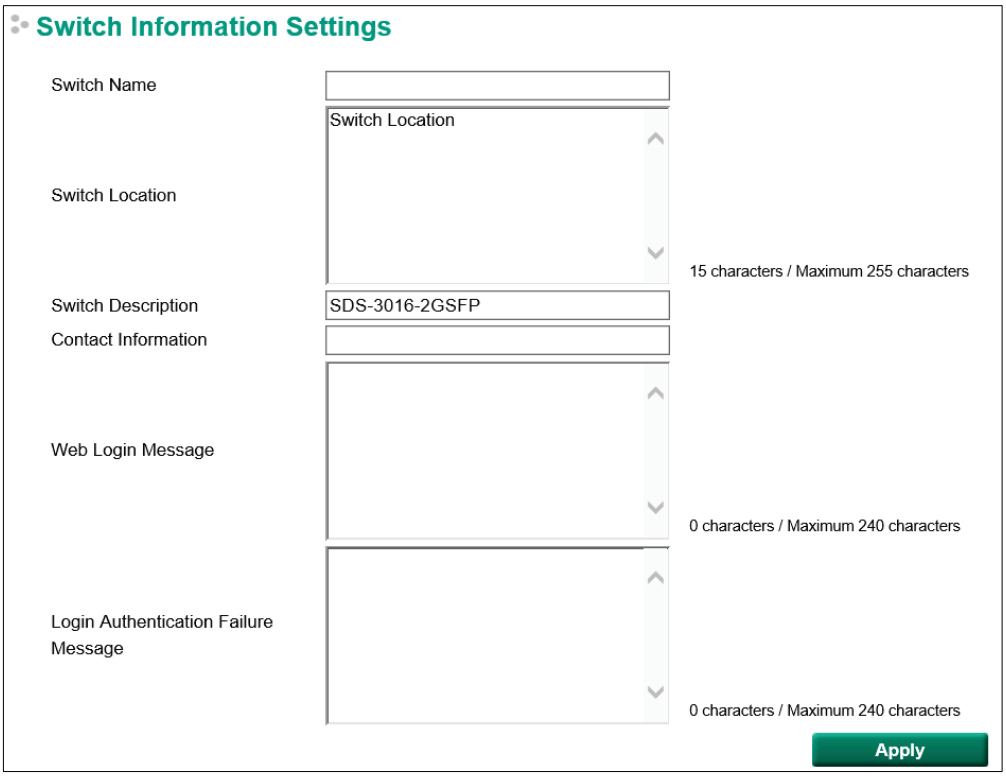
1. System Information
2. Network Information
3. Date and Time Information

Click the **Edit** button to the right of the item you would like to edit.



System Information

The following configuration page will pop up when you click the **Edit** button for the Switch Information Settings section. You can edit the Switch Name, Switch Location, etc.



Switch Name

Setting	Description	Factory Default
Max. 30 characters	This option is useful for differentiating between the roles or applications of different units. Example: Factory Switch 1.	none

NOTE

The Switch Name field follows the PROFINET I/O naming rule. The name can only include these characters: **a-z/A-Z/0-9/-/.**, and the name cannot start with **port-xyz** or **port-xyz-abcde** where xyzabcde=0, 1, ..., 9 or is in the form n.n.n.n where n=0, 1, ..., 9

Switch Location

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

Switch Description

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

Contact Information

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

Web Login Message

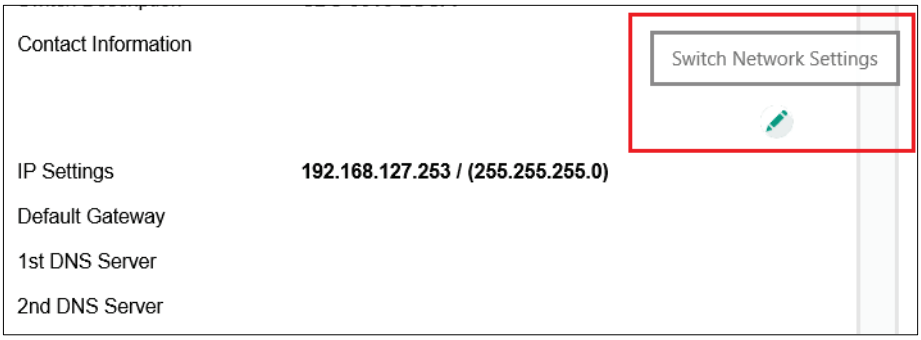
Setting	Description	Factory Default
Max. 240 characters	This option is useful as it shows a message when a user's login is successful	None

Login Authentication Failure Message

Setting	Description	Factory Default
Max. 240 characters	This option is useful as it shows a message when a user's login has failed	None

Network Information

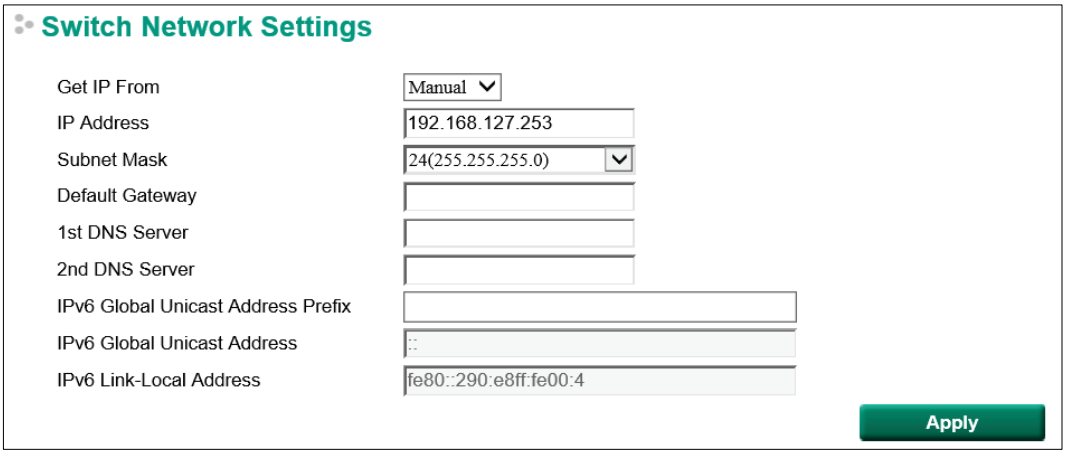
Click the **IP Settings** edit icon to update the network settings.



The configuration page shown below will pop up. The switch supports both IPv4 and IPv6, and can be managed through either of these address types.

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

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



NOTE

If the Moxa industrial smart Ethernet switch is configured for other VLAN settings, make sure the PC host is connected to the same management VLAN (default is 1) that the Moxa smart switch is connected to.

Get IP From

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

IP Address

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

Subnet Mask

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

Default Gateway

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

DNS Server IP Addresses

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

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

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

IPv6 Global Unicast Address

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

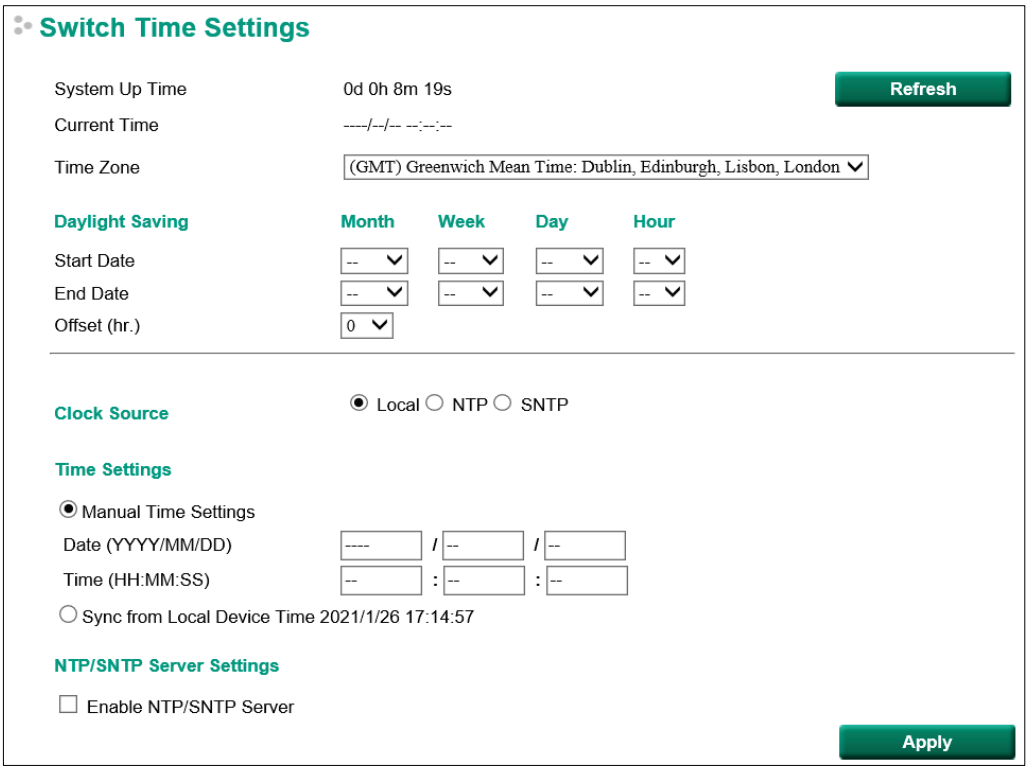
IPv6 Link-Local Address

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

Date and Time Information

The following page will pop up when you click the Switch Information System Time Settings **Edit** button. You can configure the System Up Time, Current Time, etc.

The Moxa industrial smart Ethernet switch also has a time calibration function based on information from an NTP/SNTP server or user-specified time and date, allowing functions such as log and trap to include a time and date stamp.



System Time

System Up Time

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

Current Time

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

Time Zone

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

NOTE

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

Daylight Saving Time

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

Start Date

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

End Date

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

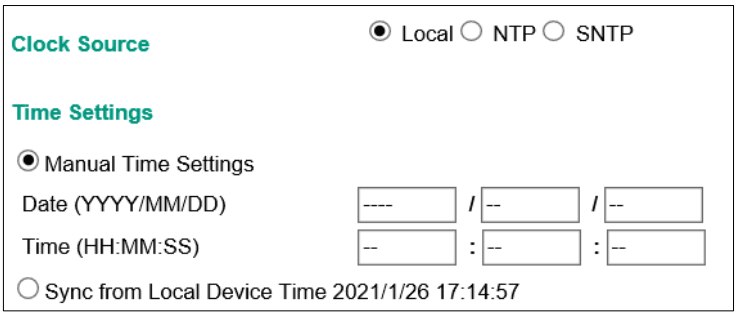
Offset

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

Clock Source

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

Clock Source is From Local

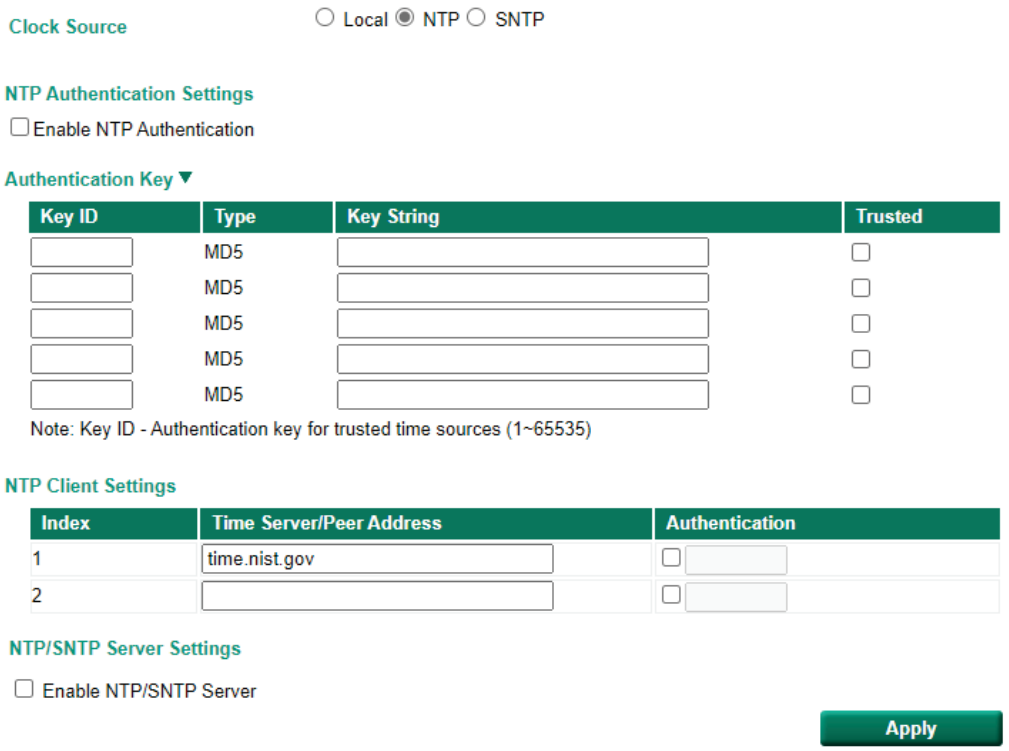


Time Settings

You can set the smart switch's date and time manually by selecting the **Manual Time Settings** option. Type in the corresponding Date and Time or sync automatically from a local host (local device) connected to the smart switch.

Clock Source is From NTP

The Moxa smart switch can work as an NTP client. You can enable the NTP Authentication function to authenticate between the NTP client and NTP server using a configured Authentication Key.



NTP Authentication Settings

Setting	Description	Factory Default
Checked	Enable NTP Authentication	Unchecked
Unchecked	Disable NTP Authentication	

Authentication Key

You can configure up to five Authentication Keys in Moxa smart switch's database. The Keys are encrypted by type MD5 and authorized between the NTP server and the NTP client.

Key ID

Setting	Description	Factory Default
Key ID	ID of the Authentication Key	Unchecked

Key String

Setting	Description	Factory Default
Key String	Password of the Authentication Key (maximum 32 characters)	Unchecked

Trusted

Setting	Description	Factory Default
Checked	Enable the Authentication Key	Unchecked
Unchecked	Disable the Authentication Key	

NTP Client Settings

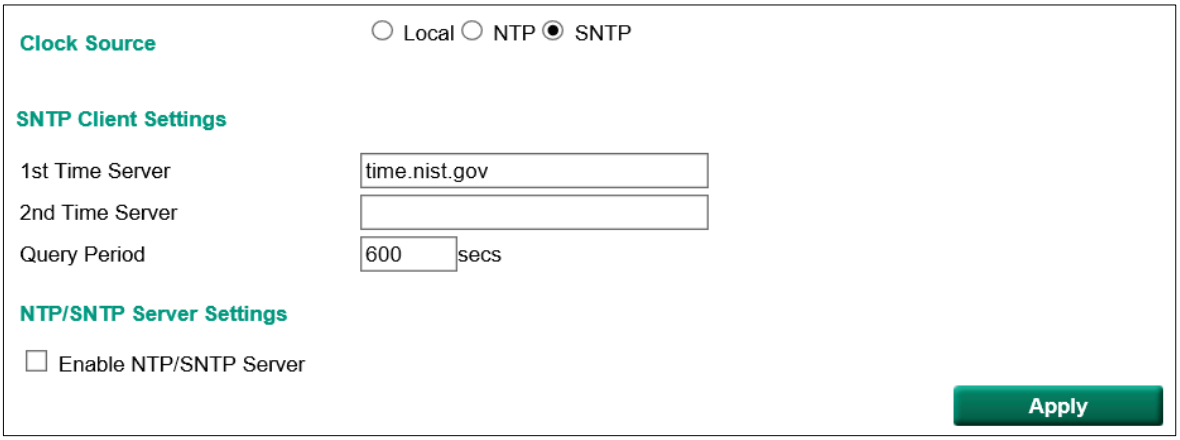
The NTP server should be set when the Moxa smart switch is configured to work as an NTP client.

Setting	Description	Factory Default
Time Server/Peer Address	The domain of Time Server or Peer Address	time.nist.gov

Authentication

Setting	Description	Factory Default
Checked	Enable NTP Authentication	Unchecked
Unchecked	Disable NTP Authentication	
Key ID	The Key ID used for authorization	Null

Clock Source is from SNTP



SNTP Client Settings

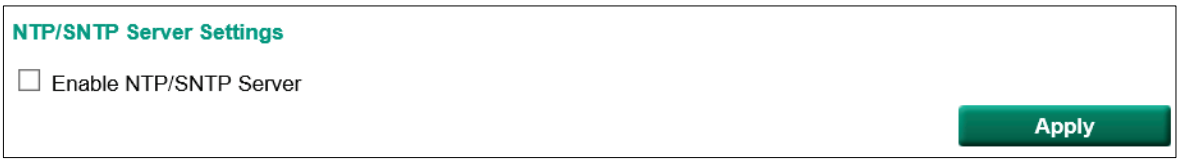
Setting	Description	Factory Default
1st Time Server	The IP or domain address (e.g., 192.168.1.1, time.stdtime.gov.tw, or time.nist.gov).	Time.nist.gov
2nd Time Server	The Moxa smart switch will try to locate the secondary SNTP server if the first SNTP server fails to connect.	
Query Period	The time period to sync with the time server	600 sec.

NOTE

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

NTP/SNTP Server Settings

The Moxa switch can work as an NTP server. The NTP server checkbox should be enabled when the Moxa smart switch will be used as an NTP server.



Enable NTP/SNTP Server

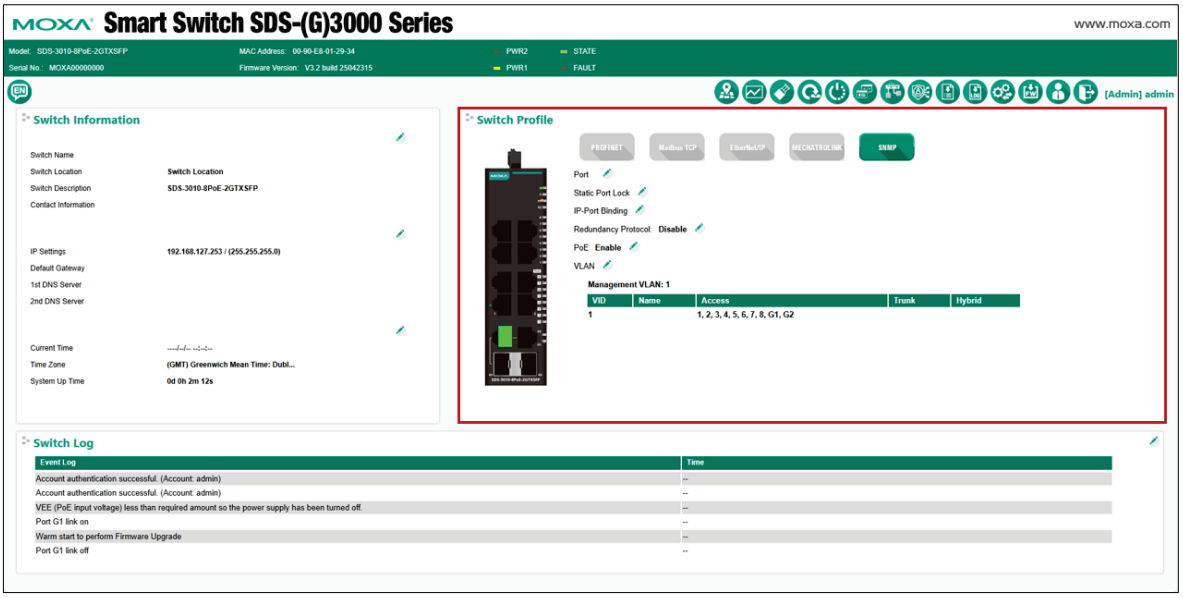
Setting	Description	Factory Default
Enable/Disable	Enables SNTP/NTP server functionality for clients	Disabled

Switch Panel and Profile

The Switch Profile panel is located on the right side of the switch's configuration information dashboard. The panel indicates the current status of the following items:

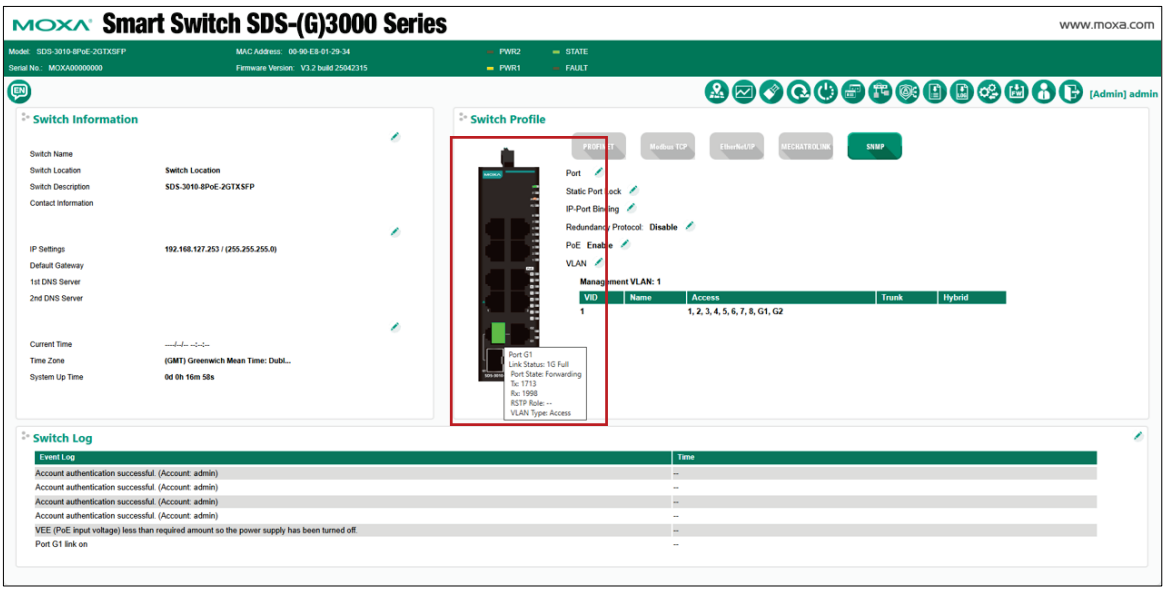
1. Port (port status and TX/RX statistics shown on the panel diagram)
2. Static Port Lock (configure static port lock settings)
3. IP-Port Binding (configure IP-port-binding settings)
4. Redundancy Protocol (configure redundant protocol settings)
5. VLAN (configure VLAN settings)

Click a **Protocol** button to activate or deactivate a protocol, and click the **Edit** button if you need to modify the settings.



Switch Panel and Statistics

The image of the front panel of the smart switch shown on the dashboard can be used to view the switch's current operational information. When you pass the mouse over a port on the panel, a table summarizing the port's current TX/RX statistics will pop up. The example below shows the status of port 8.



The following is shown in the summary table:

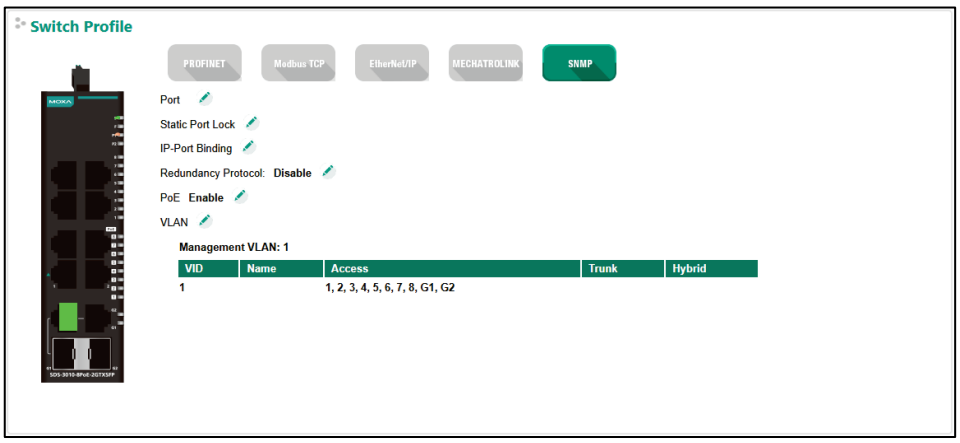
Port Number Index	The port number
Link Status	The current connection speed and duplex mode of the port
Port State	The link state of the port; there are several states, including Disable, Blocking, Listening, Learning, and Forwarding
TX	The TX transmission speed (packets per second)
RX	The RX transmission speed (packets per second)
RSTP Role	The RSTP role of the port; there are several states, including Unknown, Alternate, Root, Designated, and Backup
VLAN Type	An index to show you the VLAN port type setting on the specific port; there are three types the VLAN ports: Access (Default), Trunk, and Hybrid
PD Type (PoE models only)	The type of the PD connected to the port; there are several types, including NIC, IEEE 802.3af, IEEE 802.3at, Legacy PoE Device, and Unknown
PD Consumption (Watts) (PoE models only)	The power consumption of the PD connected to the port

Industrial Protocols and SNMP Settings

All three industrial protocols are disabled by default and can be enabled by clicking the corresponding button. A green button indicates the function is enabled; a grey button means the function is disabled. The protocol will operate based on the protocol's default settings, which can be modified if needed.

SNMP is disabled by default although the button will appear green. To enable and configure SNMP settings, click the SNMP button.

When a certain industrial profile is enabled, some of the managed functions and corresponding parameters will be activated and set automatically. For example, when EtherNet/IP is enabled, the smart switch will automatically enable IGMP Snooping and IGMP Query to ensure efficient EtherNet/IP transmissions,

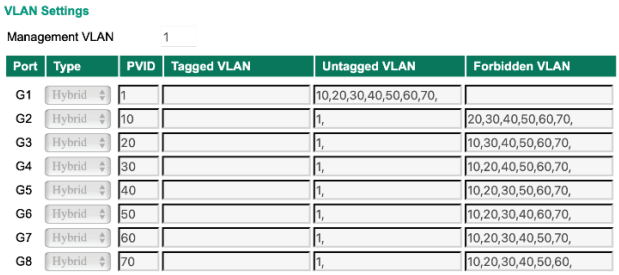


Industrial Protocol and SNMP profiles

<table>
<tr><th>Setting</th><th>Description</th><th>Factory Default</th></tr>
<tr><td>PROFINET</td><td>
1. Click the PROFINET button to enable the Moxa smart switch to perform as a PROFINET I/O device (conformance class B). A comprehensive set of PROFINET I/O attributes (sent via cyclic or acyclic I/O data) are available for more flexible setup and monitoring. To integrate the switch into PROFINET-based HMI/SCADA and PLC (programmable logic controller) systems, you may also need the switch's GSD (General Station Description) file and product image, which you can download from the Moxa industrial smart Ethernet switch product pages.
2. When PROFINET is enabled, a bundle of PROFINET cyclic I/O data will be sent between the PLC and switch periodically (default period = 128 ms). The data is transmitted in near real time, allowing the PLC to check the health and availability of the switch. The following PROFINET cyclic I/O data are provided:
<table>
<tr><th>Category</th><th>Direction</th><th>Byte</th><th>Bit</th><th>Name</th><th>Description</th></tr>
<tr><td rowspan="4">Device</td><td rowspan="4">Input</td><td rowspan="4">0</td><td>0</td><td>Device status</td><td>0: failed
1: OK</td></tr>
<tr><td>1</td><td>Power 1</td><td>0: unavailable
1: OK</td></tr>
<tr><td>2</td><td>Power 2</td><td>0: unavailable
1: OK</td></tr>
<tr><td>3</td><td>RSTP status</td><td>0: disabled
1: enabled</td></tr>
<tr><td rowspan="8">Port</td><td rowspan="8">Input</td><td rowspan="8">1</td><td>0</td><td>Port 1 Connection</td><td rowspan="8">0: not connected
1: connected</td></tr>
<tr><td>1</td><td>Port 2 Connection</td></tr>
<tr><td>2</td><td>Port 3 Connection</td></tr>
<tr><td>3</td><td>Port 4 Connection</td></tr>
<tr><td>4</td><td>Port 5 Connection</td></tr>
<tr><td>5</td><td>Port 6 Connection</td></tr>
<tr><td>6</td><td>Port 7 Connection</td></tr>
<tr><td>7</td><td>Port 8 Connection</td></tr>
<tr><td rowspan="8">Port</td><td rowspan="8">Input</td><td rowspan="8">2</td><td>0</td><td>Port 9 Connection</td><td rowspan="8">0: not connected
1: connected</td></tr>
<tr><td>1</td><td>Port 10 Connection</td></tr>
<tr><td>2</td><td>Port 11 Connection</td></tr>
<tr><td>3</td><td>Port 12 Connection</td></tr>
<tr><td>4</td><td>Port 13 Connection</td></tr>
<tr><td>5</td><td>Port 14 Connection</td></tr>
<tr><td>6</td><td>Port 15 Connection</td></tr>
<tr><td>7</td><td>Port 16 Connection</td></tr>
</table>
3. The Moxa smart switch supports several PROFINET I/O parameters for greater flexibility. These PROFINET I/O parameters use PROFINET acyclic I/O data to achieve communication on the PROFINET network and control PROFINET alarm functions. The PROFINET alarm is a message sent from the switch to the PLC immediately when the corresponding event occurs. These parameters are readable or writable, and users can use the SIMATIC STEP 7 tool or engineering deployment software to edit the parameters and set up the alarm. For details about the Moxa switch's support for PROFINET and a list of PROFINET I/O parameters that are supported, see the Moxa Industrial Protocols User's Guide on the Moxa industrial smart Ethernet switch product pages.

NOTE: The transfer frequency of the PROFINET Cyclic I/O data on the Moxa industrial smart Ethernet switch is fixed at 128 ms.
</td><td>Disabled</td></tr>
</table>

Setting	Description	Factory Default
Modbus TCP	1. Click the Modbus TCP button to enable the Modbus TCP protocol on the Moxa smart switch. The Modbus TCP protocol can be used to integrate the smart switch with Modbus TCP–based HMI/SCADA systems. 2. The Modbus TCP protocol is commonly used to integrate a SCADA system. It is also a vendor neutral communication protocol used to monitor and control industrial automation equipment such as PLCs, sensors, and meters. In order to be fully integrated into industrial systems, Moxa's industrial smart Ethernet switches support the Modbus TCP protocol profile to provide users with a quick way to set up and integrate the switch with HMI or SCADA systems for better monitoring. Once the Modbus TCP profile is enabled, data can be read using the following data access types: Function code 4 with 16-bit (2-word) data access, or read only. The types of data that can be read include system information, port information, packet information, redundancy information, etc. For more details regarding the Moxa industrial smart Ethernet switch's support of Modbus TCP and the Modbus TCP data mapping, see the Moxa Industrial Protocols User's Guide on the Moxa industrial smart Ethernet switch product pages.	Disabled
EtherNet/IP	1. Click the EtherNet/IP button to enable the Moxa smart switch to perform as an Ethernet/IP device (adapter class). A comprehensive set of objects and corresponding attributes and services (sent via explicit messaging or implicit messaging) are available for flexible setup and monitoring. To integrate the switch into Ethernet/IP-based HMI/SCADA and PLC (programmable logic controller) systems, you may also need the switch's EDS (Electronic Data Sheet) file, AOI (Add-on Instruction) file, and the product image, which you can download from the Moxa industrial smart Ethernet switch product pages. 2. Several CIP (Common Industrial Protocol) communication objects are defined. Moxa's smart switches support the following objects for monitoring PLCs and HMI/SCADA systems: • Identity Object • TCP/IP Interface Object • Ethernet Link Object • Assembly Object • Message Router Object • Connection Manager Object • Port Object • Moxa Networking Object (Vendor Specific) For more details regarding the supported attributes and services of the above objects and the access rules for each attribute, see the Moxa Industrial Protocols User's Guide on the Moxa industrial smart Ethernet switch product pages. **NOTE:** If you need to integrate the smart switch with an EtherNet/IP network for I/O operations, then IGMP Snooping and IGMP Query may be needed; when you click the EtherNet/IP button, the smart switch enables IGMP Snooping and IGMP Query automatically.	Disabled

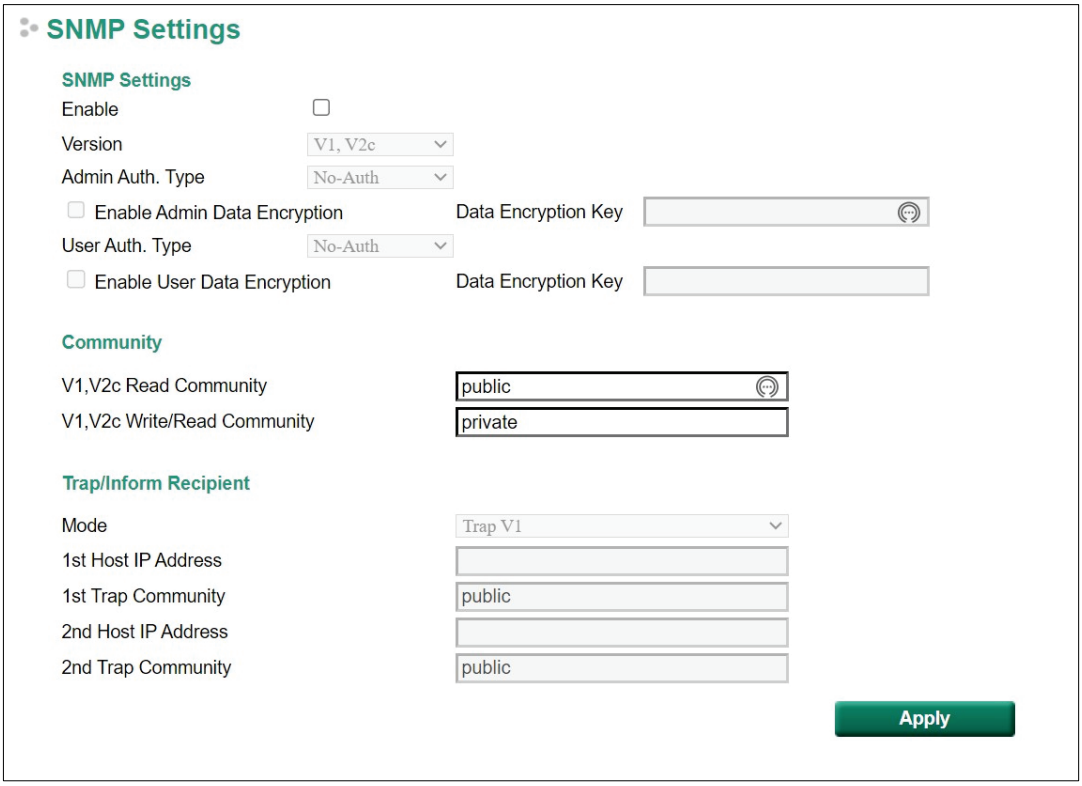
<table>
<tr><th>Setting</th><th>Description</th><th>Factory Default</th></tr>
<tr><td>MECHATROLINK-4</td><td>1. Click the MECHATROLINK button to enable the Moxa smart switch to act as a MECHATROLINK-4 device.
2. When enabling MECHATROLINK-4, the following configuration changes will be made automatically:
• Disable GVRP
• Disable LLDP
• Preconfigure Hybrid VLAN settings
 

NOTE: When MECHETROLINK-4 is enabled, the aforementioned automatic configuration changes will be applied and cannot be changed. This means the VLAN settings page will be unavailable until MECHATROLINK is disabled. If MECHATROLINK-4 was enabled through the DIP switch, it can be disabled using one of the following methods:
1. Set the DIP switch arrow back to zero, then disable MECHATROLINK in the web console.
2. Set the DIP switch arrow back to zero, then power cycle the switch.</td><td>Disabled</td></tr>
</table>

<table>
<tr><th>Setting</th><th>Description</th><th>Factory Default</th></tr>
<tr><td>SNMP</td><td>1. Click the SNMP button to enable SNMP and show a pop-up with related settings.
2. The Moxa smart switch supports SNMP V1, V2c, and V3. SNMP V1 and SNMP V2c use a community string match for authentication, which means that SNMP servers access all objects with read-only or read/write permissions using the community strings public and private by default. SNMP V3, which is the most secure protocol, requires that you select an authentication level of MD5 or SHA. You can also enable data encryption to enhance data security. SNMP security modes and levels that are supported are shown in the following table. Select the security mode and level that will be used to communicate between the SNMP agent and manager.
<table>
<tr><th>Protocol Version</th><th>UI Setting</th><th>Authentication</th><th>Encryption</th><th>Method</th></tr>
<tr><td>SNMP V1, V2c</td><td>V1, V2c Read Community</td><td>Community string</td><td>No</td><td>Uses a community string match for authentication.</td></tr>
<tr><td></td><td>V1, V2c Write/Read Community</td><td>Community string</td><td>No</td><td>Uses a community string match for authentication.</td></tr>
<tr><td>SNMP V3</td><td>No-Auth</td><td>No</td><td>No</td><td>Uses an account with admin or user to access objects</td></tr>
<tr><td></td><td>MD5 or SHA</td><td>Authentication based on MD5 or SHA</td><td>No</td><td>Provides authentication based on HMAC-MD5, or HMAC-SHA algorithms. 8-character passwords are the minimum requirement for authentication.</td></tr>
<tr><td></td><td>MD5 or SHA</td><td>Authentication based on MD5 or SHA</td><td>Data encryption key</td><td>Provides authentication based on HMAC-MD5 or HMAC-SHA algorithms, and data encryption key. In addition to a minimum password length of 8 characters, a data encryption key must be set.</td></tr>
</table>
The above parameters can be configured on the SNMP page that pops up when you click the SNMP button.

NOTE: The username and password of SNMP V3 are the same as the username and password of User Account. Accounts with admin privilege have read/write access to all configuration parameters. Accounts with user authority only have read access to configuration parameters.</td><td>Disabled</td></tr>
</table>

SNMP Settings



SNMP Read/Write Settings

SNMP Versions

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

V1, V2c Read Community

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

V1, V2c Write/Read Community

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

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

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

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

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

Setting	Description	Factory Default
Enable	Enables data encryption using the specified data encryption key (between 8 and 30 characters).	No
Disable	Specifies that data will not be encrypted.	No

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

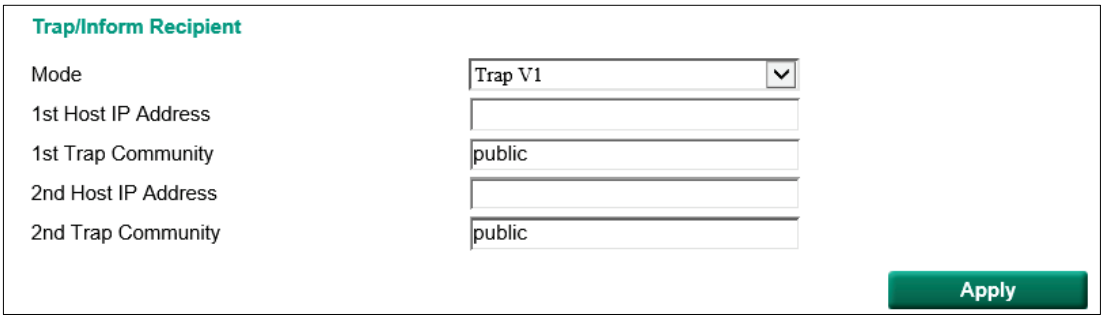
Setting	Description	Factory Default
No-Auth	Allows the admin account and user account to access objects without authentication.	No
MD5-Auth	Authentication will be based on the HMAC-MD5 algorithms. 8-character passwords are the minimum requirement for authentication.	No
SHA-Auth	Authentication will be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

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

Setting	Description	Factory Default
Enable	Enables data encryption using the specified data encryption key (between 8 and 30 characters).	No
Disable	No data encryption	No

Trap Settings

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



SNMP Trap Mode—Trap

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

SNMP Trap Mode—Inform

SNMPv2 supports an inform mechanism. When an inform message is sent from the SNMP agent to the NMS, the receiver sends a response to the sender acknowledging receipt of the event. This behavior is similar to that of the get and set requests. If the SNMP agent does not receive a response from the NMS for a period of time, the agent will resend the trap to the NMS agent. The maximum timeout time is 300 sec (default is 1 sec), and the maximum number of retries is 99 times (default is 1 time). When the SNMP agent receives acknowledgement from the NMS, it will stop resending the inform messages.

Host IP Address 1

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

1st Trap Community

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

Host IP Address 2

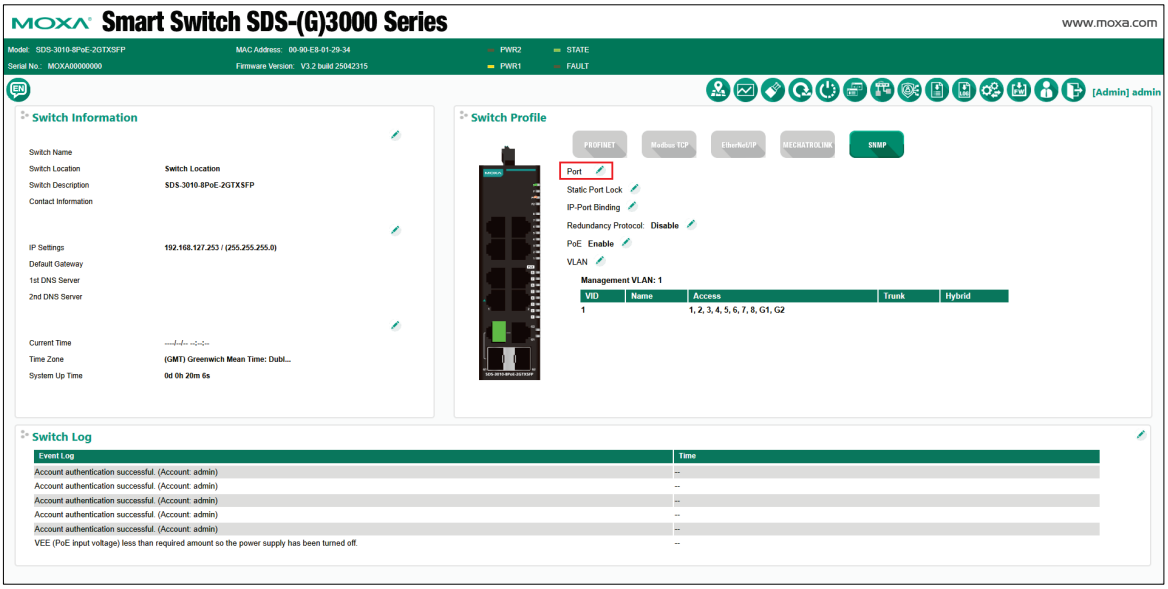
Setting	Description	Factory Default
IP or name	Specifies the IP address or name of the secondary trap server used by your network.	None

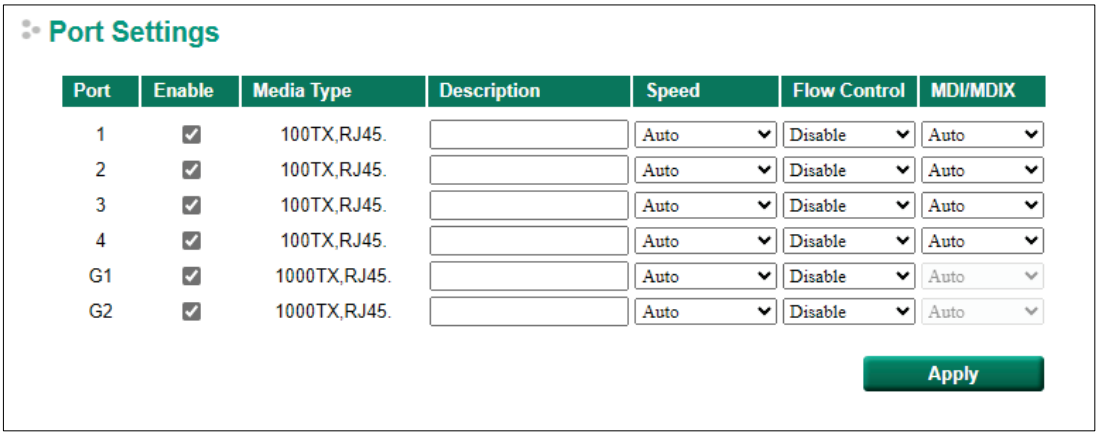
2nd Trap Community

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

Port Settings

Click the Port **Edit** button in the Switch Panel. When the **Port Settings** page pops up, you can configure port access, port transmission speed, flow control, port type (MDI or MDIX), etc.





Enable

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

Media Type

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

Description

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

Speed

Setting	Description	Factory Default
Auto	Allows the port to use the IEEE 802.3u protocol to negotiate with connected devices. The port and connected devices will determine the best speed for that connection.	Auto
100M-Full	Choose one of these fixed port speed options if the connected Ethernet device has trouble auto-negotiating for line speed.	
100M-Half		
10M-Full		
10M-Half		
1G-Full	The speed for G1 and G2 ports is fixed at 1G-Full (SDS-3016-2GFSP Series only).	1G-Full

FDX Flow Ctrl

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

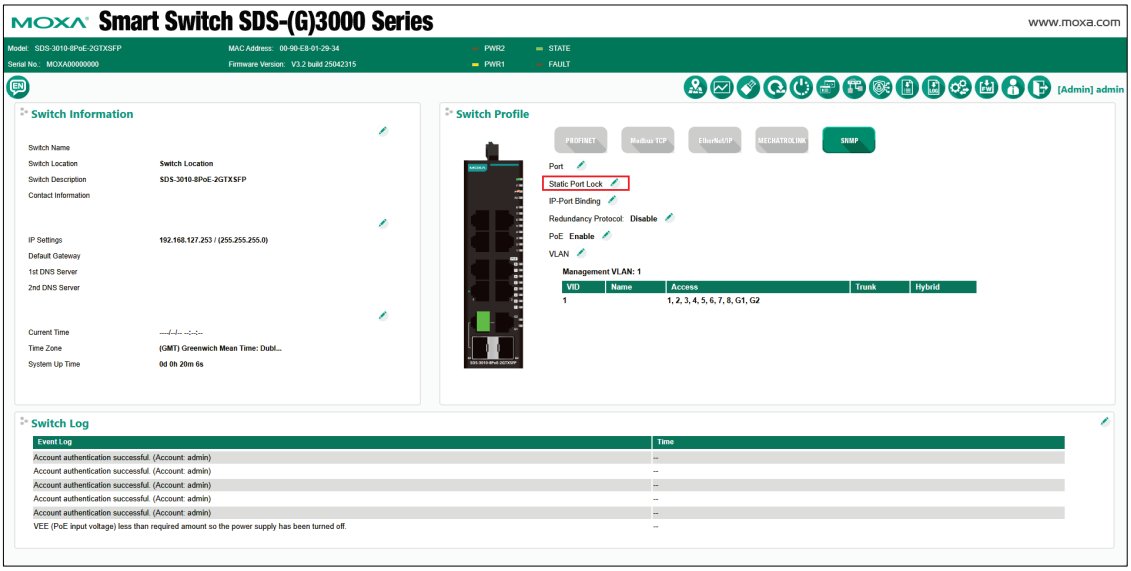
Setting	Description	Factory Default
Enable	Enables flow control for this port when the port's Speed is set to Auto.	Disabled
Disable	Disables flow control for this port when the port's Speed is set to Auto.	

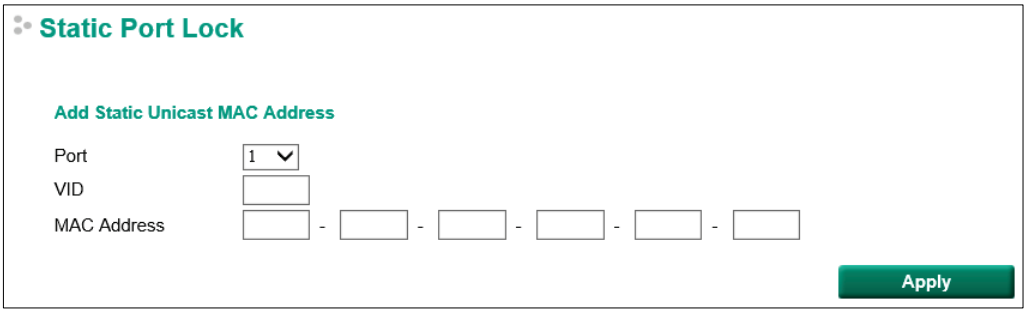
MDI/MDIX

Setting	Description	Factory Default
Auto	Allows the port to auto-detect the port type of the connected Ethernet device and change the port type accordingly. For G1 and G2 ports, the setting is fixed to Auto.	Auto
MDI	Choose MDI or MDIX if the connected Ethernet device has trouble auto-negotiating for port type.	
MDIX		

Static Port Lock Settings

Static Port Lock: Allow users to configure the specific MAC addresses that can access the port. Click the Static Port Lock **Edit** button in the Switch Panel to configure the settings.





Port

Setting	Description	Factory Default
Select the port from the drop-down list	Select the port(s) that will be used with Static Port Lock function.	None

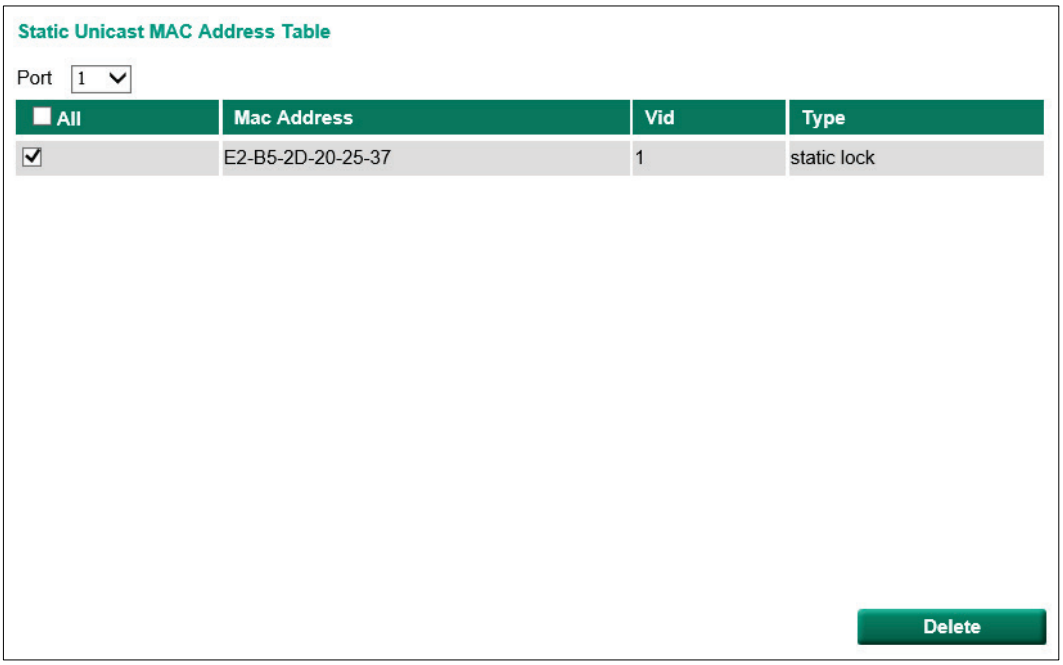
VLAN ID

Setting	Description	Factory Default
Input the VLAN ID	Select the VLAN ID that will use Static Port Lock function.	None

MAC Address

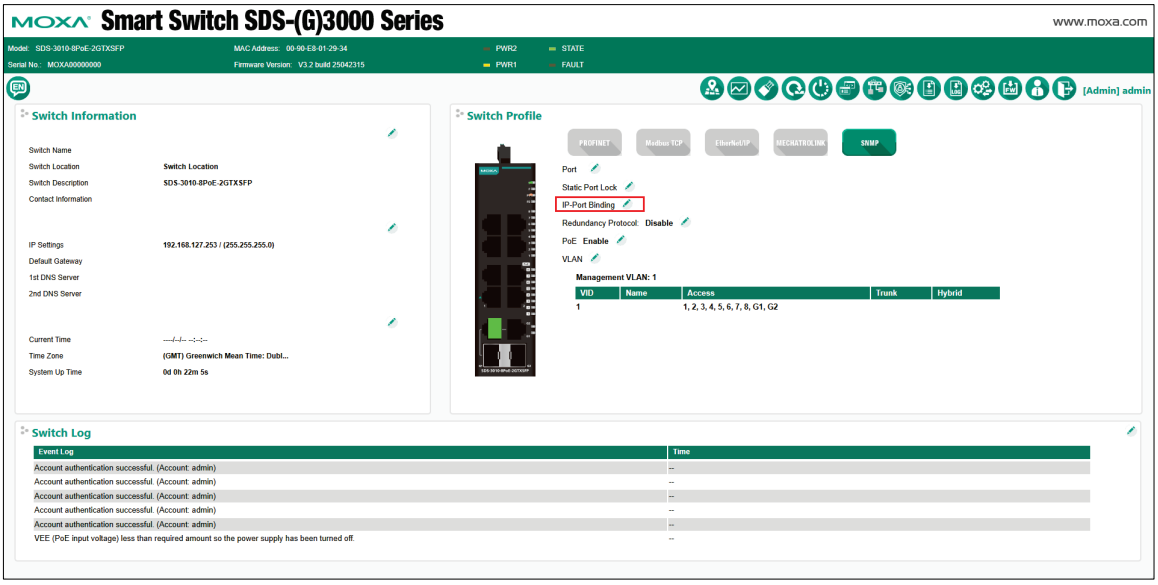
Setting	Description	Factory Default
Input the MAC address that will be used	Provide the MAC Address of the device that will be used as the reliable source for accessing the network.	None

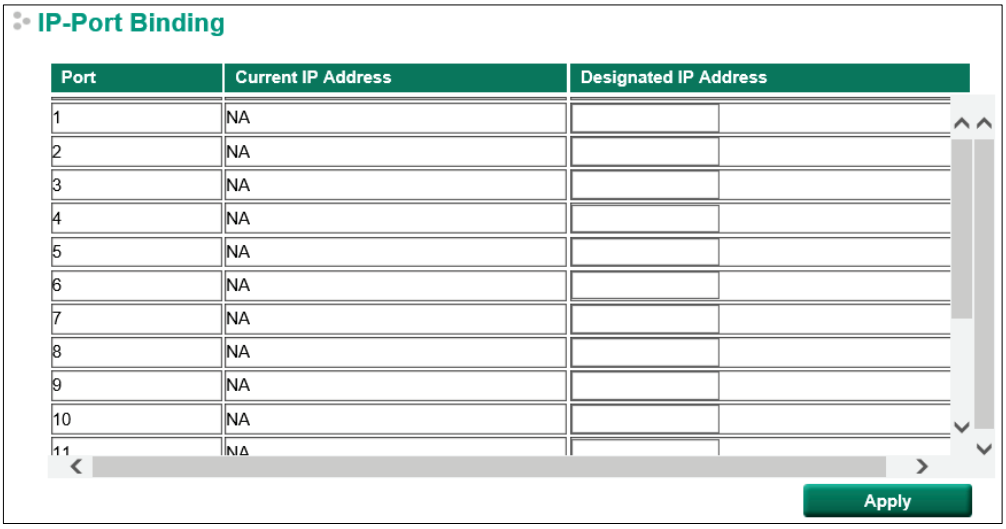
You can view the Static Unicast MAC Address Table on the page. To delete the setting, check the item, and click **Delete**.



IP-Port Binding Settings

Click the IP-Port Binding **Edit** button to configure the settings.





Current IP Address

Setting	Description	Factory Default
Enter the IP address for each port	Specify the IP address for each port on your switch.	None

Designated IP Address

Setting	Description	Factory Default
Enter the designated IP address for each port	Specify the designated IP address for each port you wish to bind to.	None

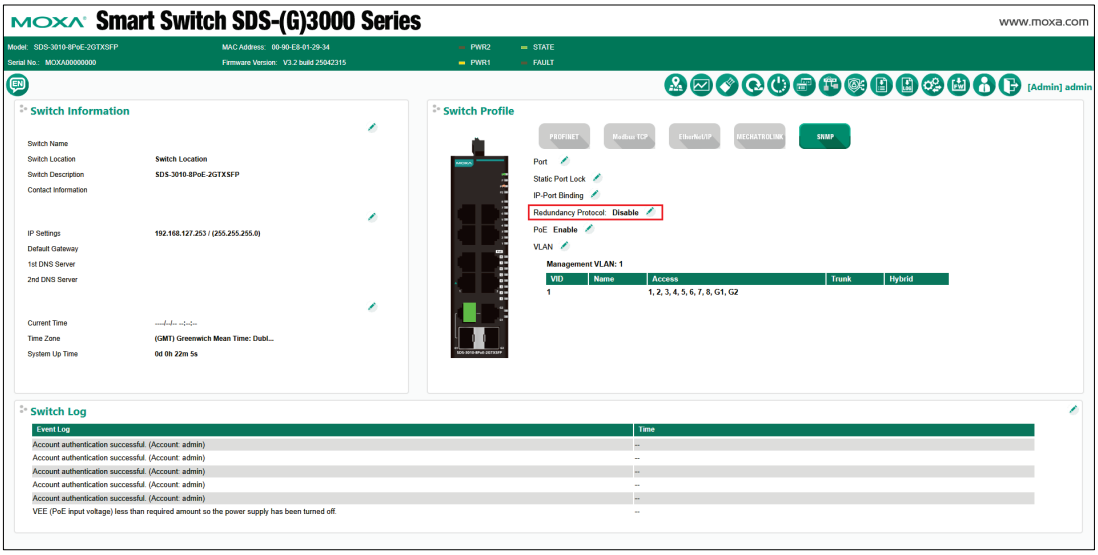
Redundancy Protocol Settings

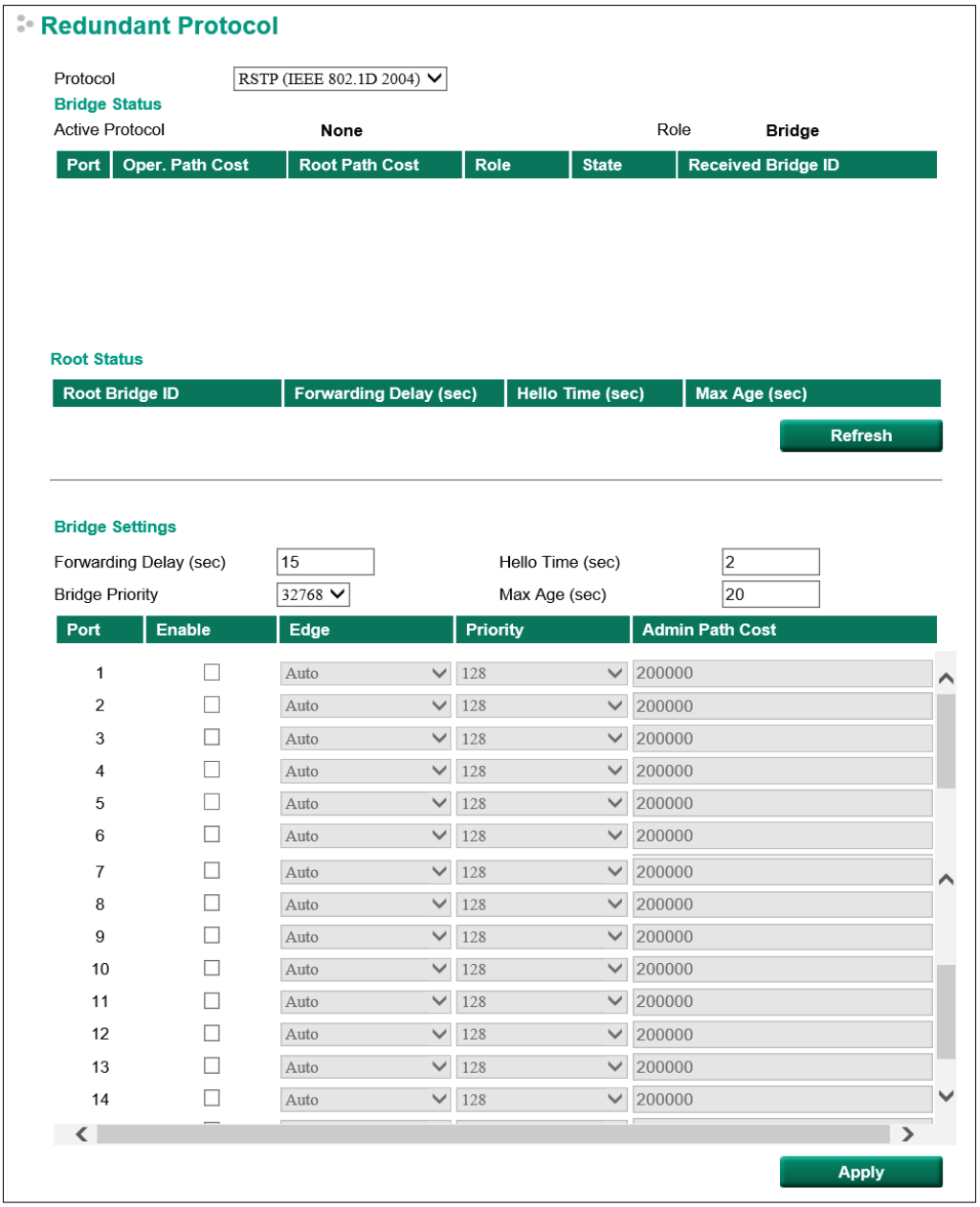
RSTP Settings

The Moxa smart switch supports the standard Rapid Spanning Tree Protocol (RSTP) redundancy mechanism to increase network and system reliability. Click the RSTP (IEEE 802.1D 2004) section Edit button in the Switch Panel's and Profile section to open the settings page to further configure the RSTP protocol. You will also be able to see an overview of the RSTP status in the first part of the page.

NOTE

RSTP can be enabled by port. For more information about the RSTP concept, see **Appendix A**.





Forwarding delay (sec.)

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

Bridge priority

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

Hello time (sec.)

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

Max. Age (sec.)

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

Enable STP per Port

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

NOTE

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

Edge

Setting	Description	Factory Default
Auto	1. If the port does not receive a BPDU within 3 seconds, the port will be in the forwarding state. 2. Once the port receives a BPDU, it will start the RSTP negotiation process.	Auto
Force Edge	The port is fixed as an edge port and will always be in the forwarding state	
False	The port is set as the normal RSTP port	

Priority

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

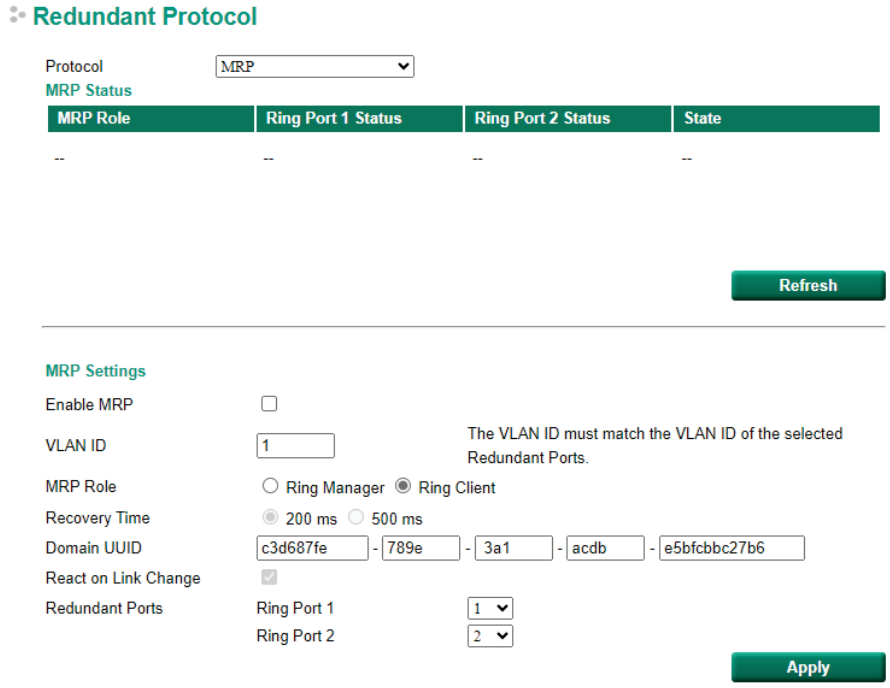
Cost

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

MRP Settings

Media Redundancy Protocol (MRP) is a protocol regulated by the International Electrotechnical Commission as the IEC 62439-2 standard. The main purpose of MRP is that it allows rings of Ethernet switches to recover using a redundant design. It can achieve fast self-redundancy recovery to ensure continuous network data transmission.

Selecting **MRP** from the **Protocol** drop-down list on the Redundant Protocol screen shows the status of the MRP ring and the configurable MRP settings. Refer to the sections below for a detailed description of each parameter.



MRP Status

MRP Role

This indicates if the switch is the **Manager** or a **Client** of the MRP ring.

Ring Port 1/2 Status

This indicates the current ring port status. This will show **Forwarding** when the port is transmitting data normally, **Blocking** if this port is connected to a backup path which is blocked, and **Link down** if there is no connection.

State

This shows the condition of the MRP ring, depending on the MRP role of the switch.

MRP Manager: **Initiation / Awaiting Connection / Primary Ring Port Link Up / Ring Open / Ring Closed.**

MRP Client: **Initiation / Awaiting Connection / Data Exchange Idle / Pass Through / Data Exchange / Pass Through Idle.**

MRP Settings

Enable MRP

Setting	Description	Factory Default
Enable/Disable	Enable or disable the MRP function.	Unchecked

VLAN ID

Setting	Description	Factory Default
1-4094	Specify the VLAN ID, which must align with the Redundant port's VLAN settings.	1

MRP Role

Setting	Description	Factory Default
Ring Manager	Designate the switch as the MRP Manager (MRC).	Ring Client
Ring Client	Designate the switch as an MRP Client (MRC).	

Recovery Time

Setting	Description	Factory Default
200 ms	Set the maximum recovery time to 200 ms.	200 ms
500 ms	Set the maximum recovery time to 500 ms.	

Domain UUID

Setting	Description	Factory Default
User-defined UUID	Specify the UUID (Universal Unique Identifier) to distinguish frames when implementing multiple MRP instances.	Generic UUID example

React on Link Change

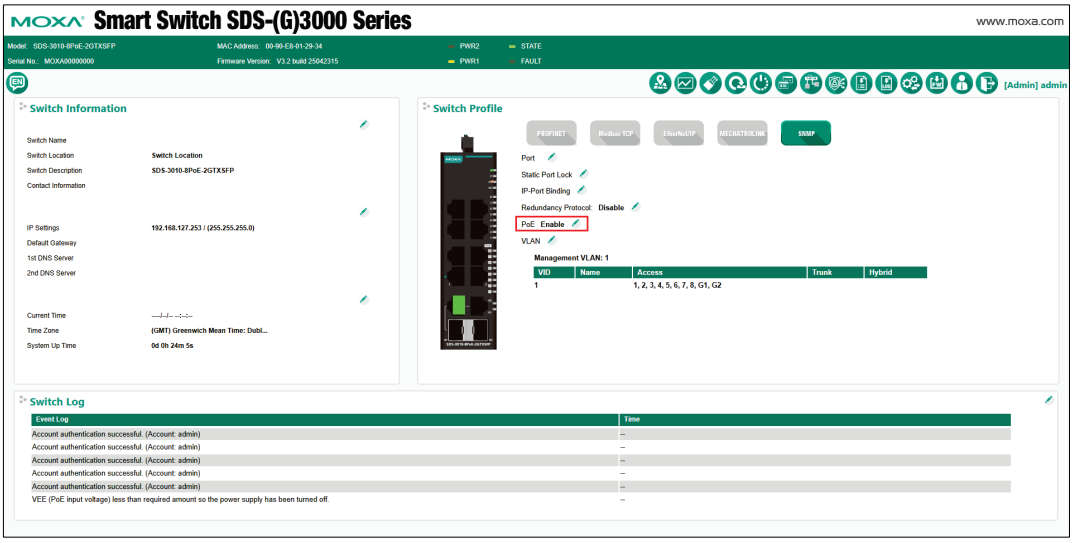
Setting	Description	Factory Default
Enable/Disable	If enabled, the MRM will react to Link Down frames received from an MRC with a Topology Change frame without the need for extra polling mechanisms.	Enabled

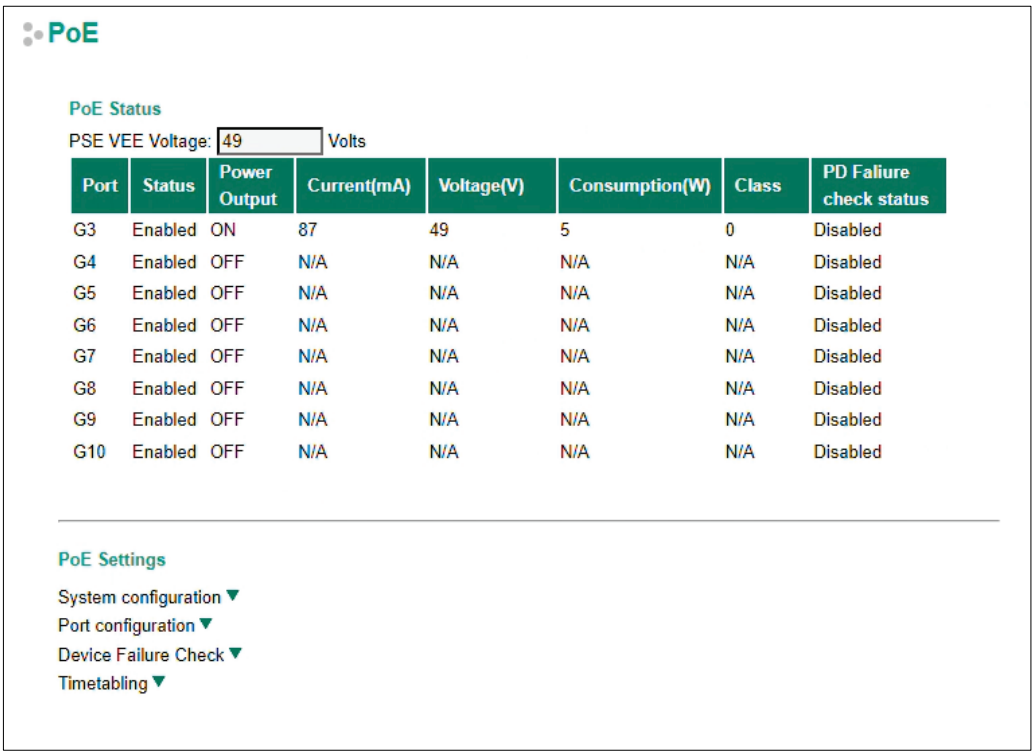
Redundant Ports

Setting	Description	Factory Default
Ring Port 1/2	Select the port from the drop-down list to assign as a redundant port.	Ring Port 1: 1 Ring Port 2: 2

PoE Settings

Click the PoE Edit button to open the PoE page. The PoE page is divided into two parts: PoE Status and PoE Settings. The PoE Status table gives users an overall view of the power supply conditions of each port. The PoE Settings page contains several subsections for granular configuration, including system configuration, port configuration, device failure check, and timetabling.





PoE Status

PSE VEE Voltage

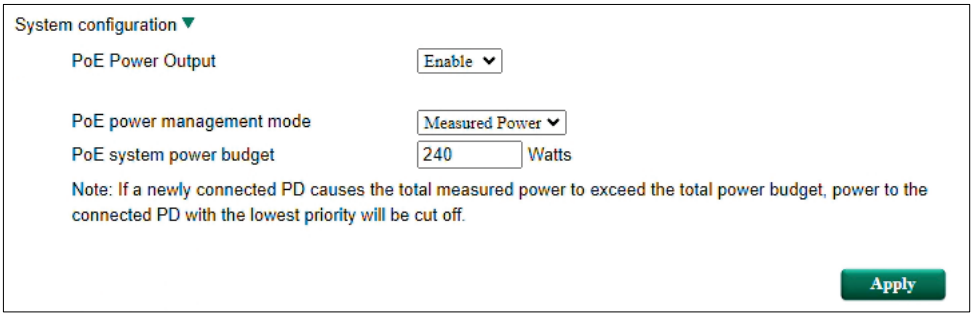
Setting	Description	Factory Default
Voltage (Read-only)	Shows the VEE voltage supplied by the PSE.	N/A

PoE Status Table

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

PoE Settings

System Configuration



PoE Power Output

Setting	Description	Factory Default
Enable	Enable PoE power output to PD on the port.	Enable
Disable	Disable PoE power output to PD on the port.	

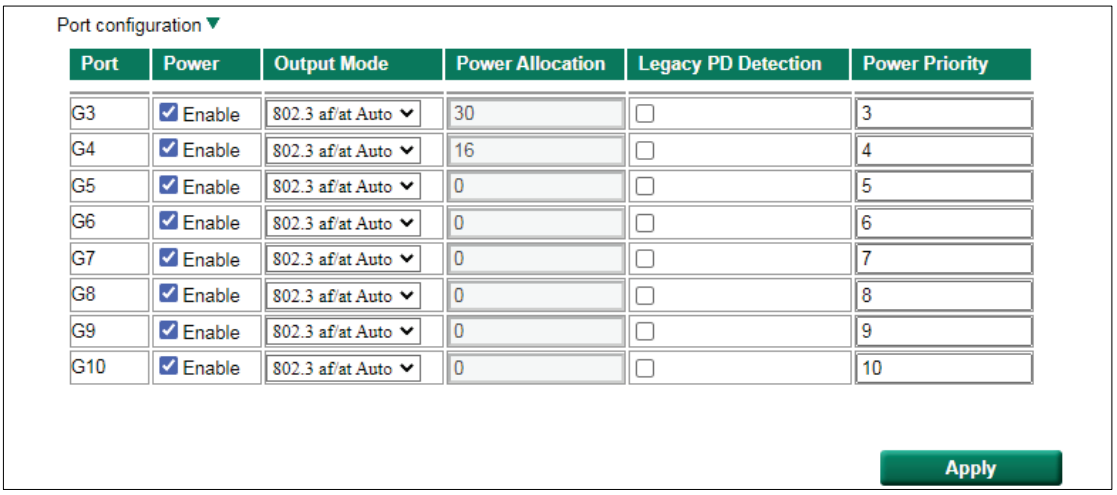
Power Management Mode

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

PoE System Power Budget

Setting	Description	Factory Default
Watt	Specify the total available PoE power budget for all ports combined.	SDS-(G)3006-4PoE-2GTXSFP: depends on input voltage (12 VDC: 45 W, 24 VDC: 90 W, 48 VDC: 120 W) SDS-(G)3010-8PoE-2GTXSFP: 240W

Port Configuration



Power

Setting	Description	Factory Default
Checkbox	Check to enable or disable data and power to be transmitted through the port. If unchecked, power to that port is immediately cut off.	Checked

Output Mode

Setting	Description	Factory Default
802.3 af/at Auto	Power transmission follows the IEEE 802.3af/at protocols. The acceptable PD resistance range is 17 kΩ to 29 kΩ.	802.3 af/at Auto
High Power	Provides a higher power output to the 2-Pair PD. The acceptable PD resistance range is 17 kΩ to 29 kΩ and the power allocation of the port is automatically set to 36 W.	
Force	Provides power output to non-802.3af/at PDs. The acceptable PD resistance is over 2.4 kΩ and the power allocation range is 0 to 36 W.	

Power Allocation

Setting	Description	Factory Default
0 to 36	When the Output Mode is set to Force, specify the power allocation of the port. The valid range is from 0 to 36 W.	Enable

Legacy PD Detection

The PoE Ethernet switch supports the Legacy PD Detection function. When the capacitance of the PD is higher than 3 μF, checking the Legacy PD Detection checkbox enables the system to output power to the PD. In this case, it will take 10 to 15 seconds for PoE power to be output through this port after the switch is turned on.

Setting	Description	Factory Default
Checkbox	Check to enable legacy PD detection.	Unchecked

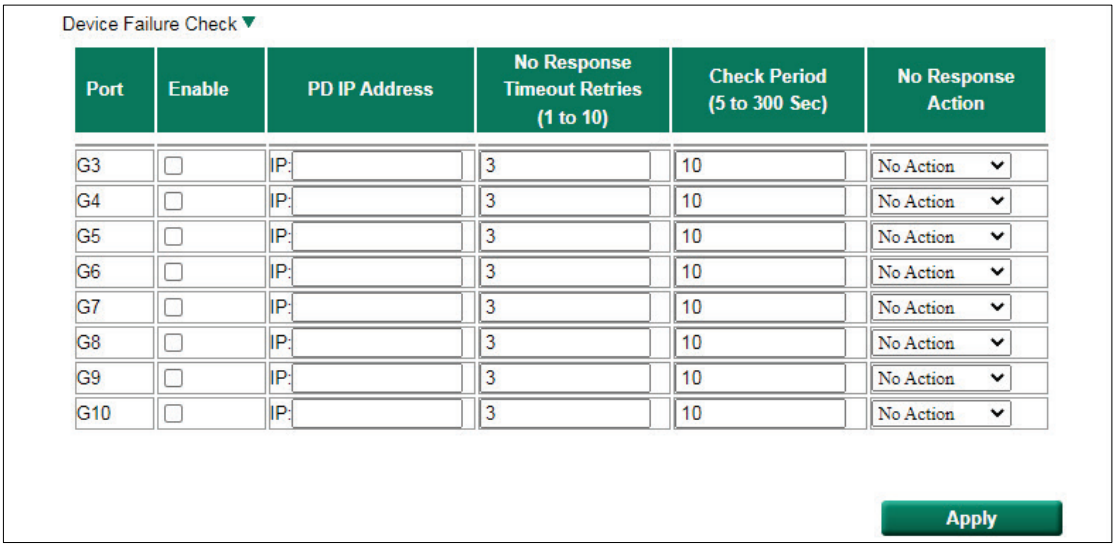
Power Priority

Use Power Priority to define port priorities when using Measured Power mode. The smaller the number, the higher the priority. You may set the same priority for different PoE ports. If you configure two ports with the same priority, the port with the lower port number will have the higher priority. The setting can range from 1 up to the total number of ports. When the PoE measured power exceeds the assigned limit, the switch will disable the PoE port with the lowest priority.

Setting	Description	Factory Default
1 to (max number of PoE ports)	Specify the PoE power port priority for Measures Power mode. The smaller the number, the higher the PoE port priority. When the PoE measured power exceeds the assigned limit, the switch will disable the PoE port with the lowest priority.	PoE port index number

Device Failure Check

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



Enable

Setting	Description	Factory Default
Checkbox	Check to enable or disable device failure checks on the PoE port. If checked, the switch will send packets at the specified interval to check if the connected PD is still alive.	Unchecked

PD IP Address

Setting	Description	Factory Default
IP Address	Specify the IP address of the PD.	N/A

No Response Timeout Retries

Setting	Description	Factory Default
1 to 10	Specify the number of times the switch will attempt to check the PD after not receiving a response before considering the PD unavailable.	3

Check Period

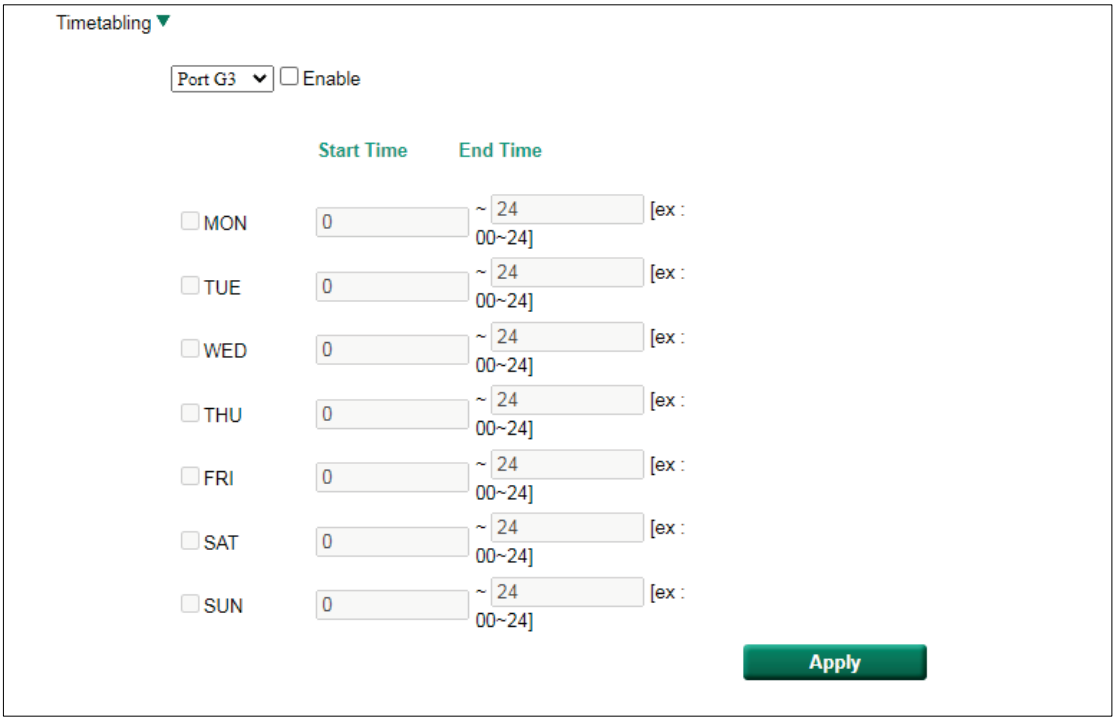
Setting	Description	Factory Default
5 to 300	Specify the time (in seconds) the switch will wait for a response between each check cycle.	10

No Response

Setting	Description	Factory Default
No Action	The PSE will perform any action if the PD fails the PD Failure Check.	No Action
Reboot PD	The PSE will reboot the PD if the PD fails the PD Failure Check.	
Power Off PD	The PSE will power off the PD if the PD fails the PD Failure Check.	

Timetabling

If powered devices do not need to be running 24/7, the PoE Ethernet switch provides a PoE timetabling mechanism that lets users economize the system's power burden by setting a flexible working schedule for each PoE port.



Port

Setting	Description	Factory Default
Port	Select the port to configure a PoE power schedule for.	Port 1

Enable

Setting	Description	Factory Default
Checkbox	Check to enable or disable PoE power scheduling on the selected port.	Unchecked

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

Setting	Description	Factory Default
Checkbox	Check the box to enable or disable PoE power scheduling for the corresponding days of the week. If unchecked, the system will not provide PoE power to the port on that day.	Unchecked

Start/End Time

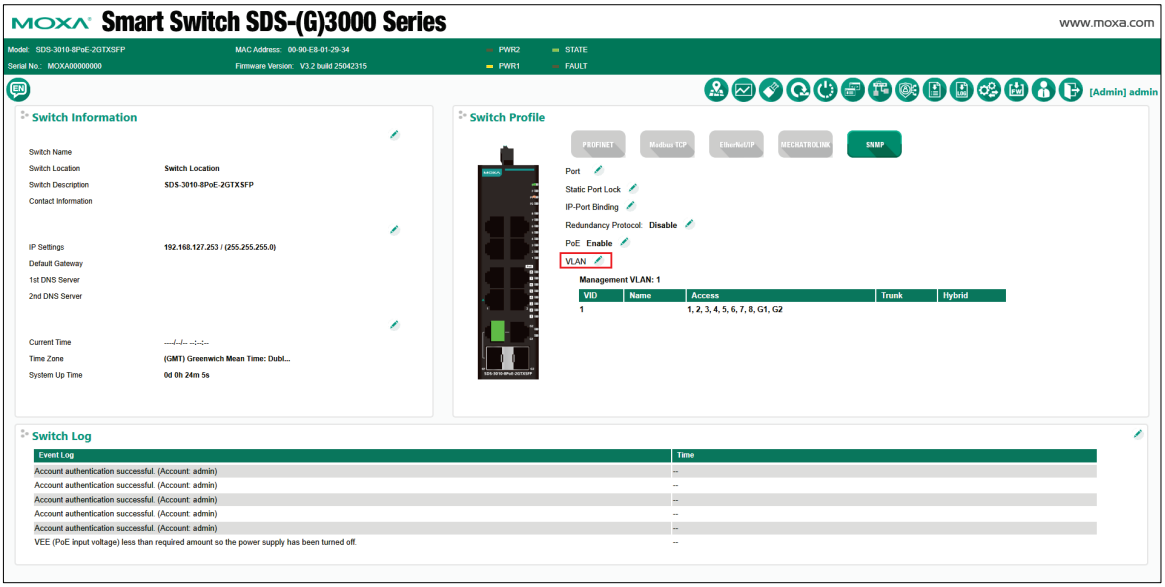
Setting	Description	Factory Default
00 to 24	If PoE power scheduling is enabled, specify the start and end time when the system will provide PoE power to the port on that day.	Start Time: 00 End Time: 24

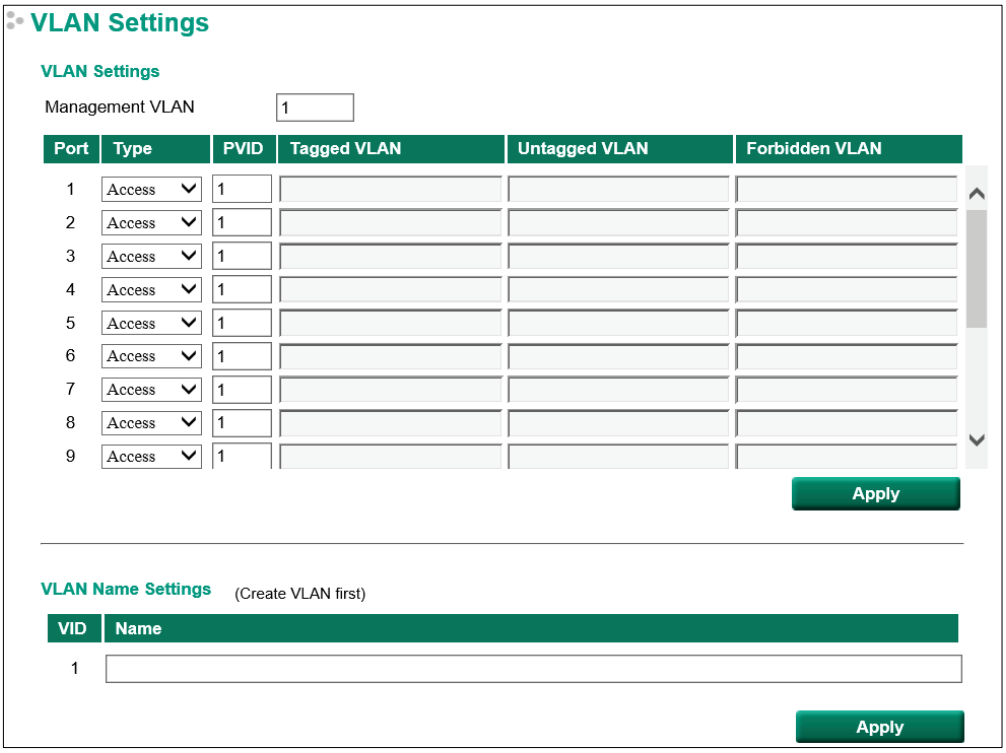
VLAN Settings

Click the VLAN Edit button to open the VLAN Settings page. VLANs are used to increase the efficiency of your network by dividing the LAN into logical segments, as opposed to physical segments.

NOTE

See **Appendix B** for more information about the Virtual LAN (VLAN) Concept.





Management VLAN ID

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

NOTE

If the smart switch is configured for other VLAN settings, to access the switch itself the PC host must be connected to the same VLAN as the management VLAN of the smart switch.

Port

Setting	Description	Factory Default
Port number	Ready only	N/A

Type

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

PVID

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

Tagged VLAN

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

Untagged VLAN

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

Forbidden VLAN

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

VLAN Name Settings

You may associate a VLAN name with each VLAN ID (VID).

VLAN Name Settings

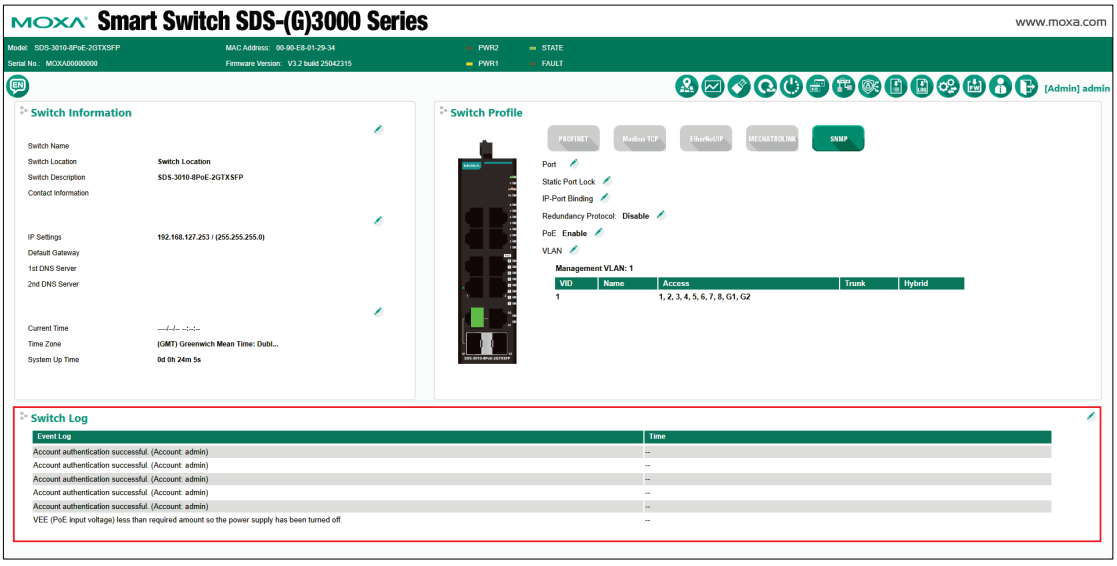
Setting	Description	Factory Default
Name	The VLAN name can only include these characters: a-z/A-Z/0-9/-/_/	None

NOTE

Create the VLAN first, and then assign the VLAN name.

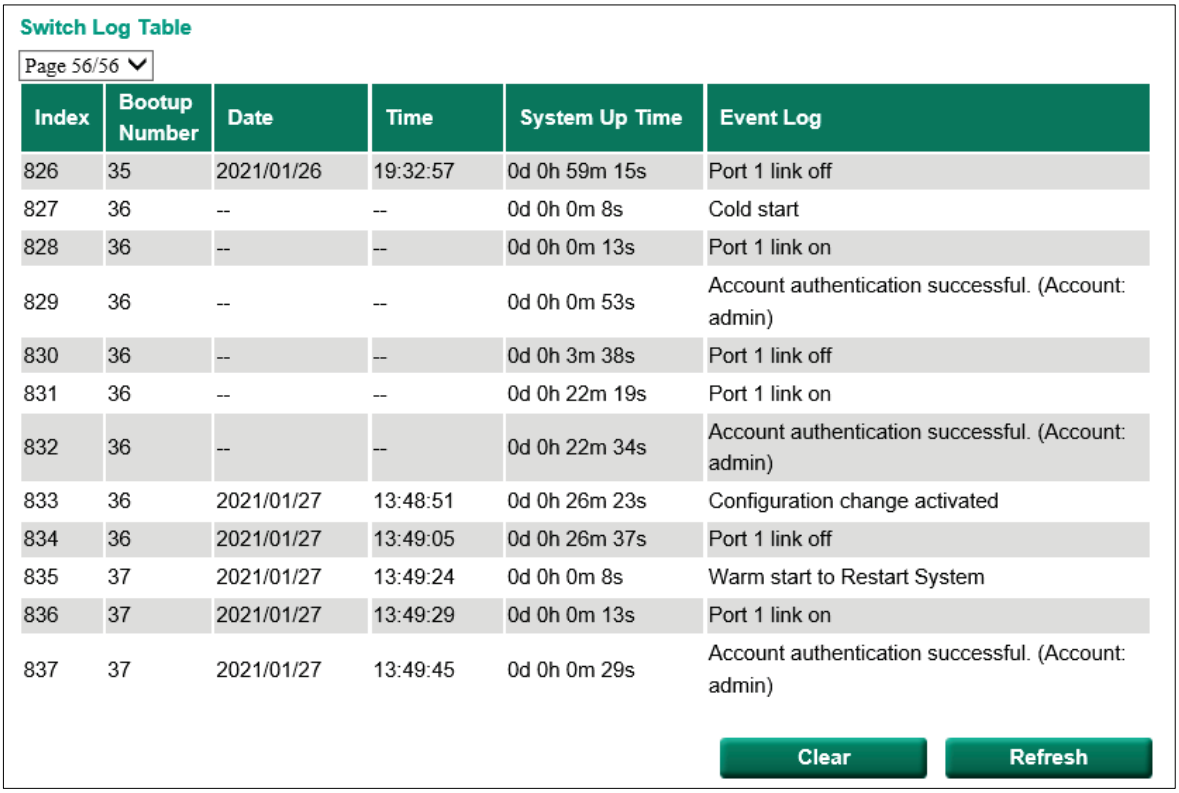
Switch Log

The **Switch Log** at the bottom of the switch's configuration information dashboard shows the latest event log that was recorded. Click the Warning Edit button to check other event logs that have already been recorded, or to set event warning notifications.



Switch Log Table

The smart switch can save up to 1000 event log entries. When the 1000-entry storage limit is reached, the switch will overwrite and delete the oldest saved event log. An example of the Switch Log Table is shown below.

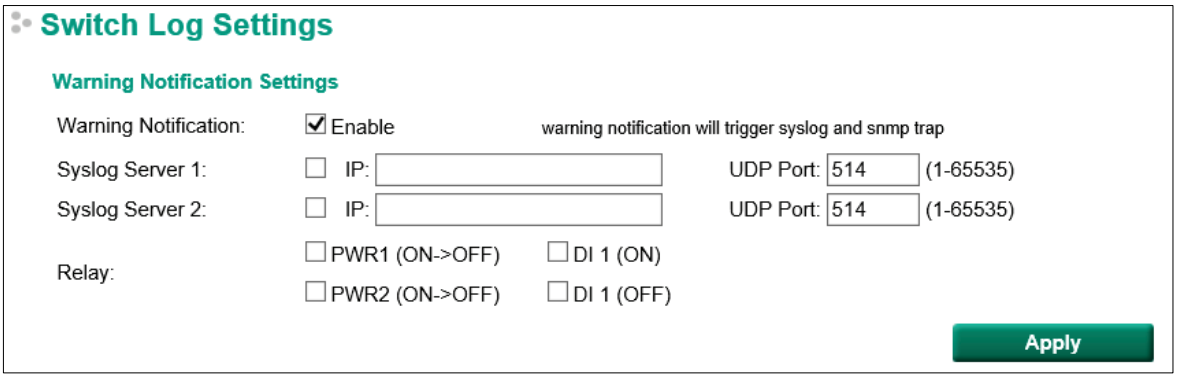


The Switch Log Table displays the following information for each event:

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

Warning Notification Settings

Since industrial Ethernet devices are often located at the endpoints of a system, these devices will not always know what is happening elsewhere on the network. To get around this problem, the industrial Ethernet switches that connect to these devices should be able to send real-time alarm messages to system maintainers. Even when control engineers are out of the control room for an extended period of time, they can still be informed of the status of devices almost instantaneously when exceptions occur. Moxa's smart switches support SNMP trap, syslog, and relay output, and each switch has one digital input for integrating sensors. Click the Switch Log Edit button to view the Switch Log Settings page.



NOTE

Syslog server requires UTF-8 encoding.

A. The STP/RSTP Concept

Spanning Tree Protocol (STP) was designed to help reduce link failures on a network, and provide an automatic means of avoiding loops. This is particularly important for networks that have a complicated architecture, since unintended loops in the network can cause broadcast storms. By default, STP is disabled on all Moxa switches. To work properly, RSTP/STP must be enabled on every Moxa switch connected to your network.

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

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

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

NOTE

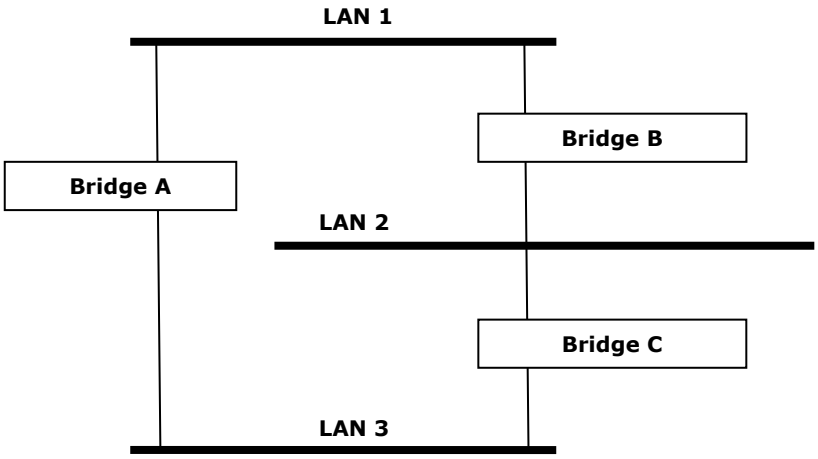
The STP protocol is part of the IEEE Std 802.1D, 2004 Edition bridge specification. The following explanation uses "bridge" instead of "switch."

What is STP?

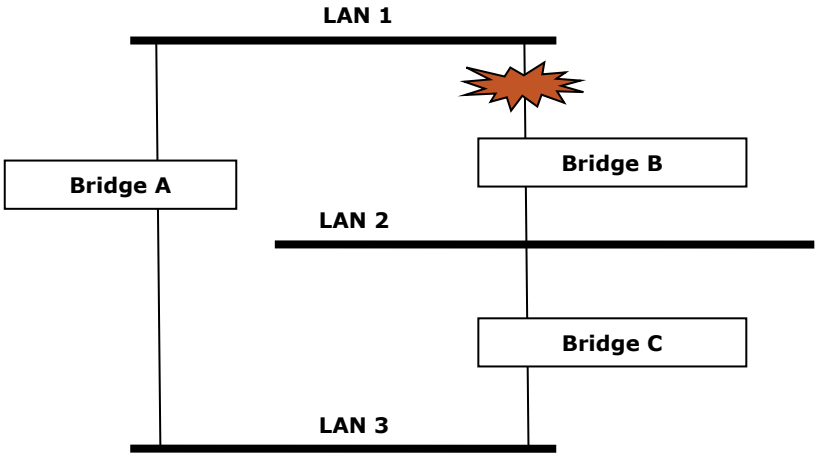
STP (802.1D) is a bridge-based system that is used to implement parallel paths for network traffic. STP uses a loop-detection process to:

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

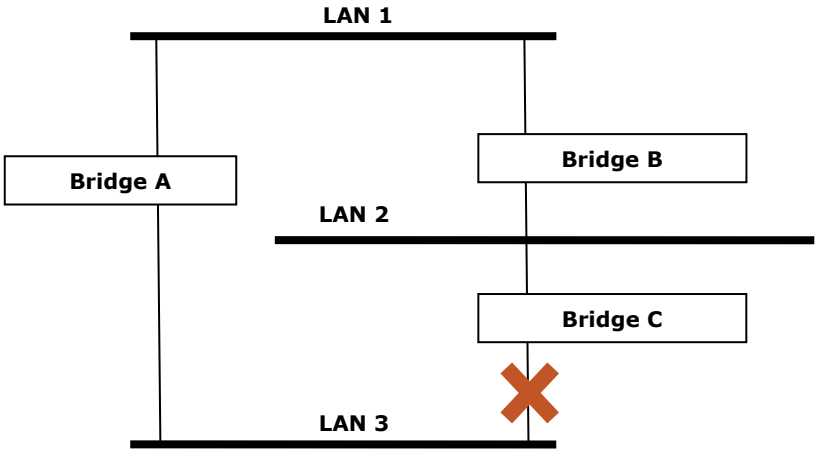
The figure below shows a network made up of three LANs separated by three bridges. Each segment uses at most two paths to communicate with the other segments. Since this configuration can give rise to loops, the network will overload if STP is NOT enabled.



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



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



STP will examine each bridged segment determine which path is most efficient, and then assign a specific reference point on the network. When the most efficient path has been identified, the other paths are blocked. In the previous 3 figures, STP first determined that the path through bridge C was the most efficient, and as a result, blocked the path through bridge B. After the failure of bridge C, STP re-evaluated the situation and opened the path through Bridge B.

How STP Works

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

STP Requirements

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

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

STP Calculation

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

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

STP Configuration

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

STP Reconfiguration

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

Differences between STP 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.

B. The MRP Concept

What is MRP

MRP (Media Redundancy Protocol) is a network protocol based on the IEC 62439-2 standard that allows users to create a redundant ring system. MRP provides redundancy and fault tolerance by creating two logical paths around the ring, allowing network traffic to flow in both directions. This provides an alternate path if one of the devices or links in the primary path fails. With a recovery time of less than 200 ms or 500 ms (depending on settings), it can support up to 50 devices in each ring.

Roles in MRP

MRP supports two roles:

MRM (Media Redundancy Manager):

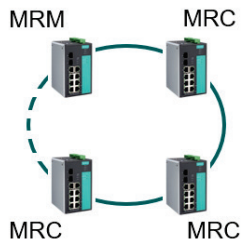
Also known as the Ring Manager, is a node that observes and controls the ring topology in order to react to network faults. There is only one MRM in the network. In the event of a Link Down scenario, the MRM diagnoses the issue and notifies all MRCs (Media Redundancy Clients) to clear their FDB (Filtering Database) and relearn the path. Additionally, the MRM changes the port status of the secondary port from blocking to forwarding to restore connectivity.

MRC (Media Redundancy Client):

Also known as the Ring Client, is a node in the network topology that reacts to received reconfiguration frames from the MRM. An MRC also detects and signals link changes on its ring ports in the event of a Link Down or Link Up situation. When receiving Topology Change frames as requested by the MRM, the MRC will clear its FDB (Filtering Database).

How MRP Works

Implementing MRP requires two ports which should be designated as ring port 1 and ring port 2, respectively. One ring port of the MRM will be connected to a ring port of an MRC. The other ring port of that MRC should be connected to a ring port of another MRC or to the second ring port of the MRM.



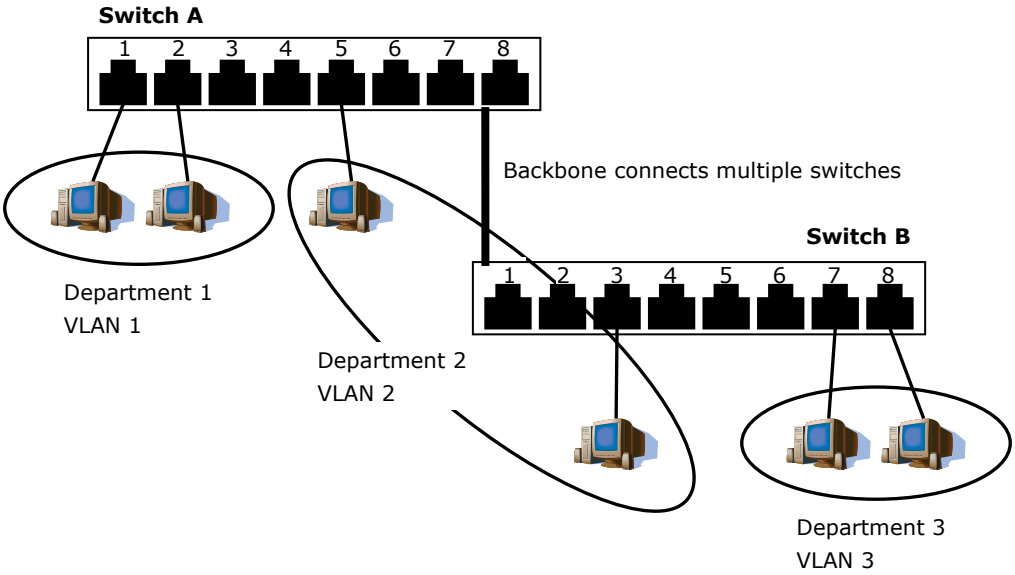
One of the ring ports on MRM will be in a blocking state, while the other port will be in a forwarding state. The path connected to the blocking port is the redundant path. Similarly, MRCs require two ports, both of which would be in a forwarding state.

C. The Virtual LAN (VLAN) Concept

What is a VLAN?

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

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



Benefits of VLANs

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

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

VLANs and the Rackmount switch

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

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

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

Managing a VLAN

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

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

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

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 needs to be installed. Communication between VLANs can only take place if they are all connected to a routing or Layer 3 switching device.

VLANs: Tagged and Untagged Membership

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

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

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

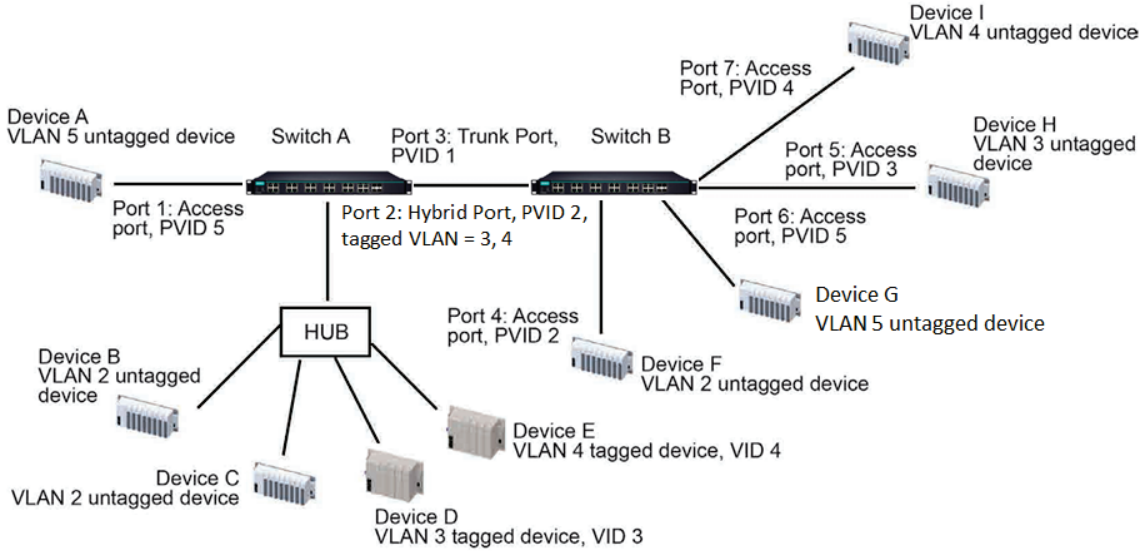
To carry multiple VLANs across a single physical link (backbone, trunk), each packet must be tagged with a VLAN identifier so that the switches can identify which packets belong in which VLAN. To communicate between VLANs, a router must be used.

The Moxa switch supports three types of VLAN port settings:

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

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

Sample Applications of VLANs Using Moxa Switches



In this application:

- Port 1 connects a single untagged device and assigns it to VLAN 5; it should be configured as an **Access Port** with PVID 5.
- Port 2 connects a LAN with two untagged devices belonging to VLAN 2. One tagged device with VID 3 and one tagged device with VID 4. It should be configured as a **Hybrid Port** with PVID 2 for untagged 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.

QoS

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

The Traffic Prioritization Concept

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

- Improve network performance by controlling a wide variety of traffic and by managing network congestion.
- Assign priorities to different categories of traffic. For example, set higher priorities for time-critical or business-critical applications.
- Provide predictable throughput for multimedia applications, such as video conferencing or voice over IP, and minimize traffic delay and jitter.
- Improve network performance as the amount of traffic grows.

The main advantages of the above are that it will reduce costs since it will not be necessary to keep adding bandwidth to the network. Traffic prioritization uses the four traffic queues that are present in your Moxa switch to ensure that high priority traffic is forwarded on a different queue from lower priority traffic. Traffic prioritization provides Quality of Service (QoS) for your network. The Moxa switch traffic prioritization depends on two industry-standard methods:

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

IEEE 802.1D Traffic Marking

The IEEE Std 802.1D, 1998 Edition marking scheme, which is an enhancement to IEEE Std 802.1D, enables Quality of Service on the LAN. Traffic service levels are defined in the IEEE 802.1Q 4-byte tag, which is used to carry VLAN identification as well as IEEE 802.1p priority information. The 4-byte tag immediately follows the destination MAC address and Source MAC address.

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

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

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

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

Refer to the table below for default settings of different traffic types in the Moxa Smart Switch.

CoS Value and Priority Queues

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

Differentiated Services (DiffServ) Traffic Marking

DiffServ is a Layer 3 marking scheme that uses the DiffServ Code Point (DSCP) field in the IP header to store the packet priority information. DSCP is an advanced intelligent method of traffic marking that allows you to choose how your network prioritizes different types of traffic. DSCP uses 64 values that map to user-defined service levels, allowing you to establish more control over network traffic. Some of the advantages of DiffServ over IEEE 802.1D are:

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

Refer to the table below for the default settings of different traffic types in Moxa's Smart Switch.

DSCP Value and Priority

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

Traffic Prioritization

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

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

Traffic Queues

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

NOTE

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

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

NOTE

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