Moxa Industrial Smart Ethernet Switch User Manual

Version 3.2, March 2026

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 when using it for the first time. This chapter also provides an overview of the management function icons that are accessible from the switch's web interface.
- **Chapter 3: Management Functions**
  In chapter 3, we explain in detail how to access, configure, and use the various management functions of your Moxa smart switch.

2. Quick Start Guide

The Moxa industrial smart Ethernet switch has a browser-based UI with quick access function buttons to streamline configuration. This chapter will help you set up your Moxa smart switch for first-time use.

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:

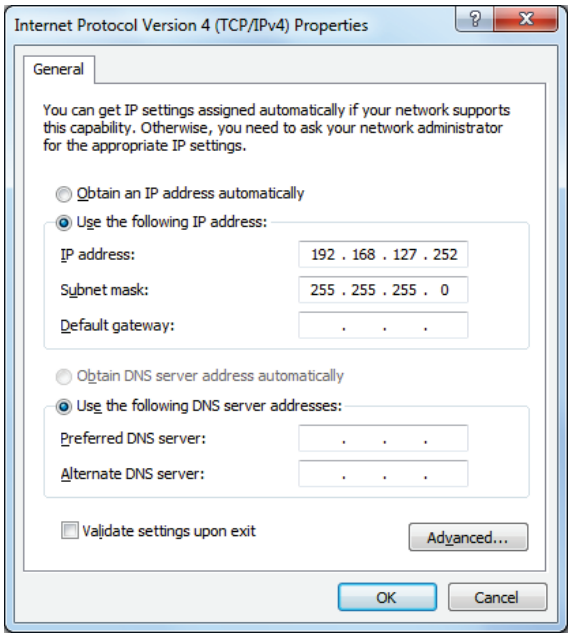
Smart Switch Factory Default Settings

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, both must be connected to the same logical subnet.

For example, to connect a host PC to the switch using the default network settings, open the **Internet Protocol Version 4 (TCP/IPv4) Properties** page, set the subnet mask to 255.255.255.0, and the IP address to 192.168.127.252.



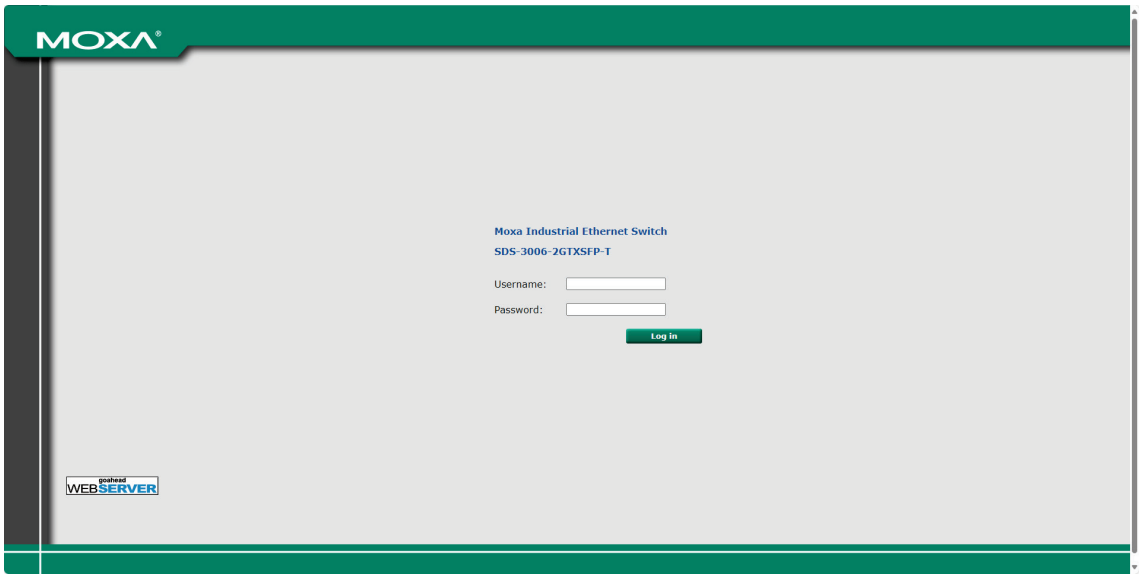
Step 2: Configure the resolution of your computer screen

For best results, set the resolution of your PC's display to 1920 x 1080 pixels.

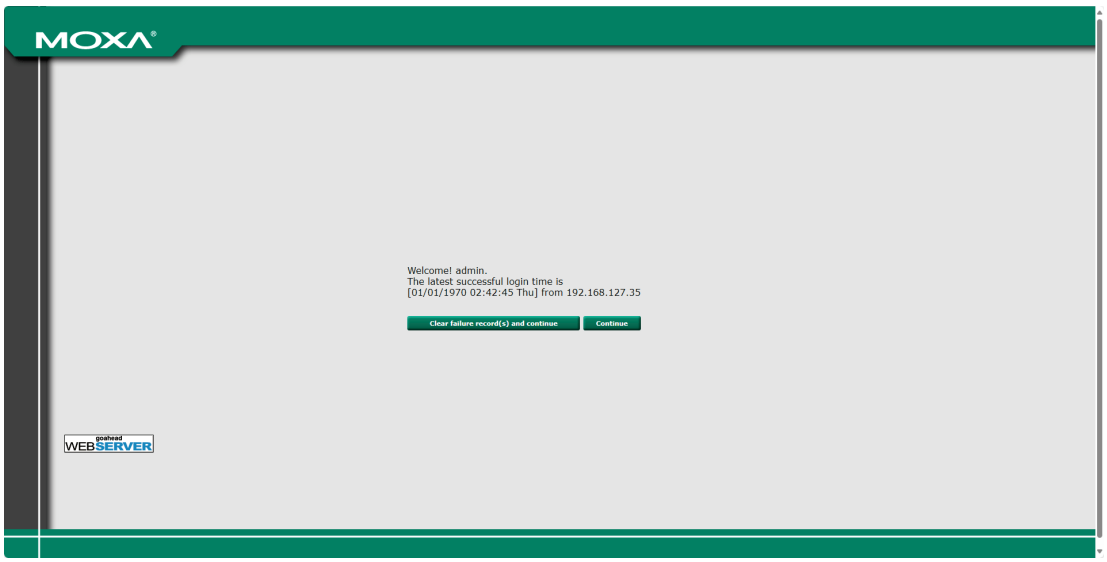
Step 3: Connect to the smart switch's browser-based UI

1. Open your computer's web browser and enter the switch's IP address in the address bar.
   Default IP address: 192.168.127.253

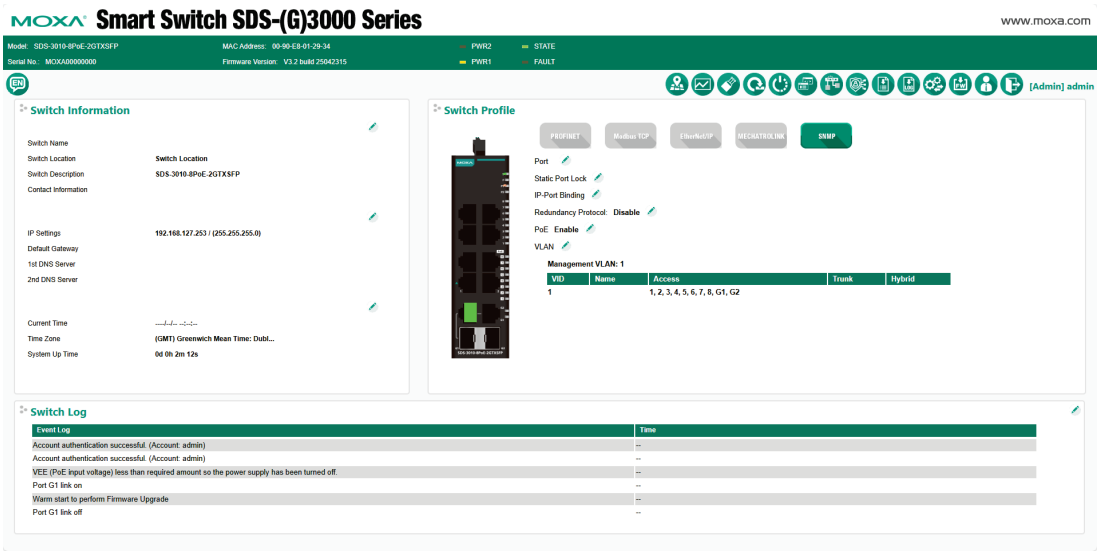
2. When the smart switch's web console opens, enter the username and password, and click **Log In**.
   Default username: admin
   Default Password: moxa



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



4. After logging in, the web console will appear after a few moments.

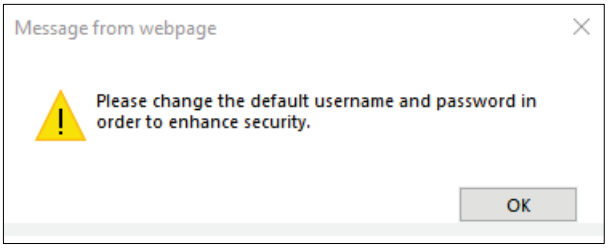


Important Reminders

Change the Default Password

> **IMPORTANT**
>
> For security reasons, we strongly recommend changing the default password of your Moxa smart switch after logging in for the first time.

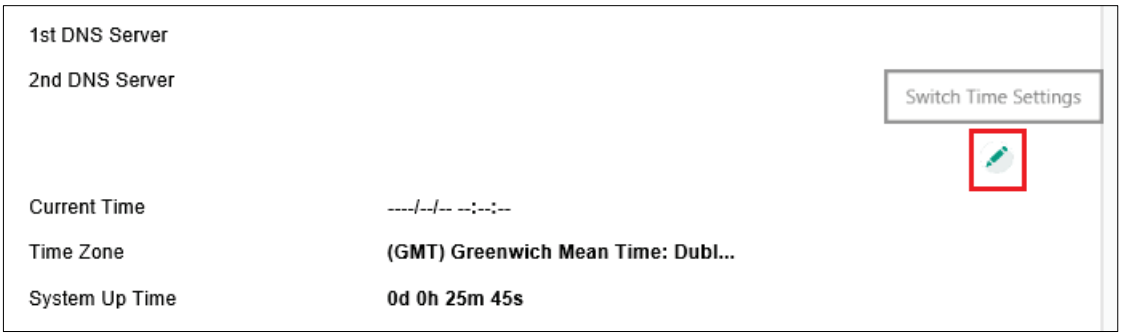
To reduce the chance of malicious actors accessing your device or your network assets, be sure to change the factory default password (moxa) after logging in to the switch for the first time. Until the default password is changed, a reminder message will appear every time you log in.



Refer to **User Account Instructions** for details on how to change the password.

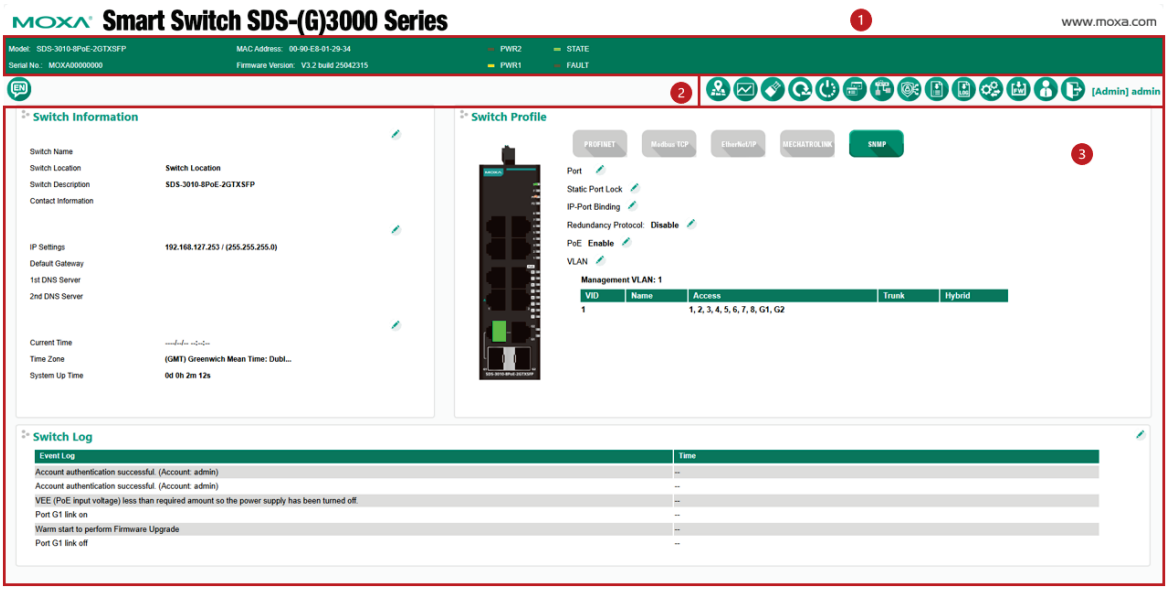
Configure the Device's Date and Time Settings

We recommend updating the device's internal date and time settings when logging in for the first time to ensure the device uses correct date and time stamps for the log and trap functions.



Refer to **Date and Time Information** for details.

UI Dashboard



The dashboard consists of three main sections:

#	Section	Description
1	**Switch Information Bar**	Displays basic switch information, including the model name, MAC address, serial number, and firmware version.
2	**Management Bar**	Contains the function buttons used to perform various management functions. For a detailed explanation of each button, refer to the **Management Bar Icons and Functionality**.
3	**Configuration Panels**	The configuration panels section includes three panels: Switch Information, Switch Profile, and Switch Log. Click the pencil icon to configure settings for the corresponding section. For more details about each function, refer to **Management Functions**.

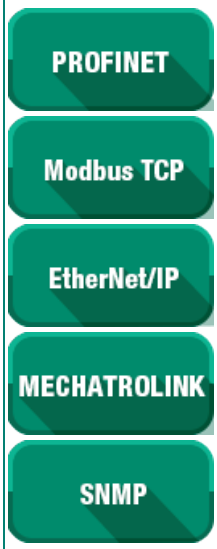
Management Bar Buttons and Functionality

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
	**Language**	Click the **Language** button to select the interface display language. The following languages are supported: 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 clicked, the STATE and FAULT LEDs on the switch will blink green and red, respectively, at a 0.5-second interval for 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 and show fiber parameters including wavelength, temperature, voltage, Tx power, and Rx power. You can also configure the upper and lower bounds of each parameter according to specific application needs. For a detailed explanation of each setting, refer to **Fiber Check Instructions**.
	**Factory Default**	Click the **Factory Default** button to restore the device to its factory default values. When prompted to confirm, click **OK** to reset the switch, or **Cancel** to cancel the action. The device can also be reset using the physical reset button on the top panel of the switch. Refer to the **Quick Installation Guide**, which can be downloaded from the Moxa website.
	**Restart System**	Click the **Restart System** button to perform a warm restart of the switch's operating system. When prompted to confirm, click **OK** to restart the system, or **Cancel** to cancel the action.
	**Management Interface**	Click the **Management Interface** button to configure management interface settings, including TCP ports for various web protocols, concurrent users, and auto-logout settings. These settings help improve network security. For a detailed explanation of each setting, refer to **Management Interface Instructions**.
	**Port Mirror**	Click the **Port Mirror** button to configure port mirroring settings for traffic monitoring and analysis. 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 and keep track of network activity. For a detailed explanation of each setting, refer to **Port Mirror Instructions**. **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.
	**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, refer to **Trusted Access Instructions**. **NOTE:** To avoid being disconnected after enabling this function, make sure to add the current IP subnet to the Trusted Access list first.

Icon	Function	Description
	**SSL Certificate Management**	Click the **SSL Certificate Management** button to import or re-generate the SSL certificate to secure the switch's management interface. For a detailed description of this function, refer to **SSL Certificate Management**.
	**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, refer to **Inventory Report Download**.
	**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 each setting, see the **Log File Backup Instructions** section later in this chapter. **NOTE:** The device can store a maximum of 1000 event log entries. When the limit is reached, the switch will overwrite the oldest 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 each setting, 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**
	**Log Out**	Click the **Log Out** 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.

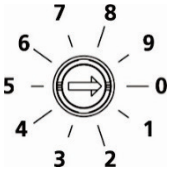
Configuration Panel Icons and Functionality

Icon	Function	Description
	**Edit**	Click the **Edit** button to edit the settings of the corresponding section.
	**Industrial Protocols and SNMP Profiles**	The Moxa smart switch supports the following industrial protocols: PROFINET, EtherNet/IP, Modbus TCP, and MECHATROLINK-4; and the following management protocols: 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. This information can then be processed on a SCADA HMI or NMS system. Click the industrial protocol button to activate or deactivate the corresponding protocol. If the industrial protocol is active, the corresponding protocol button will appear green. If the protocol is inactive, the button will be grayed out. **NOTE:** If you need to integrate the smart switch with an EtherNet/IP network for I/O operations, IGMP Snooping and IGMP Query may be required. Enabling EtherNet/IP will also enable IGMP Snooping and IGMP Query automatically. **NOTE:** When enabling MECHATROLINK, the switch will automatically disable GVRP and LLDP, and apply certain required VLAN configuration settings.

Rotary DIP Switch

The rotary DIP switch located on the bottom panel of the SDS-(G)3000 facilitate one-step configuration by enabling industrial protocol profiles and DHCP client functionality without having to access the web interface.

The rotary DIP switch has ten options that can be selected by turning the arrow dial to point to the specific position. 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 the PROFINET, Modbus, Ethernet/IP, MECHATROLINK-4 profiles, and DHCP clients. Options 8 and 9 are reserved for future use. The device must be rebooted after changing the DIP switch settings for the function to take effect.



NOTE

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

Rotary DIP Switch Settings for IA Profile:

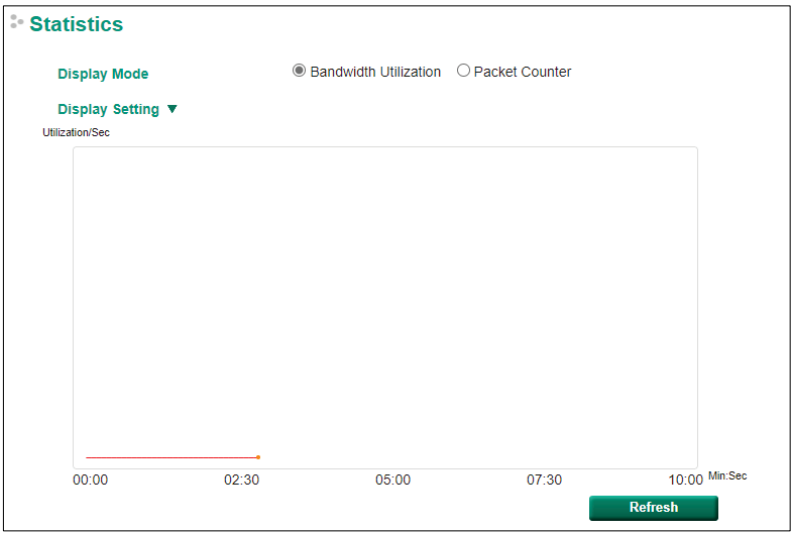
Indicator	Mode
0	No function enabled via DIP switch (default)
1	PROFINET profile enabled
2	PROFINET profile and DHCP Client enabled
3	Ethernet/IP profile enabled
4	Ethernet/IP profile and DHCP Client enabled
5	Modbus TCP profile enabled
6	Modbus TCP profile and DHCP client enabled

Indicator	Mode
7	MECHATROLINK-4 profile enabled
8-9	Reserved (currently performs the same behavior as indicator 0)

Function Button Descriptions

Statistics

This page shows a live graph to monitor the device's traffic and resource usage and traffic. The graph can be customized to show specific information.

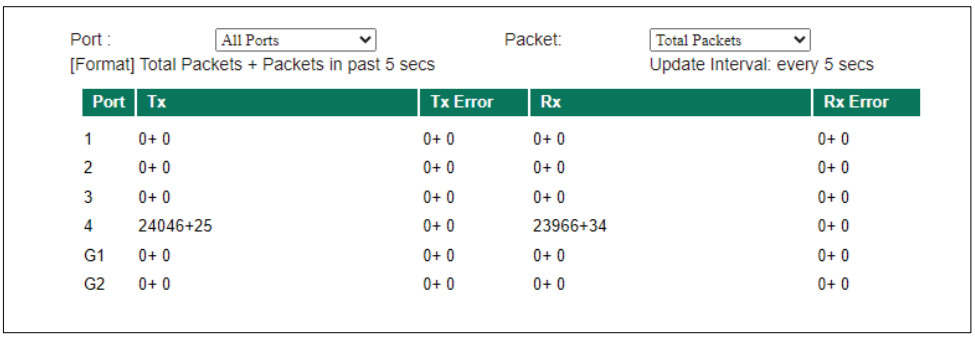


Display Mode

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** section, you can select the ports to include in the statistics graph. In **Sniffer Mode**, you can choose to view the ports' incoming or outgoing packets, or both.

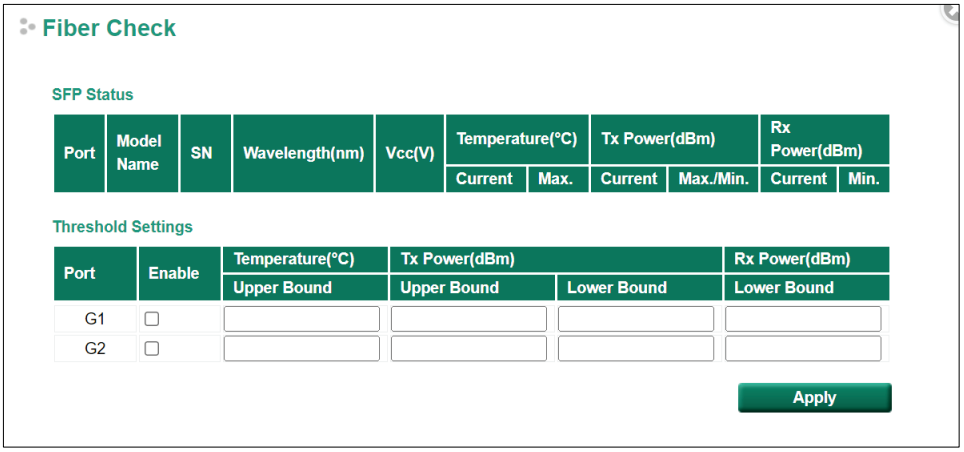


The port table below the statistics graph shows detailed packet information, depending on the selected ports and packet type. Select the packet type to monitor from the **Packet** field. There are four types of packets: **Total Packets**, **TX Packets**, **RX Packets**, and **Error Packets**. TX packets are packets sent out from the

switch, RX packets are packets received from connected devices, and error packets are packets that did not pass the TCP/IP error-checking algorithm. The **Total Packets** option displays the combined number of TX, RX, and error packets.

Fiber Check

Optical fiber is commonly used for long-distance data transmissions, which can make it difficult to troubleshoot cables and transceivers at remote sites. **Fiber Check** makes it easier for users to check fiber modules and connections for issues and will notify administrators if any user-defined performance threshold is exceeded.



SFP Status

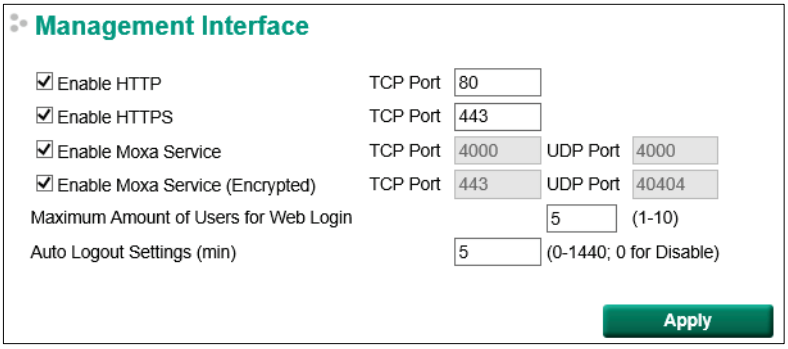
Setting	Description
Port	The port the fiber connection is established on.
Model Name	The name of the Moxa SFP fiber module.
SN	The serial number of the fiber module.
Wavelength (nm)	The wavelength of the fiber connection.
Vcc (V)	The voltage supplied to the fiber connection.
Temperature (°C) – Current	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.
Rx power (dBm) – Min.	The minimum threshold of light being received from the fiber-optic cable.

Threshold Settings

Port	Description
Port	The port the fiber connection is established on.
Enable	Check to enable fiber performance thresholds for the corresponding port. If performance drops below or exceeds the user-specified threshold, the administrator will be notified.
Temperature (°C) – Upper Bound	Specify the maximum temperature threshold for the fiber connection.
Tx Power(dBm) – Upper Bound	Specify the maximum threshold of light being transmitted through 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

This page lets you configure management interface protocols, port numbers, and login options.



Enable HTTP

Setting	Description	Factory Default
Checkbox	Enable or disable HTTP.	Enabled TCP Port: 80

Enable HTTPS

Setting	Description	Factory Default
Checkbox	Enable or disable HTTPS.	Enabled TCP Port: 443

Enable Moxa Service

Setting	Description	Factory Default
Checkbox	Enable or disable the Moxa Service. **NOTE:** Moxa Service only applies to the Moxa network management software suite.	Enabled TCP Port: 4000 UDP Port: 4000

Enable Moxa Service (Encrypted)

Setting	Description	Factory Default
Checkbox	Enable or disable Moxa Service (Encrypted). **NOTE:** Moxa Service (Encrypted) only applies to the Moxa network management software suite.	Enabled TCP Port: 443 UDP Port: 40404

Maximum Number of Users for Web Login

Setting	Description	Factory Default
1 to 10	Specify the maximum number of concurrent users allowed to log in to the web interface at any time.	5

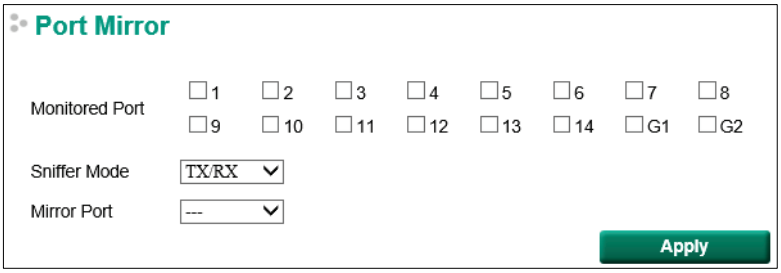
Auto Logout Setting (min)

Setting	Description	Factory Default
0 to 1440	Specify the duration (in min) a user can be inactive before being automatically logged out. If set to 0, this function will be disabled.	5

Port Mirror

This page lets you configure the port mirror function, which is used to monitor data transmitted through a specific port. This is done by setting up another port (the mirror port) to receive the same data being transmitted from, or both to and from, the port under observation.

Using a mirror port allows the network administrator to sniff the observed port to keep tabs on network activity.

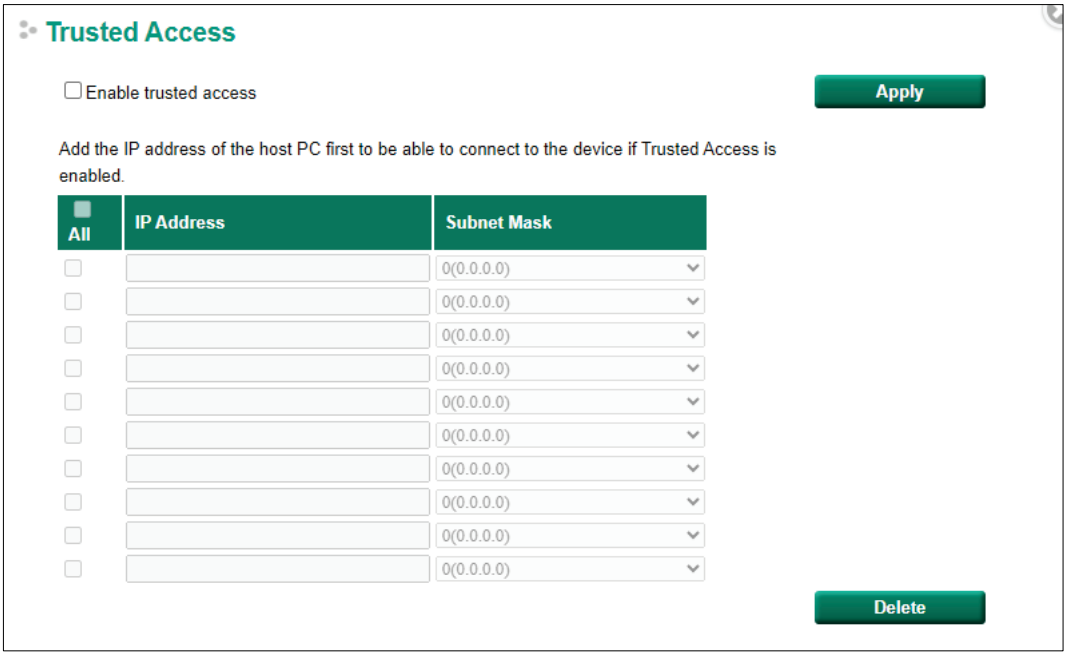


Port Mirror

Setting	Description
Monitored Port	Select the port(s) to monitor.
Sniffer Mode	Select the traffic direction to monitor: • **RX:** Only monitor data packets coming into the Moxa switch's port. • **TX:** Only monitor data packets being sent out through the Moxa switch's port. • **TX/RX:** Monitor both incoming and outgoing data packets.
Mirror Port	Select the port that will monitor the activity of the monitored port.

Trusted Access

This page lets you limit access to the device to trusted IP addresses you specify.



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 the Moxa switch. Each IP address and subnet mask 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 host's IP and subnet are already added to the Trusted Access list before enabling this function. If not, the connection will be terminated once Trusted Access is enabled and you may not be able to access the switch anymore.

Enable trusted access

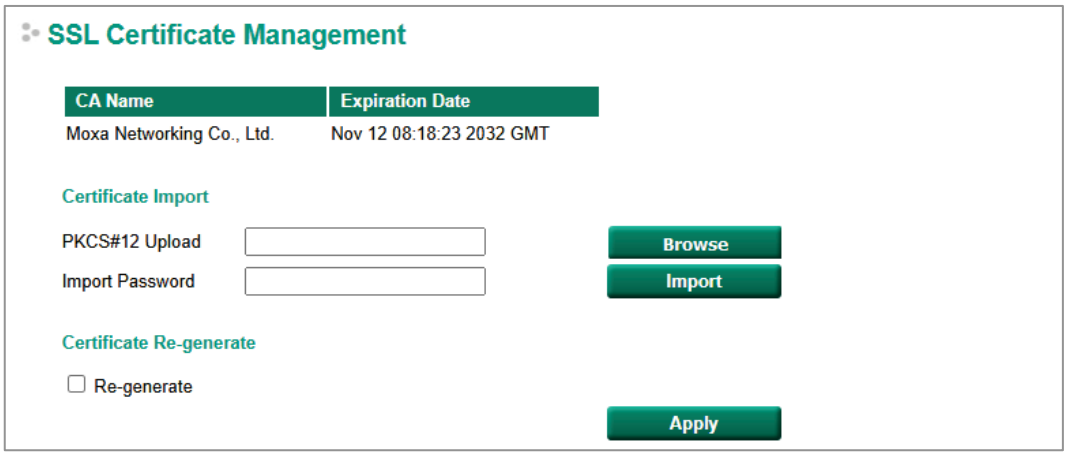
Setting	Description	Factory Default
Checkbox	Enable or disable trusted access. If enabled, only trusted IP addresses added to the table can access the device.	Disabled

To add an entry, enter the IP address and select the subnet mask.

To delete an entry, check the box of the entry or entries you want to remove and click **Delete**.

SSL Certificate Management Instructions

This page lets you import an SSL certificate or re-generate the current certificate.

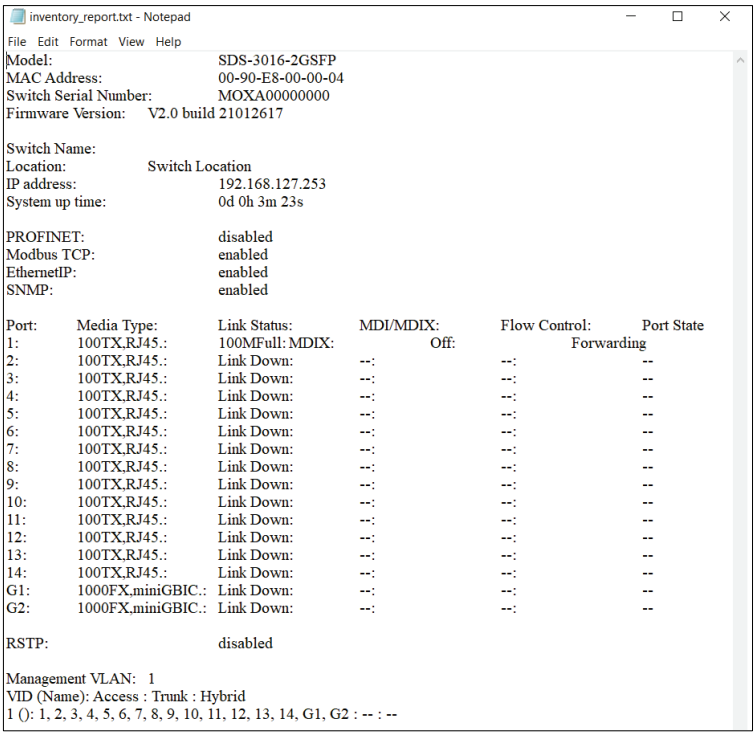


To import a certificate, click **Browse** and navigate to the certificate file (in .p12 format). Enter the import password and click **Import** to upload the certificate.

To re-generate the certificate, check the **Re-generate** checkbox and click **Apply**.

Inventory Report Download

This function lets you export the inventory report containing factory and switch information in text-file format. The file will be saved using the following filename format:
[Switch Name]_inventory_report.txt.

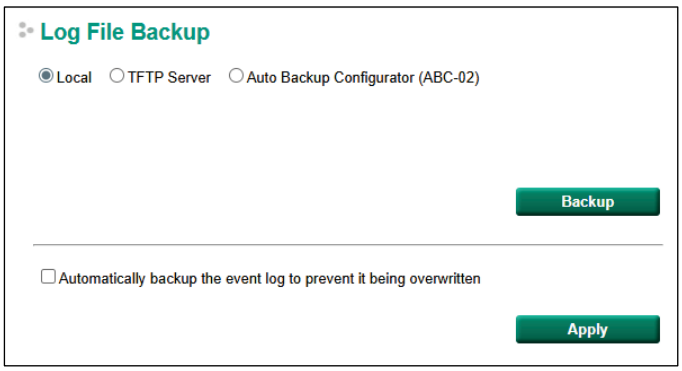


Log File Backup

This page lets you back up log files to either local storage, a TFTP server, or an ABC Series backup configurator tool. You can also enable automatic backups for long-term log records.

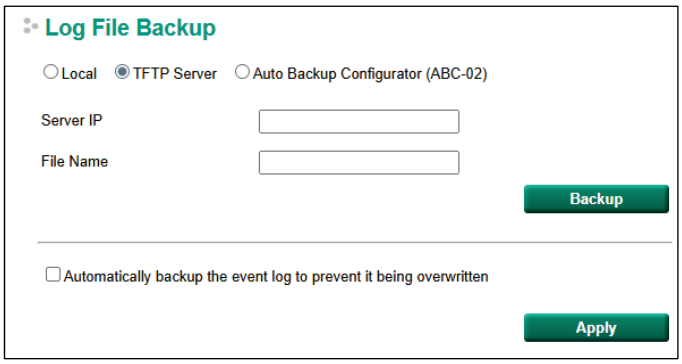
Local

1. Select **Local**.
2. Click **Backup** to save the log file to the local storage.



TFTP Server

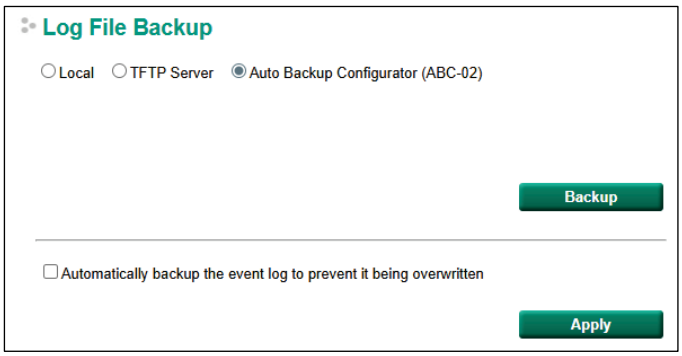
1. Select **TFTP Server**.
2. Enter the TFTP server IP address and log filename.
3. Click **Backup** to save the log file to the TFTP server using the specified filename.



Auto Backup Configurator (ABC-02)

This requires an ABC-02 Series backup configurator tool to be attached to the device.

1. Select **Auto Backup Configurator (ABC-02)**.
2. Click Backup to save the log file to the ABC-02 device.



Log File Backup Method

Setting	Description	Factory Default
Local	Save the log file to the local storage on the host. Click the **Backup** button to back up the log file.	Local
TFTP Server	Save the log file to a TFTP server. Enter the Server IP and File Name, then click **Backup** to back up the log file.	
Auto Backup Configurator (ABC-02)	Save the log file to an ABC-02 Series auto backup configurator tool. Insert the ABC-02 into the device and click **Backup** to back up the log file. The file will be saved as **Sys.log** in the **Moxa** folder on the ABC-02.	

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 keep a long-term record of the switch's log files. The device supports up to 1000 entries. When the storage limit is reached, the switch will overwrite the oldest 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 overwritten. Enable the **Automatically backup the event log to prevent it being overwritten** option and click **Apply**. When the ABC-02 is plugged into the switch, the last 100 event logs will automatically be saved to the ABC-02 automatically when the number of switch log entries reaches 1000. The log files are stored in the **His_log** folder, using the **MMDDHHmm.log**.filename format. **NOTE:** MM=month, DD=day, HH=hour, mm=minutes, based on the system time.	unchecked

NOTE

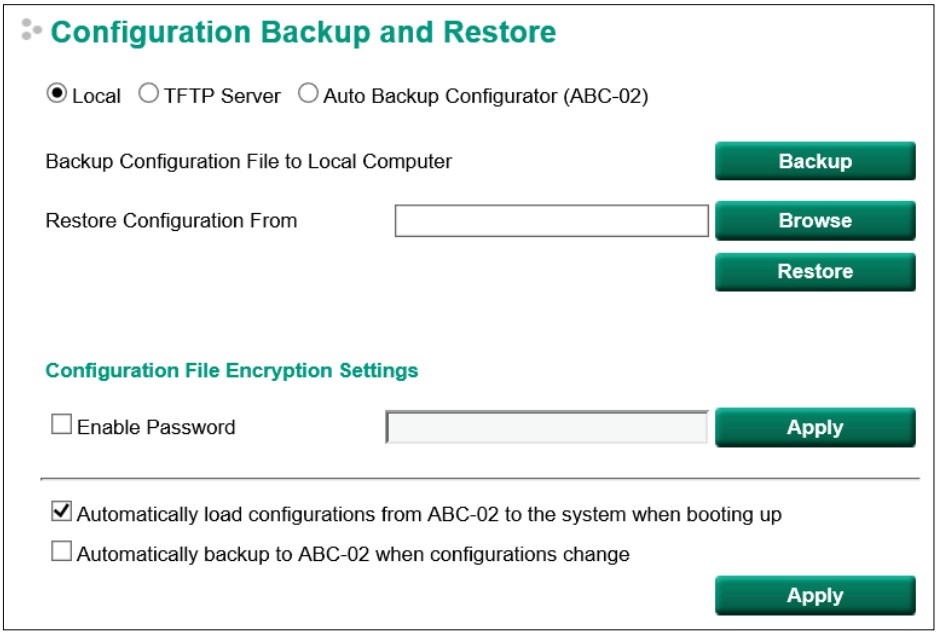
Be sure an ABC-02 backup configurator tool is attached to the Moxa industrial smart Ethernet switch's USB port before activating the function. Press **Apply** to activate the automatic backup function.

The log file includes the following information:

Index	An event index assigned to identify the event sequence.
Bootup Number	This field shows how many times the Moxa switch has been rebooted or cold started.
Date	The date the event was recorded. This timestamp is based on the system time settings.
Time	The time the event was recorded. This timestamp is based on the system time settings.
System Startup Time	The system startup time related to this event.
Event	The description of the recorded event.

Configuration Backup and Restore

This page lets you back up and restore configuration files and configure configuration file encryption settings. With an ABC-02 Series backup configurator tool, configuration files can be automatically loaded during startup, or backed up whenever the configuration is changed.



Configuration Backup and Restore

Setting	Description	Factory Default
Local	1. Click **Backup** to save the configuration file to the local storage on the host. The file will be saved as **Sys.ini**. 2. Click **Browse** to search for the configuration file on the local storage and click **Restore**.	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

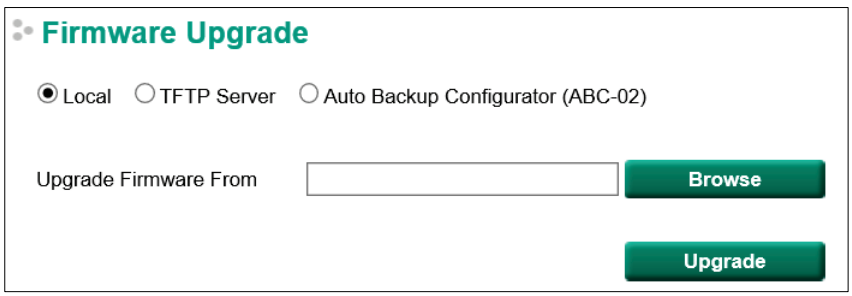
Setting	Description	Factory Default
Automatically load configurations from the ABC-02 to the system when booting up	1. Enable this function by selecting the **Automatically load configurations from ABC-02 to the system when booting up** checkbox and then click **Apply**. 6. Power off your switch first, 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

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).

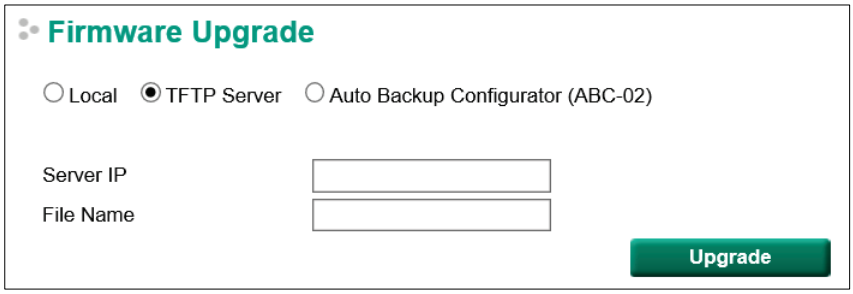
Local

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



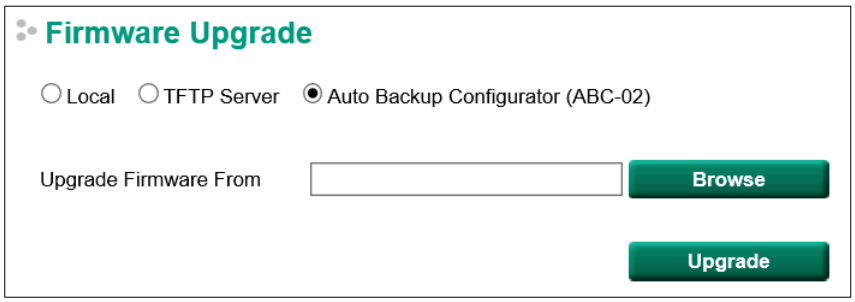
TFTP Server

1. Enter the TFTP server IP address.
2. Enter the firmware filename (*.rom).
3. Click **Upgrade**.



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 **Moxa** folder on the ABC-02. The filename cannot be longer than 8 characters, and the file extension must be .rom.
3. Click **Browse** to locate the (*.rom) file on the ABC-02.
4. Click **Upgrade**.



User Account

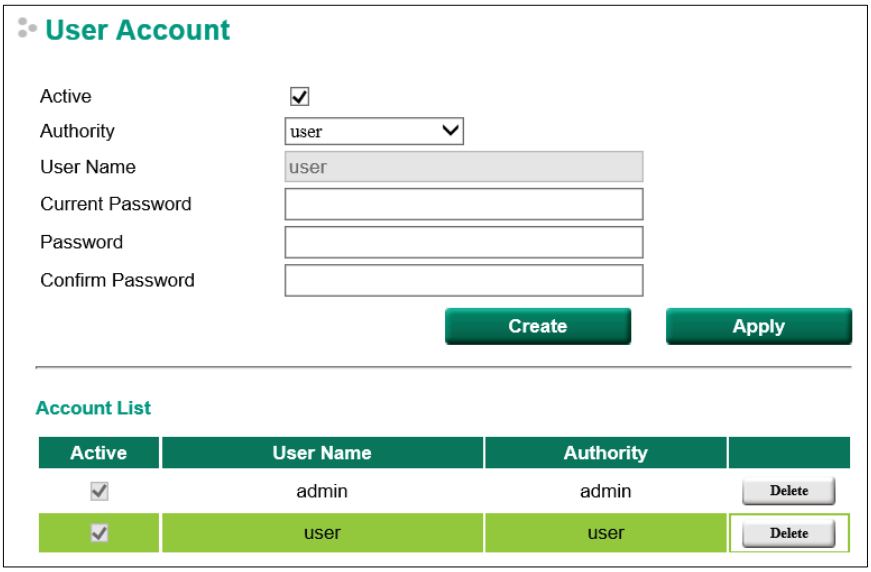
This page lets you manage user accounts. There are two levels of access privileges: **admin** and **user**. Accounts with **admin** privilege have read/write access to all configuration parameters. Accounts with **user** privilege only have read access to configuration pages.

NOTE

In order to maintain a higher level of security, we strongly recommend changing the password after logging in for the first time.

NOTE

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.



Creating a New Account

NOTE

You can create up to a maximum of 10 accounts.

To create a new user account, enter the account details and click **Create**.

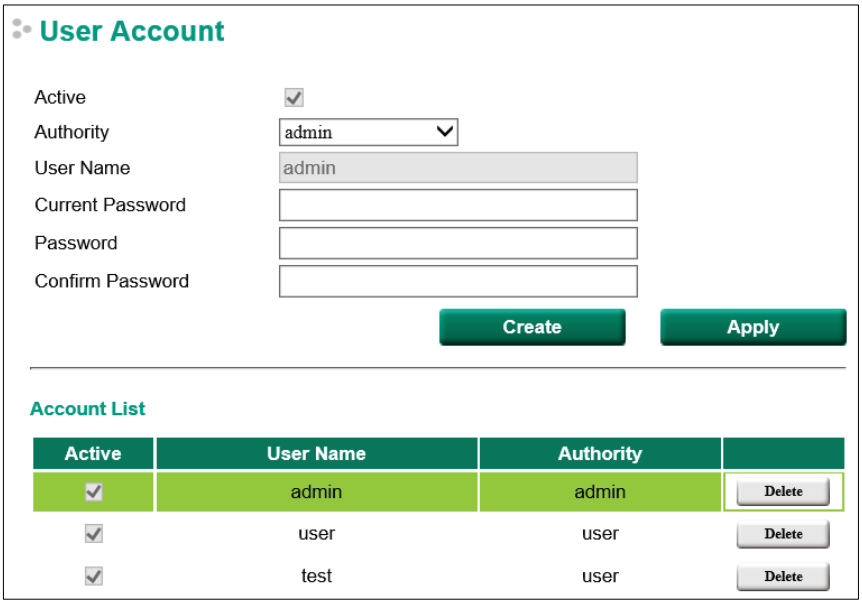
Setting	Description	Factory Default
Active	Check to activate the account. Uncheck the checkbox to deactivate the account.	Enabled
Authority	Select the access privilege for the account. **Admin**: Full read/write access to all configuration pages. **User**: Read-only access to configuration pages.	admin
User Name	Enter the username for the account (max. 30 characters).	None
Password	Enter the password for the user account (4 to 16 characters)	None
Confirm Password	Enter the password for confirmation.	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.

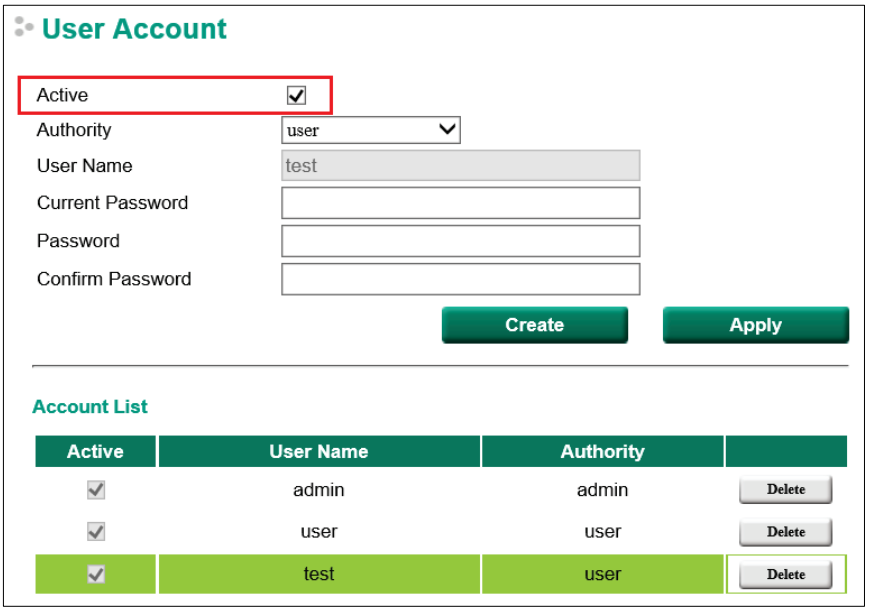
Modifying an Existing Account

To modify an existing account, select the username from the Account List and modify the account details. Click **Apply** to save the changes.



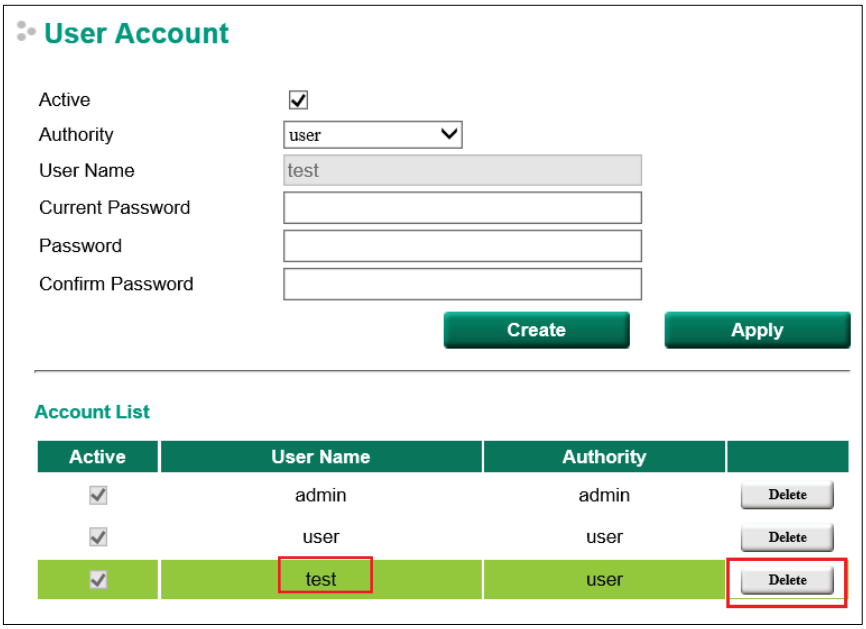
Activate or Deactivate an Existing Account

To activate or deactivate a user account, select the account from the Account List table and check or uncheck the **Active** check box. Click **Apply** to save the changes.

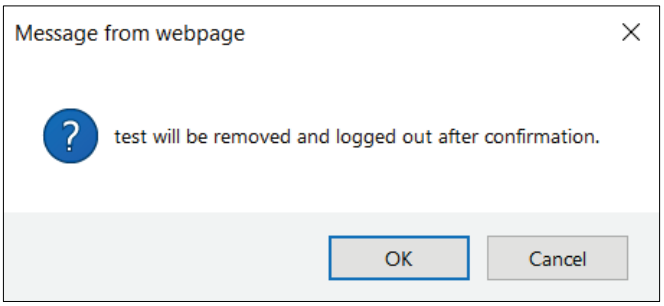


Deleting an Existing Account

To delete an account, click **Delete** for the account you want to delete.



When prompted to confirm, click **OK** to delete the account.



3. Management Functions

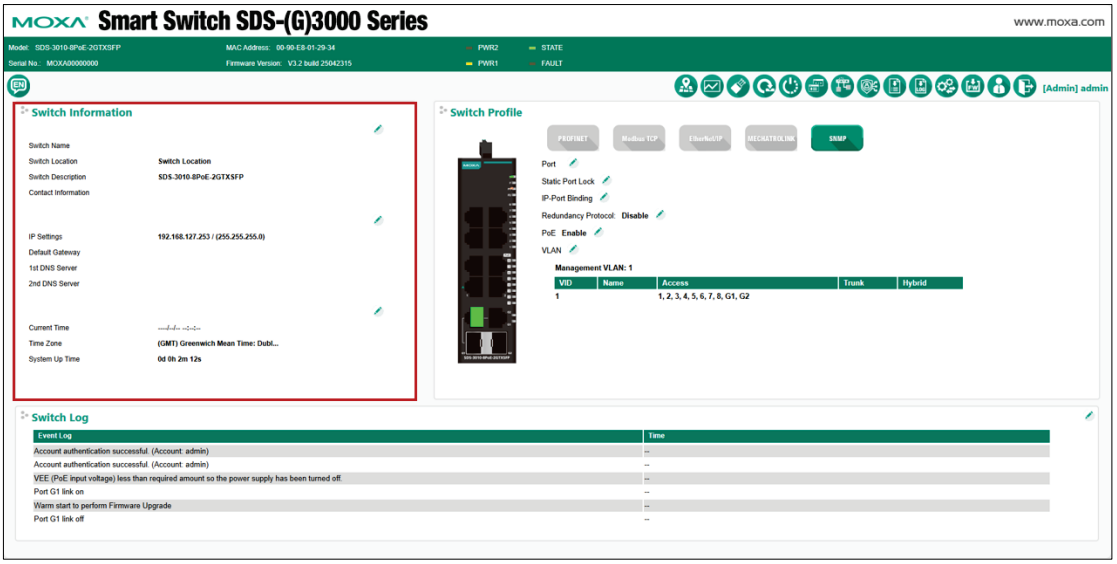
In this chapter, we explain in detail the management functions supported by Moxa's industrial smart Ethernet switch. The configuration and operating results are summarized on the switch's configuration information dashboard for quick reference. You can also use the "edit" icon to edit and adjust the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

Switch Information

The Switch Information panel shows basic device, network information, and time information about the device. Each section can be further configured. Refer to the following sections:

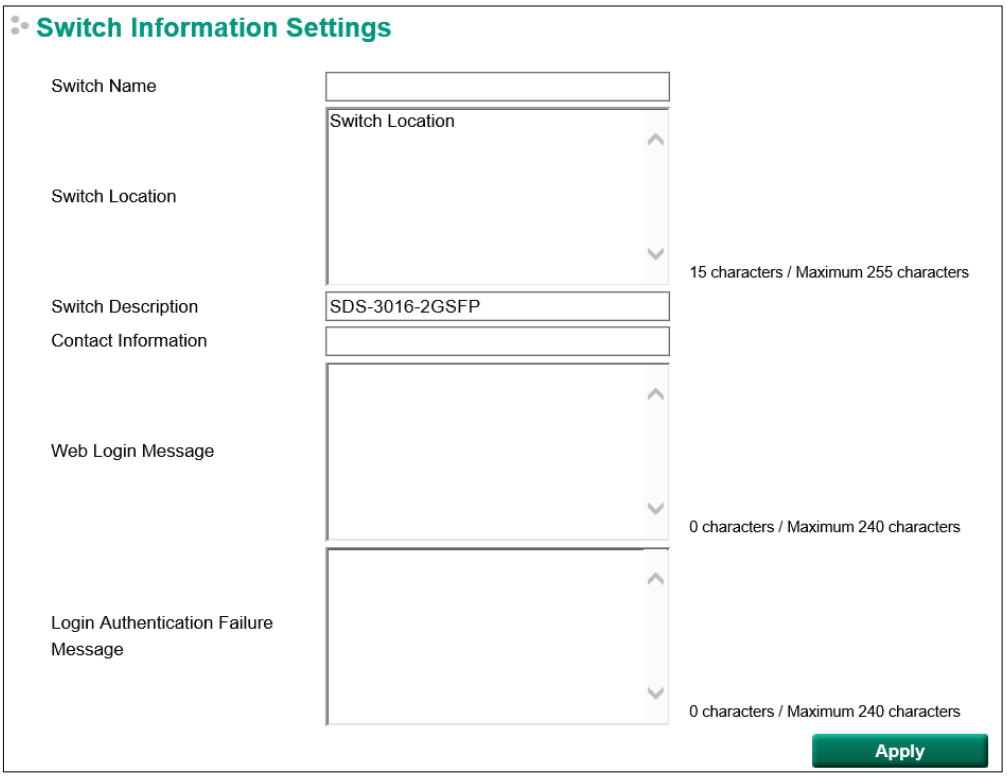
1. System Information Settings
2. Switch Network Settings
3. Switch Time Settings

Click the **Edit** ( ) button of each section to configure relevant settings.



System Information Settings

To access this page, click the **Edit** ( ) button for the switch information section. From this page, you can edit basic device information including the switch name, location, login message.



Switch Name

Setting	Description	Factory Default
Max. 35 characters	This option is useful for differentiating between the roles or applications of different units. The switch name cannot contain spaces. Example: FactorySwitch1.	none

NOTE

As of firmware v3.3, the PROFINET device name is decoupled from the switch name. The PROFINET device name can be configured via compatible engineering deployment software such as SIMATIC STEP 7.

When upgrading from firmware v3.2 to v3.3, the Switch Name and the Device name will remain the same. When downgrading from firmware v3.3 to v3.2, the switch name must be reconfigured on the device.

Switch Location

Setting	Description	Factory Default
Max. 255 characters	Enter the location of the device. This is useful for easily identifying the physical location of different switches. Example: Production line 1.	Switch Location

Switch Description

Setting	Description	Factory Default
Max. 30 characters	Add a description for the device.	Switch Model Name

Contact Information

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

Web Login Message

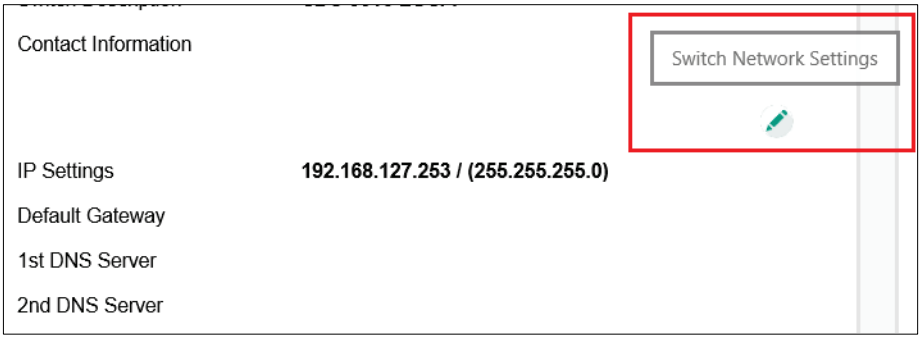
Setting	Description	Factory Default
Max. 240 characters	Enter a login message that will appear when a user successfully logged into the device.	None

Login Authentication Failure Message

Setting	Description	Factory Default
Max. 240 characters	Enter a login failure message that will appear when a user failed to log into the device.	None

Switch Network Settings

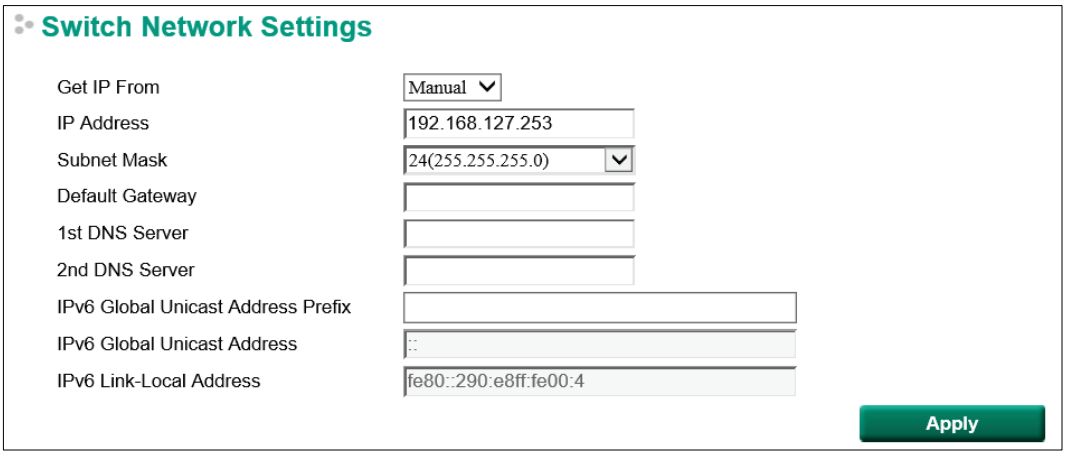
To access this page, click the **Edit** ( ) button for the IP settings section. From this page, you can edit the switch's basic network information.



The switch supports both IPv4 and IPv6. The switch can be managed through either of these address types.

The IPv4 settings cover the switch's IP address, subnet mask, default gateway address, and DNS servers.

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 switch is configured with specific 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	Specify a static IP address for the switch.	Manual
DHCP	Automatically assign the device's IP address and relevant network settings via the network's DHCP server.	
BOOTP	Automatically assign the device's IP address and relevant network settings via the network's BOOTP server.	

IP Address

Setting	Description	Factory Default
IP address	Specify the IP address of the switch. If the device is in DHCP or BOOTP mode, this is automatically assigned.	192.168.127.253

Subnet Mask

Setting	Description	Factory Default
Subnet mask	Select the subnet mask of the switch. This identifies the type of network the 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). If the device is in DHCP or BOOTP mode, this is automatically assigned.	24 (255.255.255.0)

Default Gateway

Setting	Description	Factory Default
IP address for gateway	Specify the 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	Specify the IP address of the DNS server used by your network. If configured, 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. If the device is in DHCP or BOOTP mode, this is automatically assigned.	None
2nd DNS Server	Specify the IP address of the secondary DNS server used by your network. The switch will use the secondary DNS server if the first DNS server fails to connect. If the device is in DHCP or BOOTP mode, this is automatically assigned.	None

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

Setting	Description	Factory Default
Global Unicast Address Prefix	Specify the 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	Shows 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 (the switch's MAC address).	None

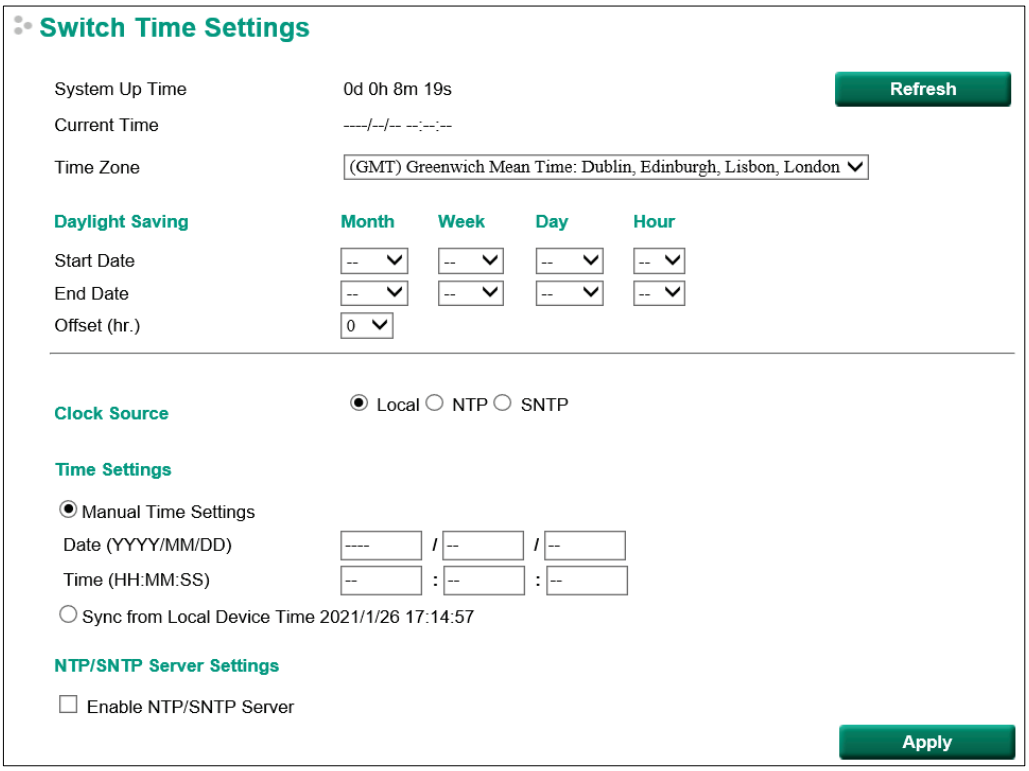
IPv6 Link-Local Address

Setting	Description	Factory Default
None	Shows the IPv6 local-link address. The network portion of the address is FE80 while the host portion of the Link-Local address is automatically generated using the modified EUI-64 form of the interface identifier (the switch's MAC address).	None

Switch Time Settings

To access this page, click the **Edit** ( ) button for the time settings section. From this page, you can edit the time zone, clock source, and system time.

The switch can synchronize its time settings with an NTP/SNTP server, or allows users to manually specify the time and date. Changing these settings will affect any functions that use time stamps, such as logs and SNMP traps.



System Time

System Up Time

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

Current Time

Setting	Description	Factory Default
Date and time	Indicates the current time in yyyy-mm-dd format.	None

Time Zone

Setting	Description	Factory Default
Time zone	Select 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 switch's time offset from national standards.

Start Date

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

End Date

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

Offset

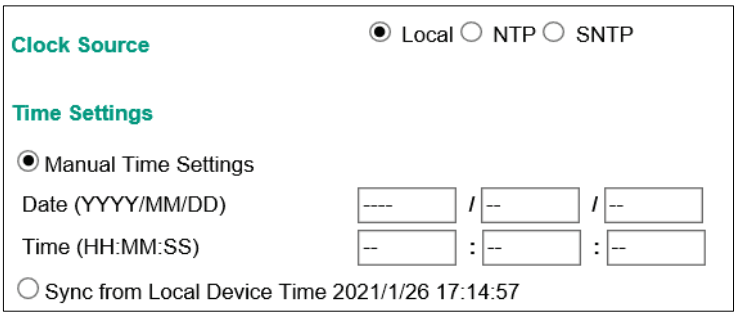
Setting	Description	Factory Default
User-specified hour	Specify the number of hours that the time should be set forward during Daylight Saving Time.	None

Clock Source

Setting	Description	Factory Default
Local	Set the clock source to local. Refer to Clock Source: Local.	Local
NTP	Set the clock source to NTP. Refer to Clock Source: NTP.	
SNTP	Set the clock source to SNTP. Refer to Clock Source: SNTP.	

Clock Source: Local

Select **Local** as the clock source to manually specify the device's time and date.

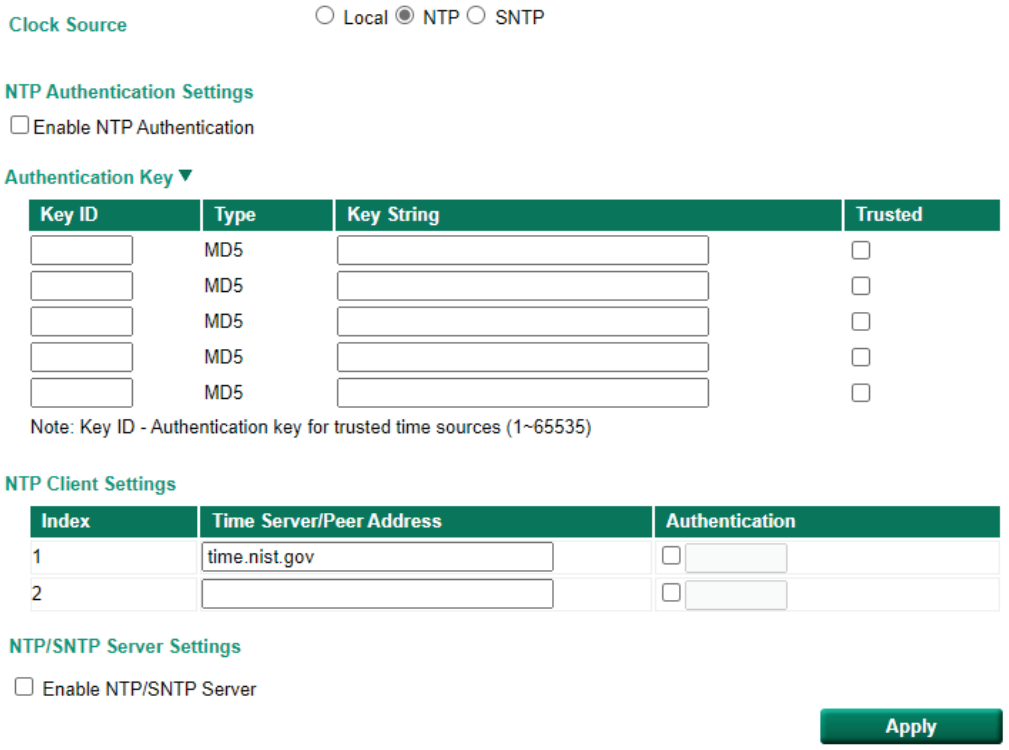


Time Settings

Setting	Description	Factory Default
Manual Time Settings	Manually specify the device time and date.	Manual Time Settings
Sync from Local Device Time	Synchronize the device time with the local time of the connected host used to access the device.	

Clock Source: NTP

The 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
Checkbox	Enable or disable NTP authentication.	Disabled

Authentication Key

You can configure up to five authentication keys. Each key is formatted in MD5 and authorizes the connection between the NTP server and the NTP client.

Key ID

Setting	Description	Factory Default
Key ID	Specify the ID of the authentication key.	None

Key String

Setting	Description	Factory Default
Max. 32 characters	Specify the password of the authentication key.	None

Trusted

Setting	Description	Factory Default
Checkbox	Enable or disable the authentication key.	Disabled

NTP Client Settings

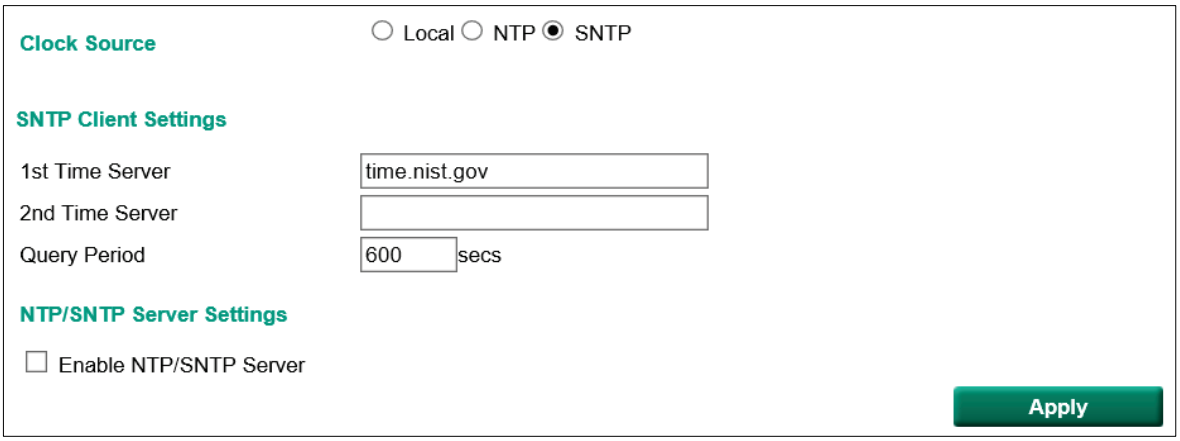
If set to act as an NTP client, NTP server settings must be configured.

Setting	Description	Factory Default
Time Server/Peer Address	Specify the domain of the time server or peer address.	time.nist.gov

Authentication

Setting	Description	Factory Default
Checkbox	Enable or disable NTP authentication.	Disabled
Key ID	Specify the key ID used for authorization.	Null

Clock Source: SNTP



SNTP Client Settings

Setting	Description	Factory Default
IP address or domain name	Specify the IP or domain address of the primary time server (e.g., 192.168.1.1, time.stdtime.gov.tw, or time.nist.gov).	Time.nist.gov
IP address or domain name	Specify the IP or domain address of the secondary time server. The switch will use the secondary SNTP server as a backup if the primary SNTP server is unreachable.	
Query Period	Specify the time interval (in seconds) to sync with the time server.	600

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 switch can act as an NTP server for connected devices.

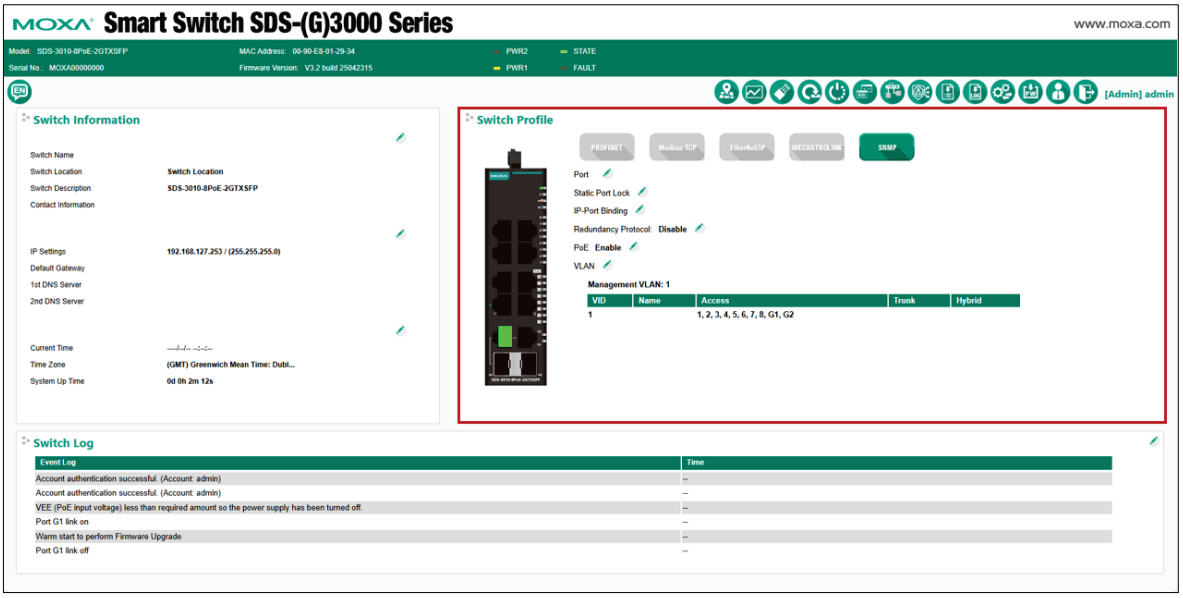
Enable NTP/SNTP Server

Setting	Description	Factory Default
Checkbox	Enables SNTP/NTP server functionality for connected clients.	Disabled

Switch Panel and Profile

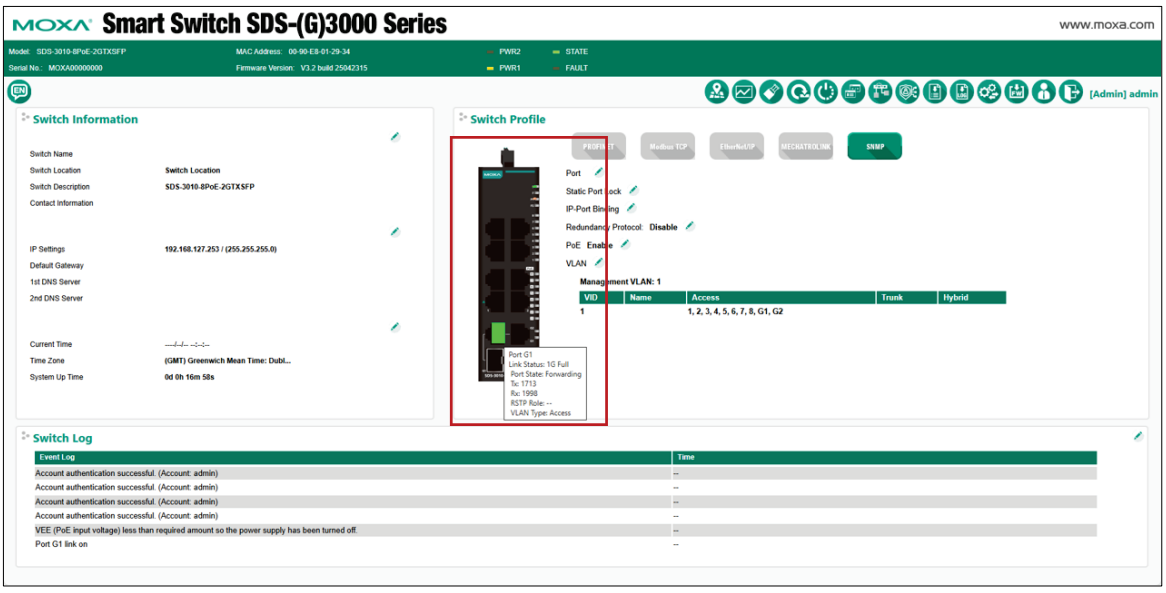
The **Switch Profile** panel is used to configure various switch functions and industrial protocols. The following functions can be configured from this section:

- **Industrial Protocols and SNMP**
- **Port**
- **Static Port Lock**
- **IP-Port Binding**
- **Redundancy Protocol**
- **PoE**
- **VLAN**



Switch Panel and Statistics

The image of the switch's front panel on the dashboard can be used to view the switch's operational information. Hovering the mouse over any port on the switch's panel will show a summary table of the port's current TX/RX statistics.



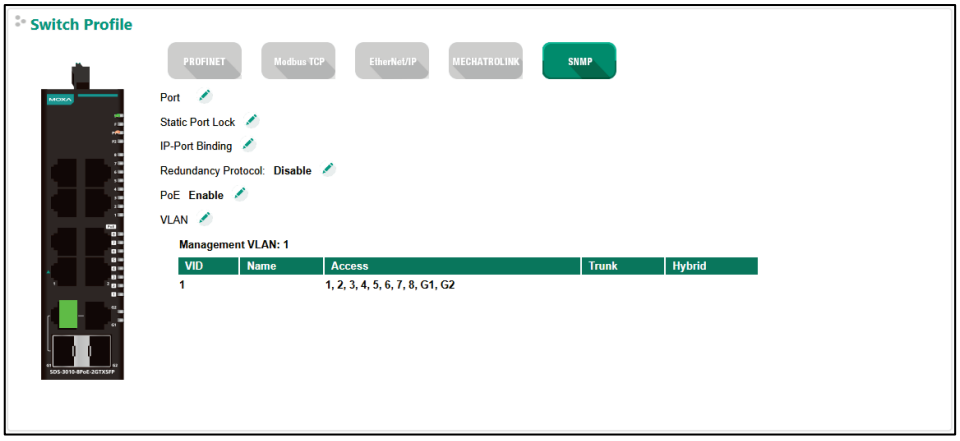
The summary window includes the following information:

Item	Description
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: Disable, Blocking, Listening, Learning, Forwarding
TX	The TX data rate (in packets per second).
RX	The RX data rate (in packets per second).
RSTP Role	The RSTP role of the port: Unknown, Alternate, Root, Designated, Backup
VLAN Type	The port's VLAN type: Access (Default), Trunk, Hybrid
PD Type (PoE models only)	The type of the PD connected to the port: NIC, IEEE 802.3af, IEEE 802.3at, Legacy PoE Device, Unknown
PD Consumption (Watts) (PoE models only)	The power consumption of the PD connected to the port.

Industrial Protocols and SNMP Settings

The switch supports multiple industrial protocols for use in different industrial applications. All protocols are disabled by default and can be enabled by clicking the corresponding protocol profile button. A green button indicates the function is enabled; a grey button means the function is disabled. SNMP will always appear green, even if the function is disabled. The protocol will operate based on the protocol's default settings, which can be modified if needed.

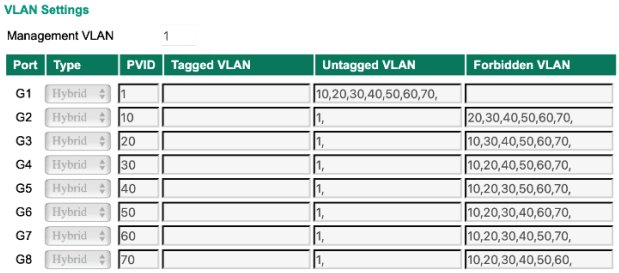
When certain industrial profiles are enabled, functions and parameters may be activated or configured automatically for compatibility reasons. For example, when EtherNet/IP is enabled, the switch will automatically enable IGMP Snooping and IGMP Query to ensure efficient EtherNet/IP data transmissions.



Industrial Protocol and SNMP profiles

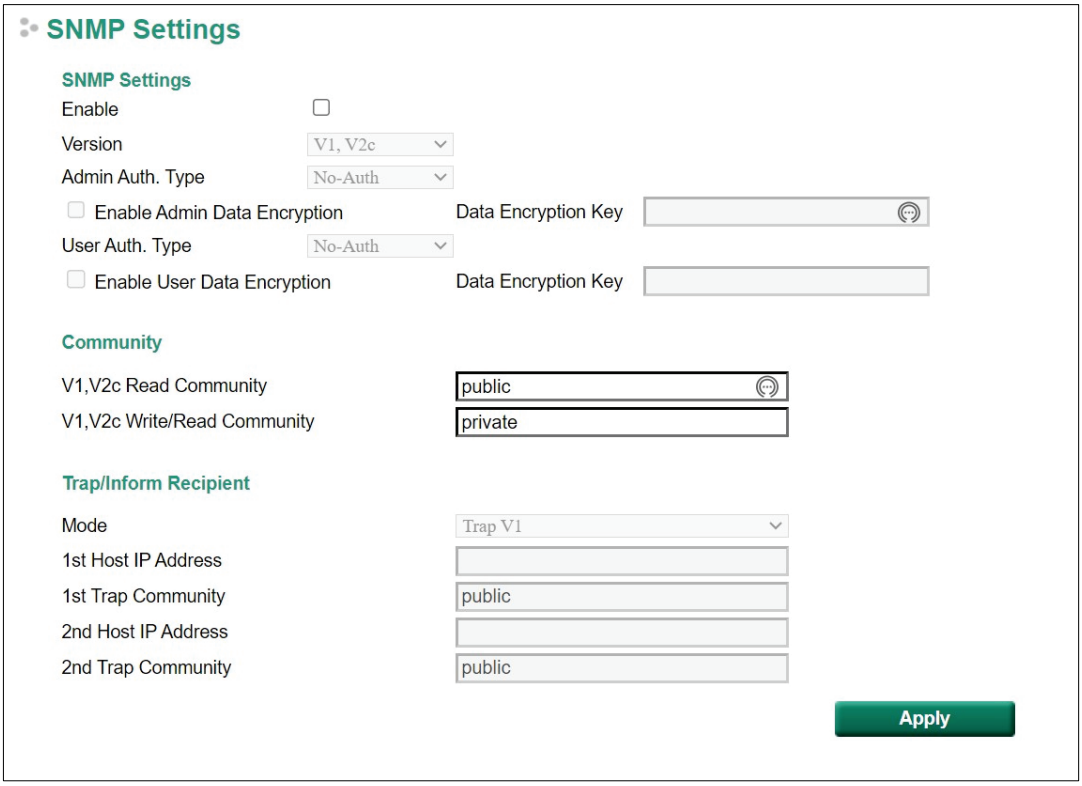
<table>
<tr><th>Setting</th><th>Description</th><th>Factory Default</th></tr>
<tr><td>PROFINET</td><td>
1. Click the PROFINET button to enable the switch to act as a PROFINET I/O device (Conformance Class B). A comprehensive set of PROFINET I/O attributes (sent via cyclic or acyclic I/O data) are available 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 product page on the Moxa website.
2. When PROFINET is enabled, a bundle of PROFINET cyclic I/O data will be periodically sent between the PLC and the switch periodically (default interval = 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>Device</td><td>Input</td><td>0</td><td>0</td><td>Device status</td><td>0: failed
1: OK</td></tr>
<tr><td></td><td></td><td></td><td>1</td><td>Power 1</td><td>0: unavailable
1: OK</td></tr>
<tr><td></td><td></td><td></td><td>2</td><td>Power 2</td><td>0: unavailable
1: OK</td></tr>
<tr><td></td><td></td><td></td><td>3</td><td>RSTP status</td><td>0: disabled
1: enabled</td></tr>
<tr><td>Port</td><td>Input</td><td>1</td><td>0</td><td>Port 1 Connection</td><td>0: not connected
1: connected</td></tr>
<tr><td></td><td></td><td></td><td>1</td><td>Port 2 Connection</td><td></td></tr>
<tr><td></td><td></td><td></td><td>2</td><td>Port 3 Connection</td><td></td></tr>
<tr><td></td><td></td><td></td><td>3</td><td>Port 4 Connection</td><td></td></tr>
<tr><td></td><td></td><td></td><td>4</td><td>Port 5 Connection</td><td></td></tr>
<tr><td></td><td></td><td></td><td>5</td><td>Port 6 Connection</td><td></td></tr>
<tr><td></td><td></td><td></td><td>6</td><td>Port 7 Connection</td><td></td></tr>
<tr><td></td><td></td><td></td><td>7</td><td>Port 8 Connection</td><td></td></tr>
<tr><td>Port</td><td>Input</td><td>2</td><td>0</td><td>Port 9 Connection</td><td>0: not connected
1: connected</td></tr>
<tr><td></td><td></td><td></td><td>1</td><td>Port 10 Connection</td><td></td></tr>
<tr><td></td><td></td><td></td><td>2</td><td>Port 11 Connection</td><td></td></tr>
<tr><td></td><td></td><td></td><td>3</td><td>Port 12 Connection</td><td></td></tr>
<tr><td></td><td></td><td></td><td>4</td><td>Port 13 Connection</td><td></td></tr>
<tr><td></td><td></td><td></td><td>5</td><td>Port 14 Connection</td><td></td></tr>
<tr><td></td><td></td><td></td><td>6</td><td>Port 15 Connection</td><td></td></tr>
<tr><td></td><td></td><td></td><td>7</td><td>Port 16 Connection</td><td></td></tr>
</table>
3. The 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. You can use the SIMATIC STEP 7 tool or engineering deployment software to edit the parameters and set up the alarm. For details about the switch's support for PROFINET and a list of supported PROFINET I/O parameters, refer to the Moxa Industrial Protocols User's Guide which can be downloaded from the product page on the Moxa website.
4. When PROFINET is enabled, the LLDP chassis-id will be set to the device name or the system MAC address in the IEC V2.2 LLDP mode and to either SystemIdentification in the IEC V2.3 LLDP mode.
5. When PROFINET is enabled, the LLDP port-id will be set to PortId in IEC V2.2 mode and to PortId.ChassisId in IEC V2.3 mode, where PortId follows the format "port-xyz" with xyz as an integer, and ChassisId is the device name.

NOTE: The transfer frequency of the PROFINET Cyclic I/O data on the 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, which can be used to integrate the 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. 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 switch's support of Modbus TCP and the Modbus TCP data mapping, refer to the Moxa Industrial Protocols User's Guide which can be downloaded from the product page on the Moxa website.	Disabled
EtherNet/IP	1. Click the EtherNet/IP button to enable the switch to act as an Ethernet/IP device (Adapter class). A comprehensive set of objects and corresponding attributes and services (sent via explicit 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 product page on the Moxa website. 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, refer to the Moxa Industrial Protocols User's Guide which can be downloaded from the product page on the Moxa website. **NOTE:** If the EtherNet/IP profile is enabled, the switch will automatically enable IGMP Snooping and IGMP Query.	Disabled
MECHATROLINK-4	1. Click the MECHATROLINK button to enable the 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. As a result, VLAN settings will be unavailable until MECHATROLINK-4 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.	Disabled

<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 open the SNMP configuration screen. For more details about each setting, refer to SNMP Settings.
2. The 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 (MD5 or SHA). SNMP V3 also supports data encryption for enhanced data security. Refer to the following table for an overview of supported SNMP security modes and levels.
<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 privileges 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 the HMAC-MD5 or HMAC-SHA algorithm. 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 the HMAC-MD5 or HMAC-SHA algorithm, and data encryption key. In addition to a minimum password length of 8 characters, a data encryption key must be set.</td></tr>
</table>
NOTE: The SNMP V3 username and password are the same as the username and password of device's 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

Enable

Setting	Description	Factory Default
Checkbox	Enable or disable SNMP.	Disabled

SNMP Versions

Setting	Description	Factory Default
V1, V2c, V3 V1, V2c V3 only	Select the SNMP protocol version.	V1, V2c

V1, V2c Read Community

Setting	Description	Factory Default
Max. 30 characters	Specify 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 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 algorithm. 8-character passwords are the minimum requirement for authentication.	No
SHA-Auth	Authentication will be based on the HMAC-SHA algorithm. 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
Checkbox	Enable or disable data encryption using the specified data encryption key (between 8 and 30 characters).	Disabled

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

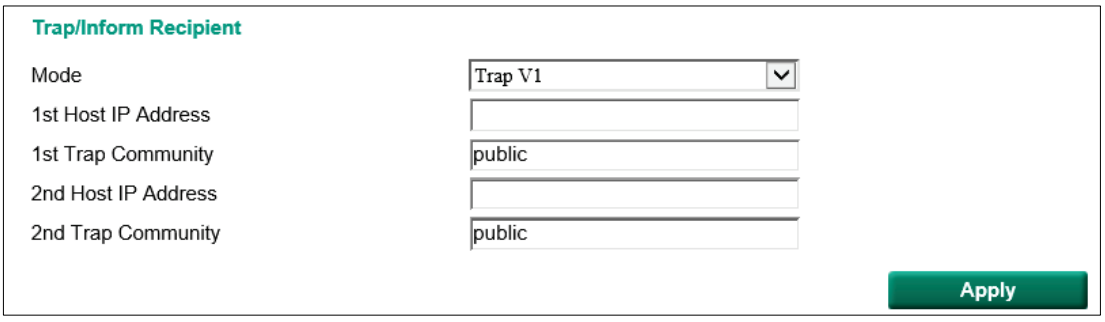
Setting	Description	Factory Default
No-Auth	Allow the admin account and user account to access objects without authentication.	No
MD5-Auth	Authentication will be based on the HMAC-MD5 algorithm. 8-character passwords are the minimum requirement for authentication.	No
SHA-Auth	Authentication will be based on the HMAC-SHA algorithm. 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
Checkbox	Enable or disable data encryption using the specified data encryption key (between 8 and 30 characters).	Disabled

Trap/Inform Settings

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



Mode

Setting	Description	Factory Default
Trap V1	Set the trap mode to Trap V1. In this mode, the SNMP agent sends an SNMPv1 trap PDU to the NMS. No acknowledgment is sent back from the NMS, meaning the agent does not know if the trap reached the NMS.	Trap V1

Setting	Description	Factory Default
Inform V2c	Set the trap mode to Inform V2. In this mode, when an inform message is sent from the SNMP agent to the NMS, the recipient 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 within a specific time frame, the agent will resend the trap to the NMS agent. The maximum timeout threshold is 300 sec (default: 1 sec), and the maximum number of retries is 99 times (default: 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 domain name	Specify the IP address or domain name of the primary trap server used by your network.	None

1st Trap Community

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

Host IP Address 2

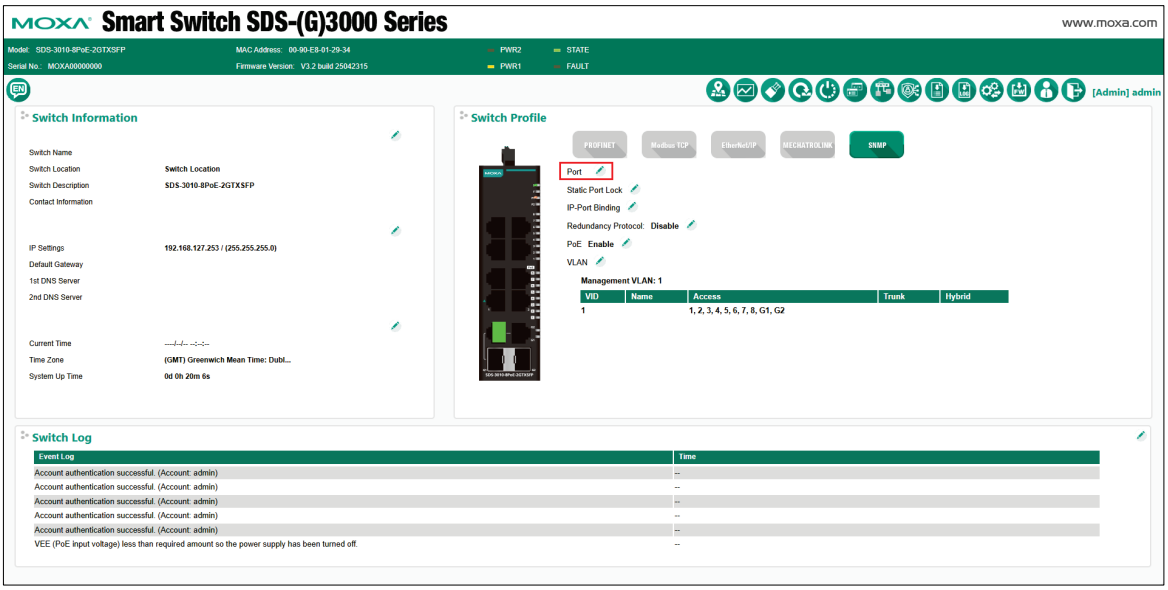
Setting	Description	Factory Default
IP or domain name	Specify the IP address or domain name of the secondary trap server used by your network.	None

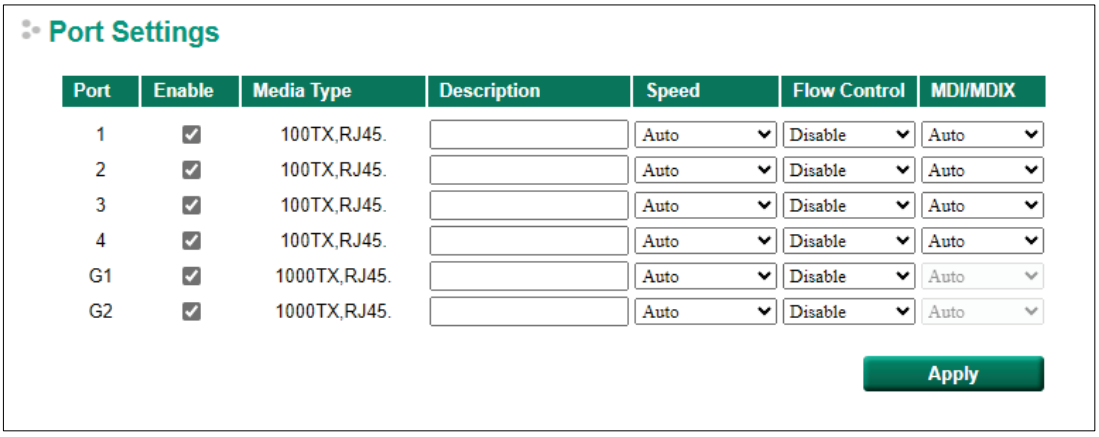
2nd Trap Community

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

Port Settings

To access this page, click the **Edit** ( ) button for **Port**. This page is used to enable or disable ports, and configure related settings including transmission speed, flow control, and port type.





Enable

Setting	Description	Factory Default
Checkbox	Enable or disable the port. Disabling a port will immediately cut off any transmissions.	Enabled

Media Type

Setting	Description	Factory Default
Media type	Shows the media and interface type of the port.	N/A

Description

Setting	Description	Factory Default
Max. 63 characters	Enter 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 auto-negotiate the most suitable transmission speed with the connected device. If the connected device cannot negotiate speed, manually set the port speed.	Auto
100M-Full	Set the port speed to 100 Mbps in full-duplex mode.	
100M-Half	Set the port speed to 100 Mbps in half-duplex mode.	
10M-Full	Set the port speed to 10 Mbps in full-duplex mode.	
10M-Half	Set the port speed to 10 Mbps in half-duplex mode.	
1G-Full	The speed for ports G1 and G2 is fixed at 1 Gbps in full-duplex mode. (for SDS-3016-2GFSP models only).	1G-Full

Flow Control

If the port speed is set to Auto, Flow Control helps manage transmission rates to prevent data overflowing and data loss for smoother and efficient communication.

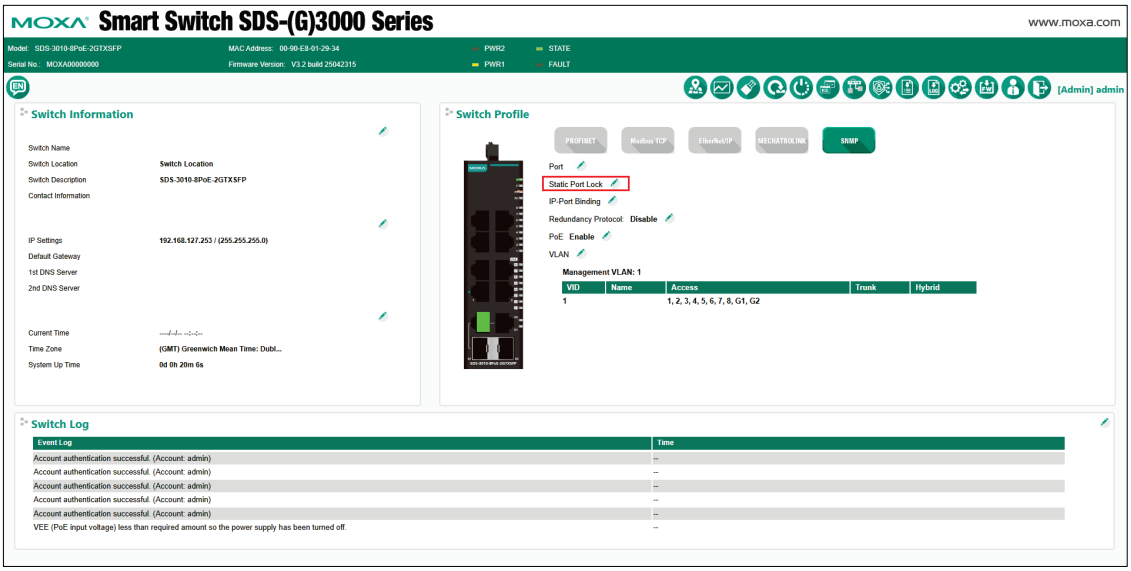
Setting	Description	Factory Default
Enable	Enable flow control for the port.	Disabled
Disable	Disable flow control for the port.	

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, this setting is fixed to Auto.	Auto
MDI	Set to the port type of the connected Ethernet device to MDI.	
MDIX	Set to the port type of the connected Ethernet device to MDIX.	

Static Port Lock Settings

To access this page, click the **Edit** ( ) button for **Static Port Lock**. From this page, you can configure the MAC addresses that can access the port.



Port

Setting	Description	Factory Default
Port	Select the port to associate a MAC address with.	None

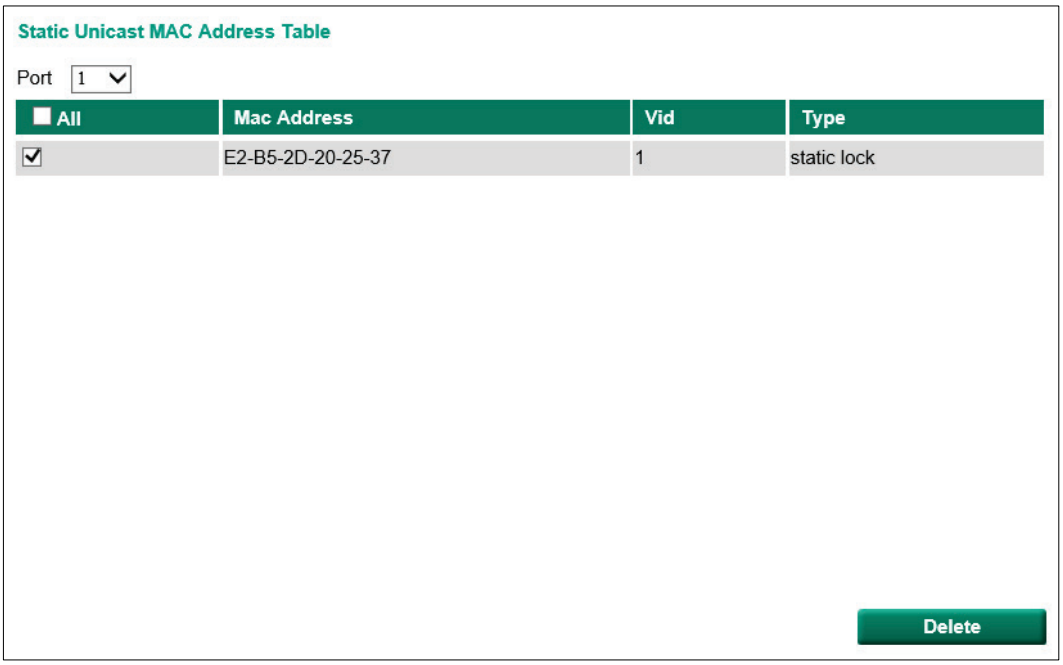
VID

Setting	Description	Factory Default
VLAN ID	Specify the VLAN ID for the port.	None

MAC Address

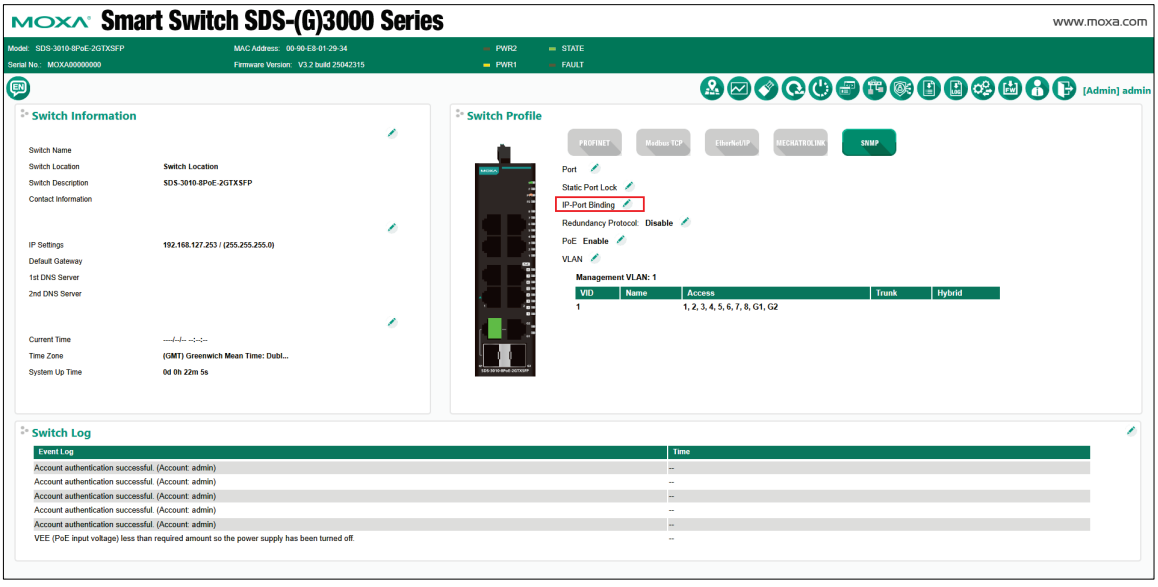
Setting	Description	Factory Default
MAC address	Specify the MAC address of the device. The associated device will be allowed to access the network.	None

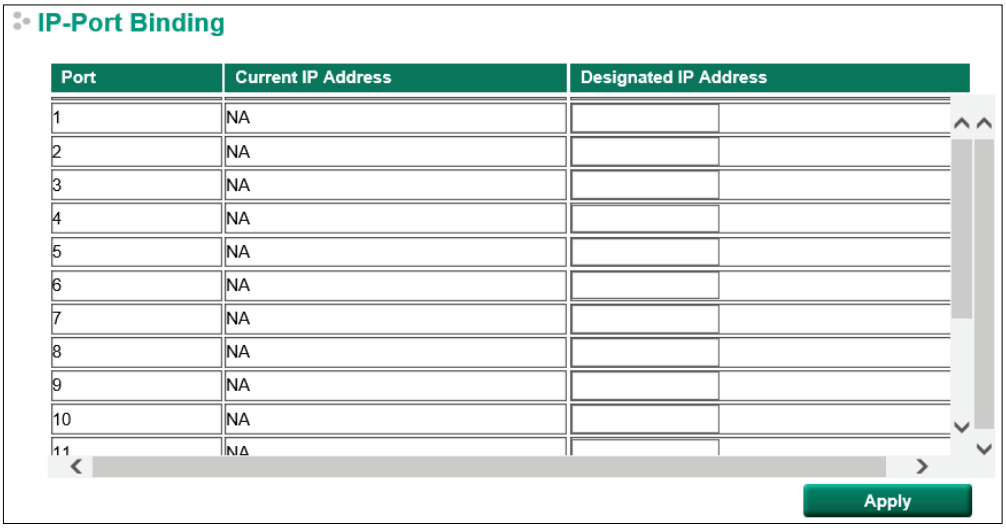
The Static Unicast MAC Address Table section shows all configured entries. To delete an entry, check the box for the entry and click **Delete**.



IP-Port Binding Settings

To access this page, click the **Edit** ( ) button for **IP-Port Binding**. From this page, you can bind a specific IP address to a port. The switch will always assign the corresponding IP address devices connected to that port.





Current IP Address

Setting	Description	Factory Default
IP address (read only)	Shows the IP address of the device connected to the port.	None

Designated IP Address

Setting	Description	Factory Default
IP address	Specify the IP address to bind the port to.	None

Redundancy Protocol Settings

To access this page, click the **Edit** ( ) button for **Redundancy Protocol**. From this page, you can configure settings for the various redundancy protocols supported by the switch. Available settings depend on the selected protocol. Refer to the following sections for more sections:

- **RSTP Settings**
- **MRP Settings**

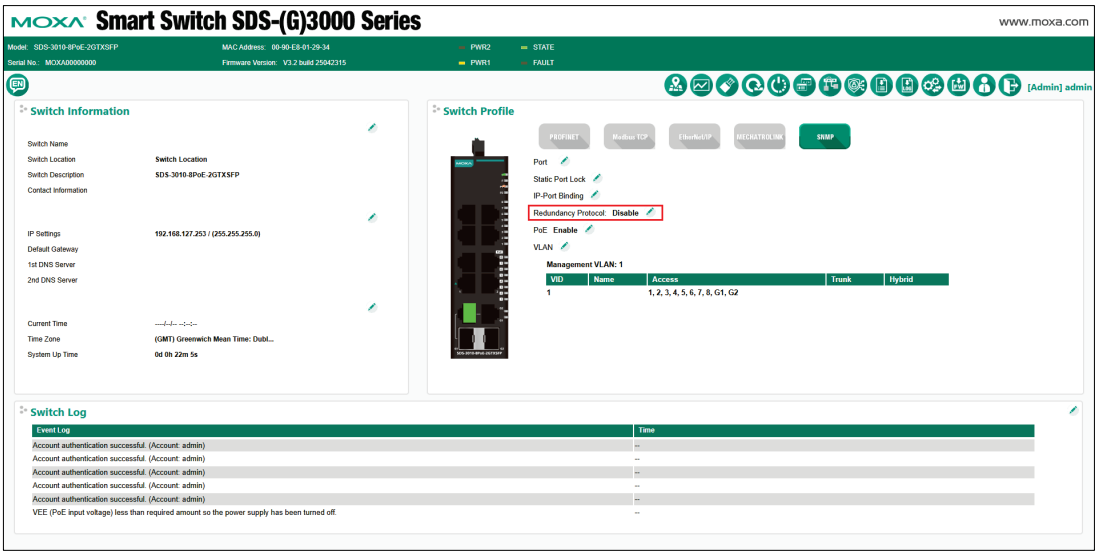
RSTP Settings

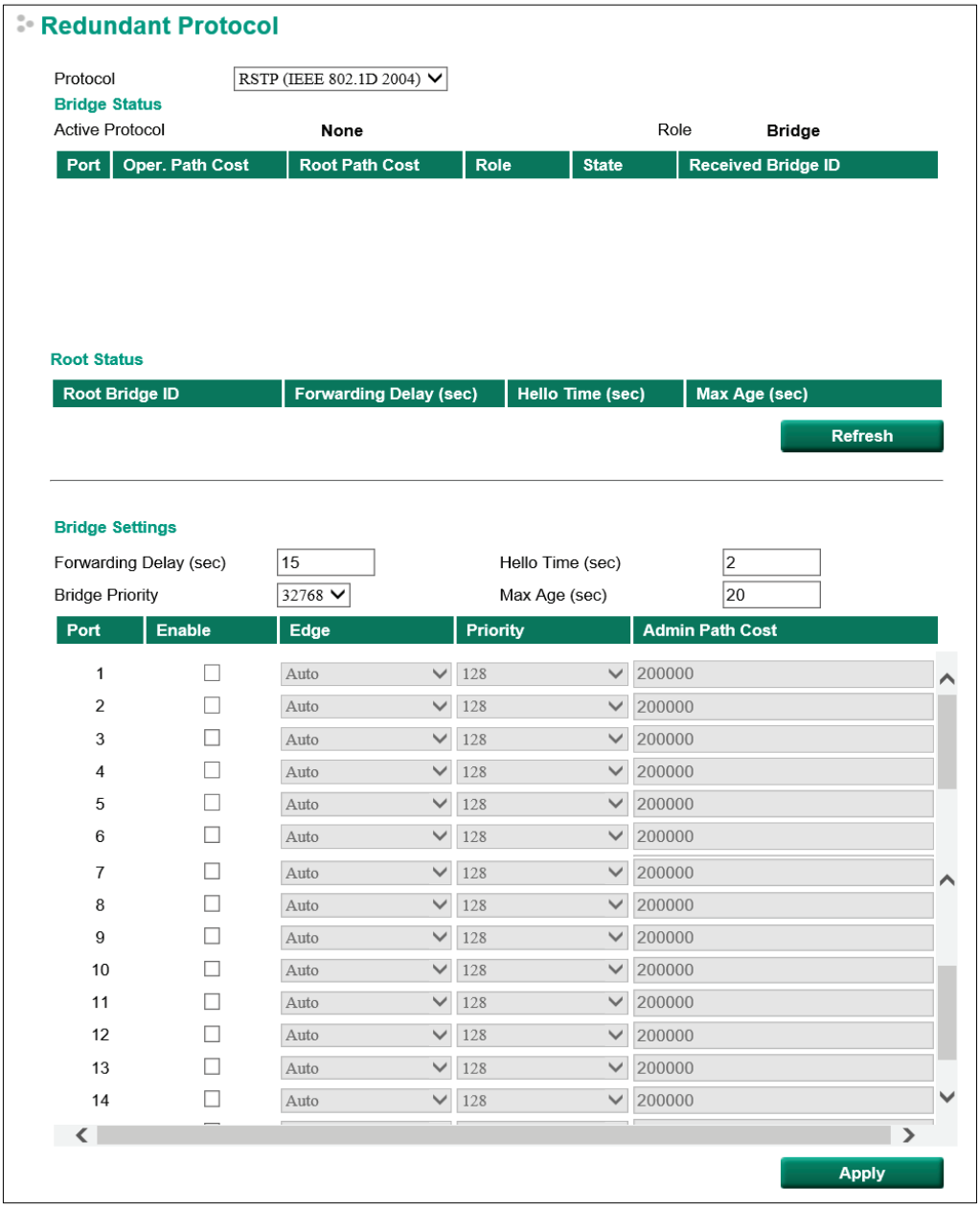
The switch supports the standard Rapid Spanning Tree Protocol (RSTP) redundancy mechanism to increase network and system reliability.

NOTE

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

To access this page, select **RSTP (IEEE 802.1D 2004)** as the protocol.


MOXA Smart Switch SDS-(G)3000 Series
www.moxa.com
Switch Information
Switch Profile
Switch Log


Redundant Protocol
Protocol
RSTP (IEEE 802.1D 2004)
Bridge Status
Active Protocol
None
Role
Bridge
Port
Oper. Path Cost
Root Path Cost
Role
State
Received Bridge ID
Root Status
Root Bridge ID
Forwarding Delay (sec)
Hello Time (sec)
Max Age (sec)
Refresh
Bridge Settings
Forwarding Delay (sec)
15
Hello Time (sec)
2
Bridge Priority
32768
Max Age (sec)
20
Port
Enable
Edge
Priority
Admin Path Cost
Apply

Forwarding delay (sec.)

Setting	Description	Factory Default
4 to 30	Specify the forwarding delay (in seconds), which determines how long the device will wait before checking if it should change to a different state.	15

Bridge priority

Setting	Description	Factory Default
0 to 61440 (multiples of 4096)	Specify the device's bridge priority. A lower value indicates a higher priority, which increases the likelihood of the switch being established as the root of the Spanning Tree topology.	32768

Hello time (sec.)

Setting	Description	Factory Default
1 to 2	Specify the Hello message interval (in seconds). The root of the Spanning Tree topology will periodically send out a "hello" message to other devices on the network to check if the topology is healthy.	2

Max. Age (sec.)

Setting	Description	Factory Default
6 to 40	Specify the max. age time (in seconds). If this device is not the root of the topology, and it has not received a hello message from the root for the specified Max. Age duration, the 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
Checkbox	Enable or disable the port as a node in the Spanning Tree topology.	Disabled

NOTE

We do not recommend enabling Spanning Tree Protocol if the port is connected to an end device (PLC, RTU, etc.) as opposed to network equipment, as this may cause unnecessary negotiation between the switch and the connected device.

Edge

Setting	Description	Factory Default
Auto	Automatically set the port state based on one of the following conditions: - If the port does not receive a BPDU within 3 seconds, the port will be put in a forwarding state. - Once the port receives a BPDU, it will start the RSTP negotiation process.	Auto
Force Edge	Set the port as a fixed edge port that will always be in a forwarding state.	
False	Set the port as a normal RSTP port.	

Priority

Setting	Description	Factory Default
Numerical value selected by user	Specify the port priority. A lower value indicates a higher priority as a node in the Spanning Tree topology.	128

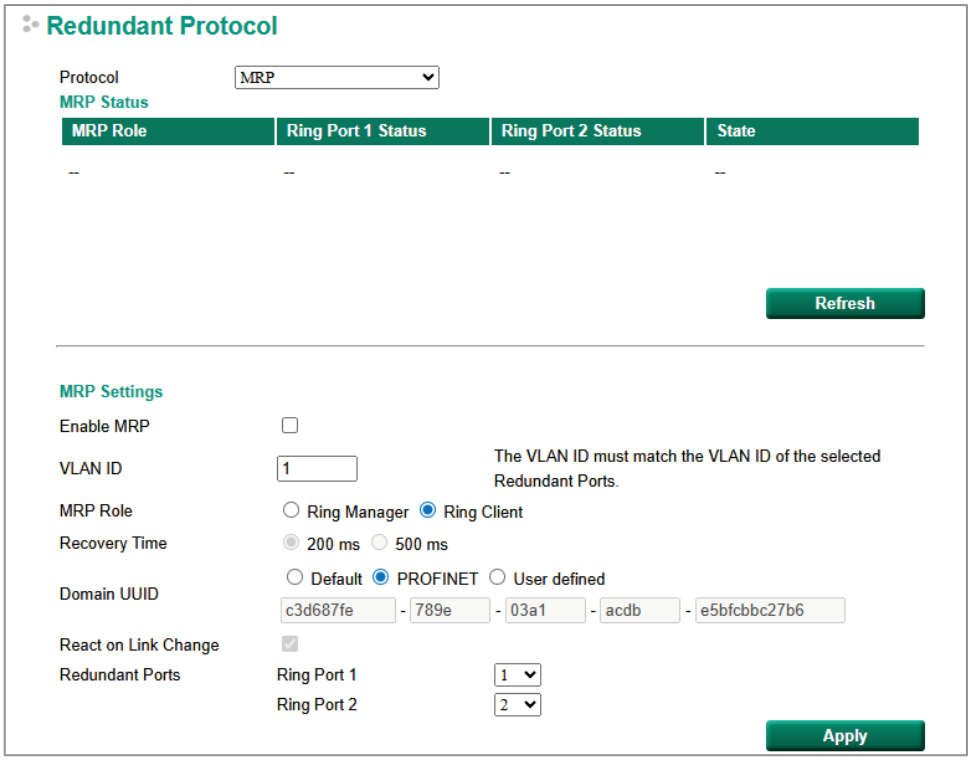
Cost

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

MRP Settings

Media Redundancy Protocol (MRP) is a protocol defined by the International Electrotechnical Commission in the IEC 62439-2 standard. The main purpose of MRP is to allow rings of Ethernet switches to recover using a redundant design. This enables fast self-redundancy recovery to ensure continuous network data flow.

To access this page, select **MRP** as the protocol.



MRP Status

The MRP Status table shows the following information:

Item	Description
MRP Role	Shows the role of the switch in the MRP ring: **Manager** or **Client**.
Ring Port 1/2 Status	Shows the current status of the ring ports. **Forwarding**: The port is transmitting data normally. **Blocking**: The port is connected to a blocked backup path. **Link Down**: No connection detected on the port.
State	Shows the condition of the MRP, dependent on the MRP role of the switch. If acting as MRP Manager: **Initiation / Awaiting Connection / Primary Ring Port Link Up / Ring Open / Ring Closed** If acting as MRP Client: **Initiation / Awaiting Connection / Data Exchange Idle / Pass Through / Data Exchange / Pass Through Idle**

MRP Settings

Enable MRP

Setting	Description	Factory Default
Checkbox	Enable or disable MRP functionality.	Disabled

VLAN ID

Setting	Description	Factory Default
1-4094	Specify the VLAN ID, which must be the same as the VLAN ID configured for the selected Redundant Ports.	1

MRP Role

Setting	Description	Factory Default
Ring Manager	Designate the switch as the MRP Manager (MRM).	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
Default	Use the default domain UUID.	PROFINET
PROFINET	Use the PROFINET domain UUID. This is recommended for PROFINET environments.	
User-defined	Specify the UUID (Universal Unique Identifier) to distinguish frames when implementing multiple MRP instances.	

React on Link Change

Setting	Description	Factory Default
Checkbox	If enabled, the MRP Manager will react to Link Down frames received from an MRP Client 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

NOTE

There are two MRP configuration sections: Module parameters and Media redundancy.

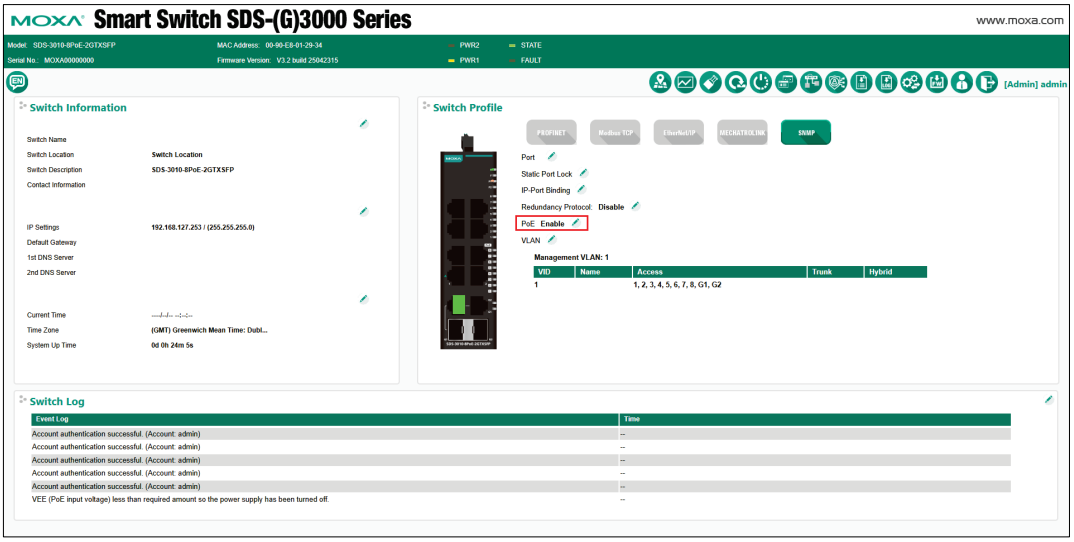
As of firmware v3.3, module parameters are no longer available in engineering deployment software such as SIMATIC STEP 7 and must be configured on the SDS device. Media redundancy can be configured in the SIMATIC STEP 7 tool or engineering deployment software.

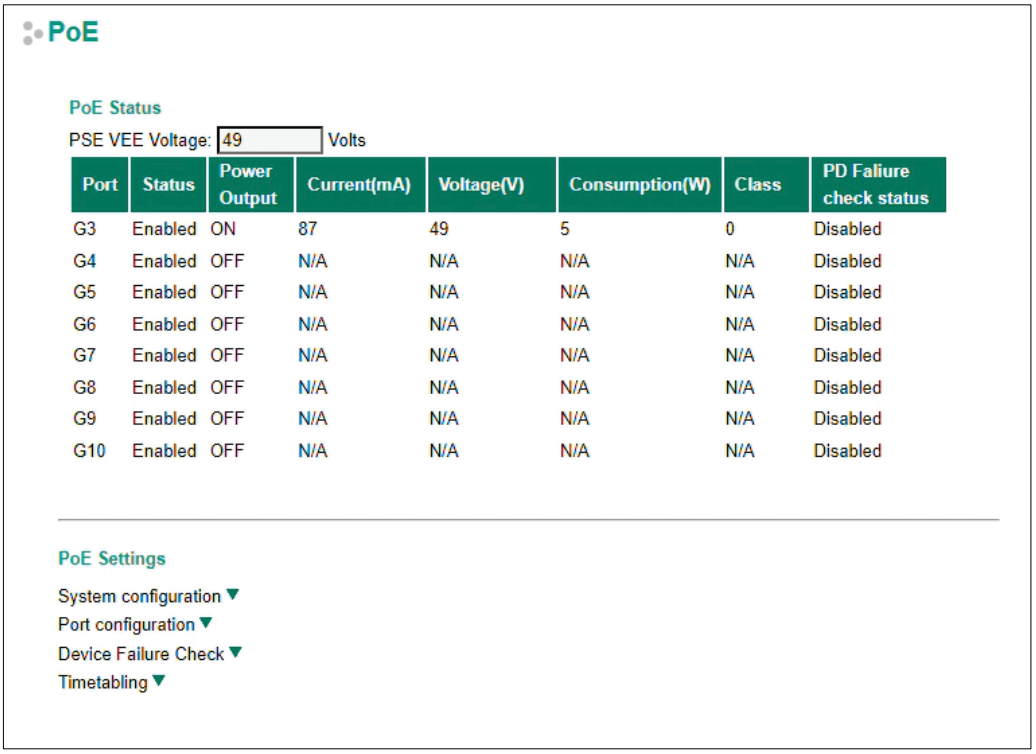
PoE Settings

To access this page, click the **Edit** ( ) button for **PoE**. From this page, you can configure additional settings for system power management, PD failure checks, and PoE power supply scheduling. The PoE Status table shows the current power supply conditions per port.

NOTE

This function is only available for SDS-(G)3000 Series PoE models.





Port	Status	Power Output	Current(mA)	Voltage(V)	Consumption(W)	Class	PD Faliure check status
G3	Enabled	ON	87	49	5	0	Disabled
G4	Enabled	OFF	N/A	N/A	N/A	N/A	Disabled
G5	Enabled	OFF	N/A	N/A	N/A	N/A	Disabled
G6	Enabled	OFF	N/A	N/A	N/A	N/A	Disabled
G7	Enabled	OFF	N/A	N/A	N/A	N/A	Disabled
G8	Enabled	OFF	N/A	N/A	N/A	N/A	Disabled
G9	Enabled	OFF	N/A	N/A	N/A	N/A	Disabled
G10	Enabled	OFF	N/A	N/A	N/A	N/A	Disabled

PoE Status

PSE VEE Voltage

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

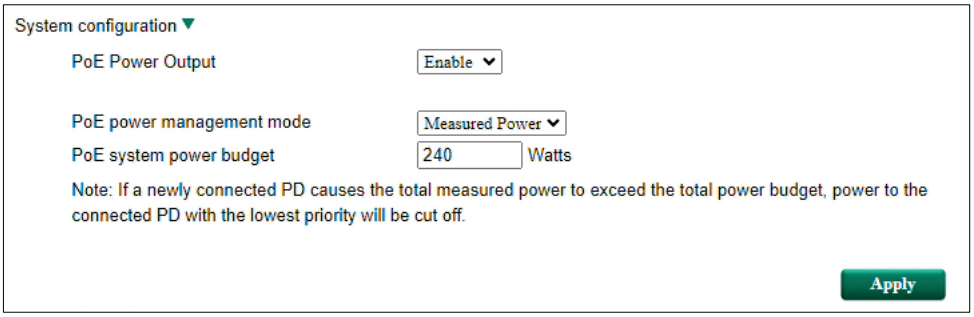
PoE Status Table

Setting	Description
Status	Shows if the PoE function is enabled or disabled on the port.
Power Output	Shows if the PoE power output to the 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.

Setting	Description
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 the PD connected to the port.	Enable
Disable	Disable PoE power output to the PD connected to the port.	

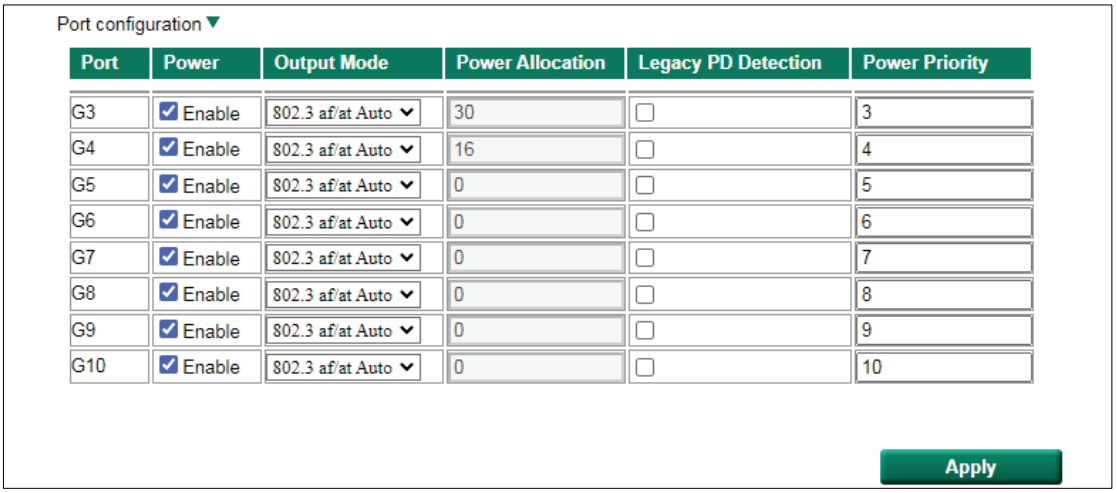
Power Management Mode

Setting	Description	Factory Default
Allocated Power	If a PD is connected that would cause the total amount of power needed for all connected devices to exceed the total allocated power limit, the switch will not power the device.	Measured Power
Measured Power	If a PD is connected that would cause the total amount of power needed for all connected devices to exceed the total measured power limit, the switch will cut the power supply 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: 240 W

Port Configuration



Power

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

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. 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. 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 switch supports the Legacy PD Detection function, which can detect if a detected PD is not compliant with the latest IEEE 802.3 PoE standard. If the capacitance of the connected PD exceeds 3 μF, it will take 10 to 15 seconds to confirm the legacy PD before PoE power is delivered to the PD through the port after the switch is turned on.

Setting	Description	Factory Default
Checkbox	Enable or disable legacy PD detection.	Disabled

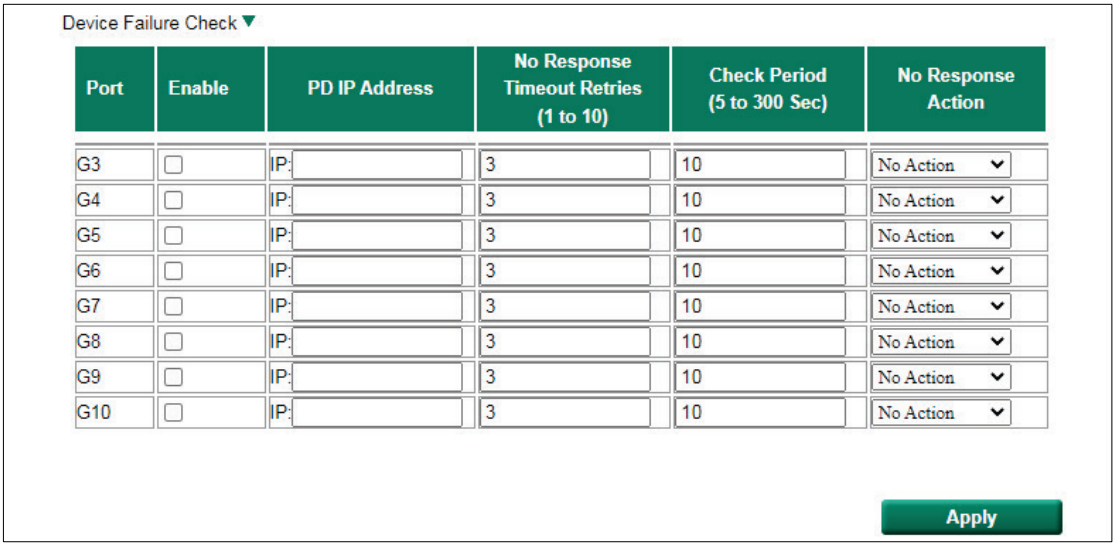
Power Priority

Use Power Priority to define port priorities when using Measured Power mode.

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. If two ports are configured with the same priority, the port with the lower port number will have the higher priority.	PoE port index number

Device Failure Check

The switch can monitor the status of a PD via its IP address. If a PD fails and the switch has not received a response from the PD after the specified Check Period, the authentication process will be restarted. This function helps ensure your network's reliability and reduces management burden.



Enable

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

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

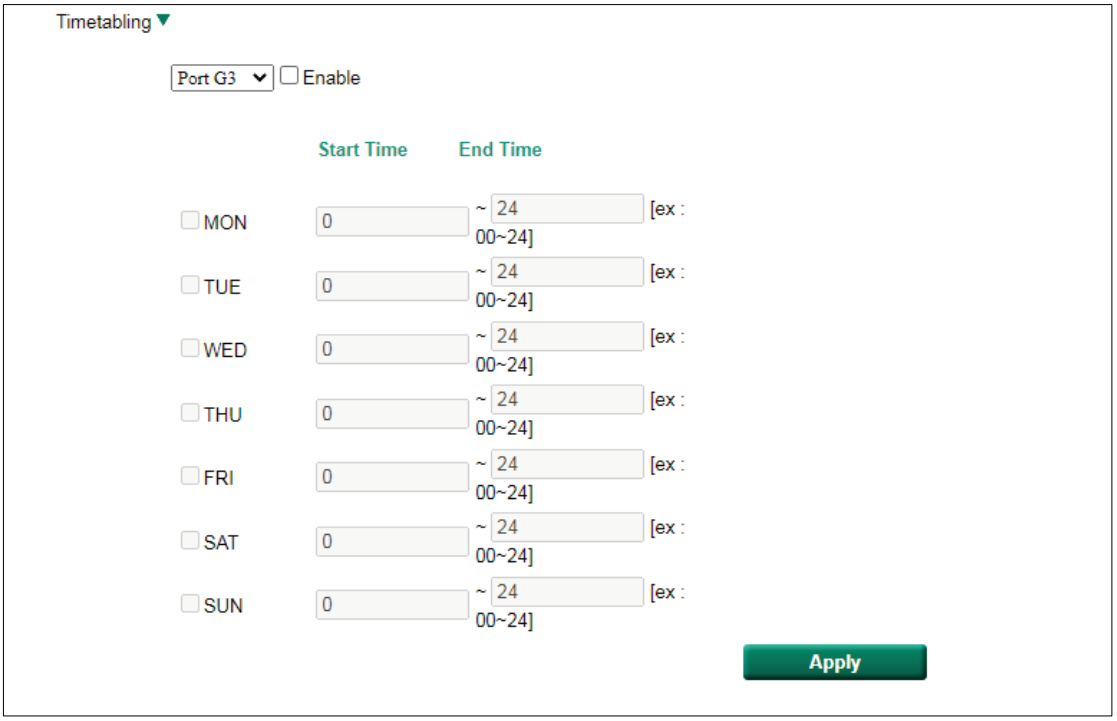
Setting	Description	Factory Default
5 to 300	Specify the time (in seconds) the switch will wait for a response between each check cycle.	10

No Response

Setting	Description	Factory Default
No Action	The PSE will not 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 switch provides a PoE timetabling mechanism that lets users economize the system's power burden by configuring 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.	Disabled

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

Setting	Description	Factory Default
Checkbox	Enable or disable PoE power scheduling for the corresponding days of the week. If timetabling if enabled on the selected port, the system will not provide PoE power to the port on days that are not checked.	Disabled

Start/End Time

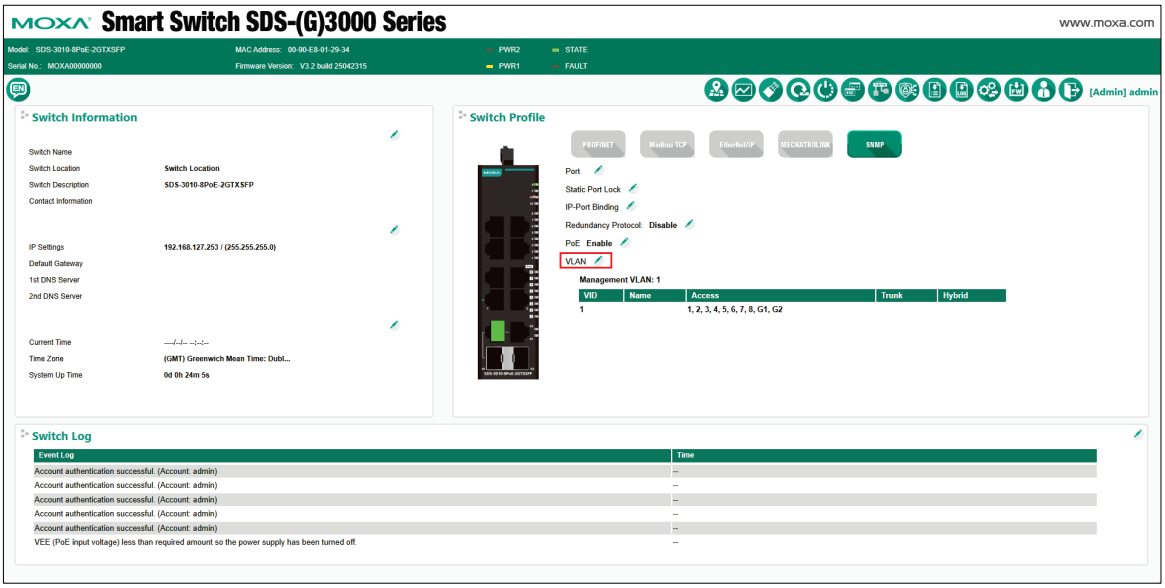
Setting	Description	Factory Default
00 to 24	If PoE power scheduling is enabled, specify the start and end time when the system will provide PoE power to the port on that day.	Start Time: 00 End Time: 24

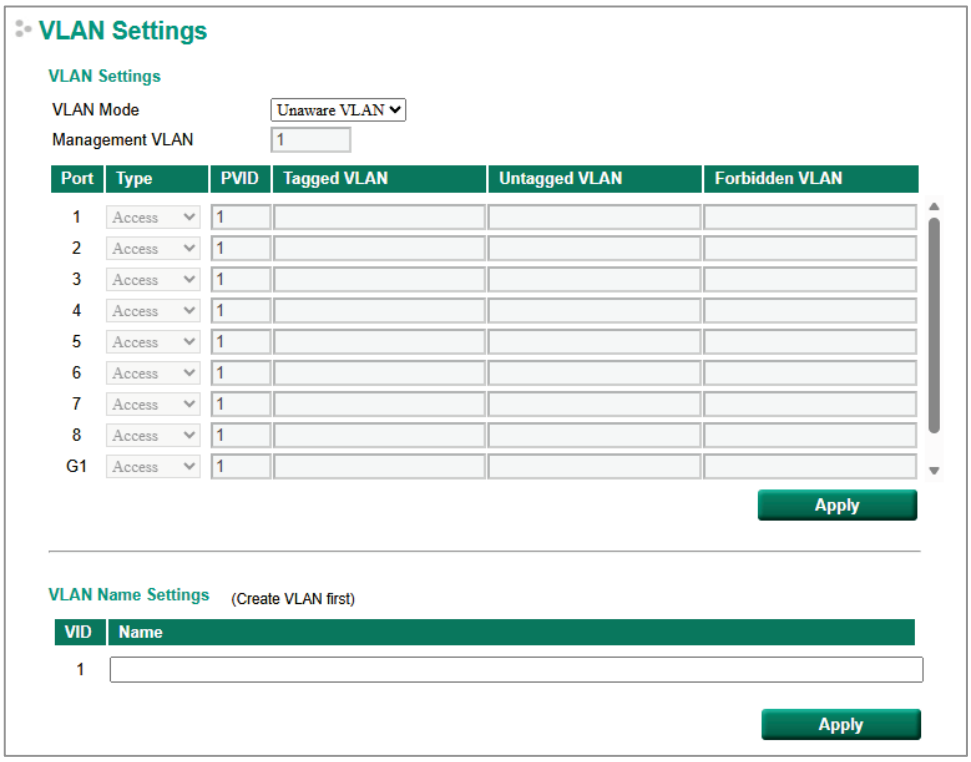
VLAN Settings

To access this page, click the **Edit** ( ) button for **VLAN**. From this page, you can configure management and port VLAN settings. 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 C** for more information about the Virtual LAN (VLAN) concept.





VLAN Mode

Setting	Description	Factory Default
802.1Q VLAN	Use 802.1Q VLAN mode. In this mode, the switch will process and redirect incoming frames to the associated VLAN based on the packet's VLAN tag.	Unaware VLAN
Unaware VLAN	Use Unaware VLAN mode. In this mode, the switch will ignore VLAN tags and process frames based on destination MAC or IP address. Using this mode will change the VLAN ID in the Static Port Lock function to 1 and will unbind all MAC addresses from the VLAN ID.	

Management VLAN ID

Setting	Description	Factory Default
1 to 4094	Specify the management VLAN ID for this switch.	1

NOTE

If the Management VLAN ID is changed, the host PC used to access the switch must be configured to be in the same VLAN.

Port

Setting	Description	Factory Default
Port number	Indicates the physical port on the switch. This is for reference only.	N/A

Type

Setting	Description	Factory Default
Access	Set the port as an access port. This is recommended when connecting to a single device for untagged VLAN traffic.	Access
Trunk	Set the port as a trunk port. This is recommended when connecting to another 802.1Q VLAN aware switch to carry tagged traffic from multiple VLANs.	
Hybrid	Set the port as a hybrid port. This is recommended when connecting to another 802.1Q VLAN aware switch or LAN that processes tagged/untagged devices and/or other switches/hubs.	

PVID

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

Tagged VLAN

Setting	Description	Factory Default
1 to 4094	If the port is set as a Trunk or Hybrid port, specify the tagged VLAN ID(s) that can be carried by the port. Use commas to separate multiple VIDs (e.g. 1,2,3).	None

Untagged VLAN

Setting	Description	Factory Default
1 to 4094	If the port is set as a Trunk or Hybrid port, specify the untagged VLAN ID(s) that can be carried by the port. The specified VLAN tags will be removed from egress traffic. Use commas to separate multiple VIDs (e.g. 1,2,3).	None

Forbidden VLAN

Setting	Description	Factory Default
1 to 4094	If the port is set as a Trunk or Hybrid port, specify the VLAN ID(s) that will be rejected by port. Use commas to separate multiple VIDs (e.g. 1,2,3).	None

VLAN Name Settings

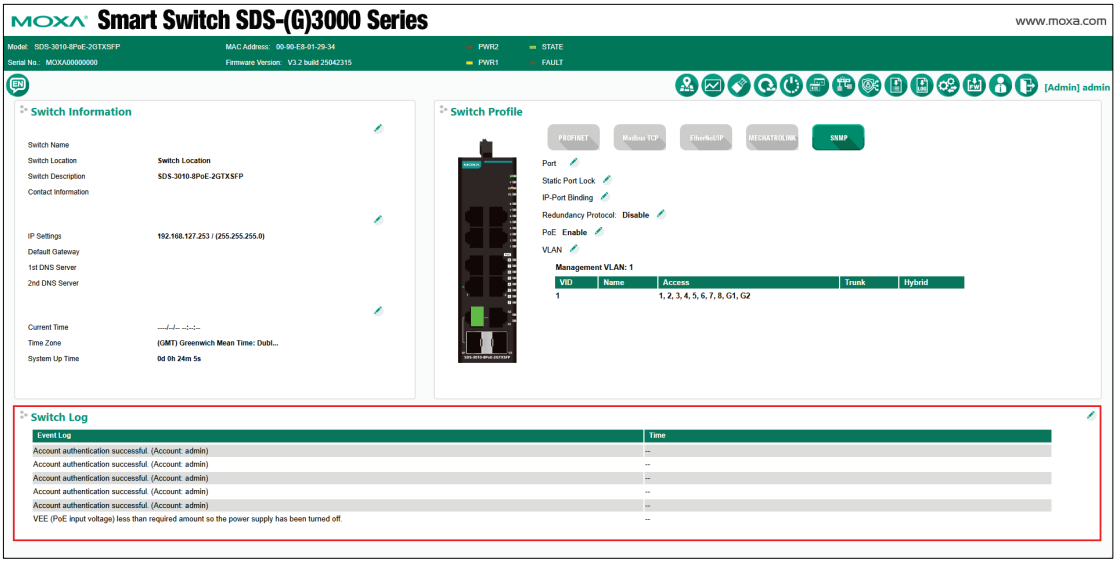
You may associate a VLAN name with each VLAN ID (VID). This requires a VLAN to be created first.

VLAN Name Settings

Setting	Description	Factory Default
Name	Enter a name for the VLAN. The VLAN name can only include the following characters: Letters (a-z, A-Z), numbers (0-9), hyphens (-), underscores (_)	None

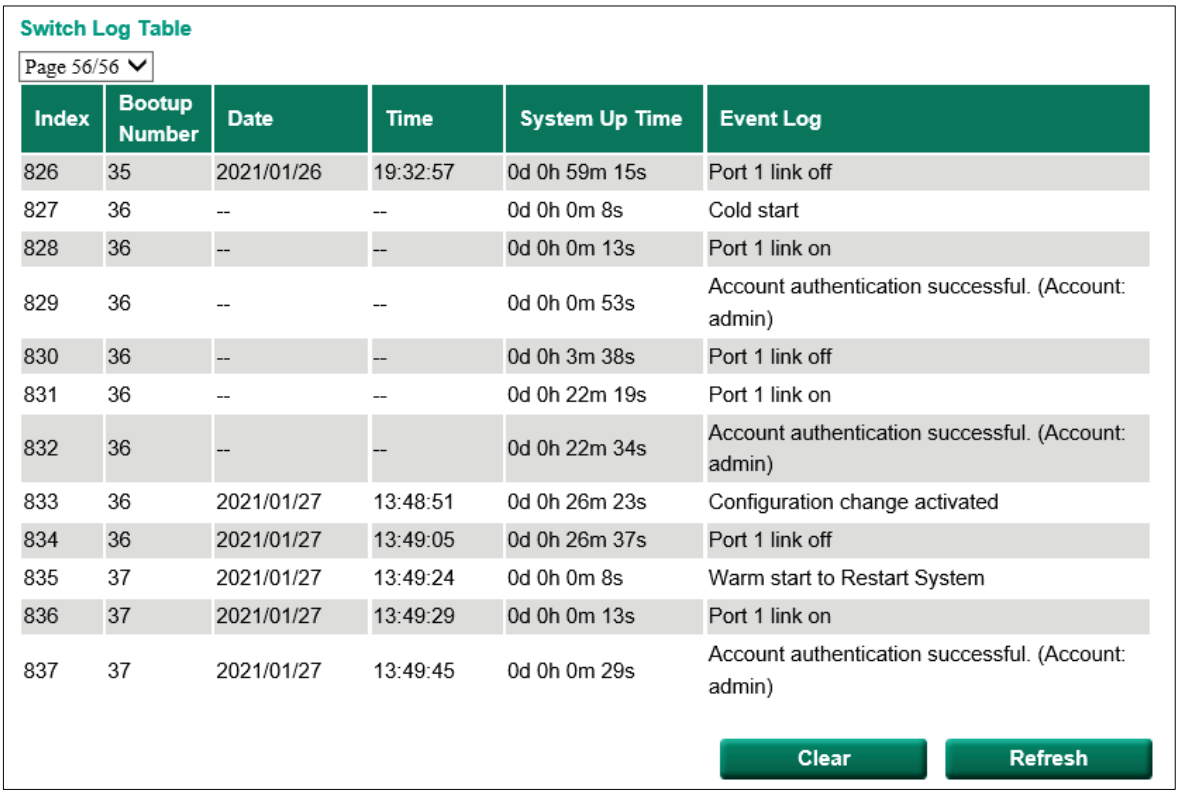
Switch Log

The **Switch Log** section of the dashboard shows the latest recorded event logs. Click the **Edit** ( ) button in the top-right of the table to check other event logs that have already been recorded, or to set event warning notifications.



Switch Log Table

The 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.



Switch Log Table

Page 56/56

Index	Bootup Number	Date	Time	System Up Time	Event Log
826	35	2021/01/26	19:32:57	0d 0h 59m 15s	Port 1 link off
827	36	--	--	0d 0h 0m 8s	Cold start
828	36	--	--	0d 0h 0m 13s	Port 1 link on
829	36	--	--	0d 0h 0m 53s	Account authentication successful. (Account: admin)
830	36	--	--	0d 0h 3m 38s	Port 1 link off
831	36	--	--	0d 0h 22m 19s	Port 1 link on
832	36	--	--	0d 0h 22m 34s	Account authentication successful. (Account: admin)
833	36	2021/01/27	13:48:51	0d 0h 26m 23s	Configuration change activated
834	36	2021/01/27	13:49:05	0d 0h 26m 37s	Port 1 link off
835	37	2021/01/27	13:49:24	0d 0h 0m 8s	Warm start to Restart System
836	37	2021/01/27	13:49:29	0d 0h 0m 13s	Port 1 link on
837	37	2021/01/27	13:49:45	0d 0h 0m 29s	Account authentication successful. (Account: admin)

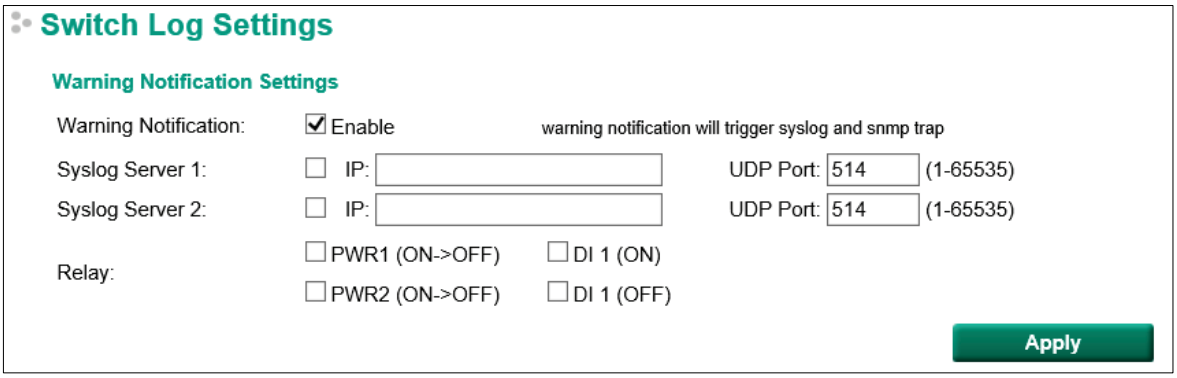
Clear Refresh

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

Index	The index of the event.
Bootup Number	This field shows how many times the Moxa switch has been rebooted or cold started.
Date	The date the event was recorded. This timestamp is based on the system time settings.
Time	The time the event was recorded. This timestamp is based on the system time settings.
System Startup Time	The system startup time related to this event.
Event Log	The event that 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. Each switch also 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.

NOTE

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

- Cold start
- Warm start
- Configuration change
- Power 1 or 2 transition: Off to On, On to Off
- Login success
- Login failure
- Redundancy protocol/topology change
- RSTP Root change
- RSTP topology change
- DI on
- DI off
- ABC-02 status
- Port looping
- LLDP table change
- Login failure lockout
- Account info change
- Configuration import
- SSL certificate import
- Fiber Check warning
- MRP multiple managers

- MRP Ring open
- Port link on
- Port link off

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

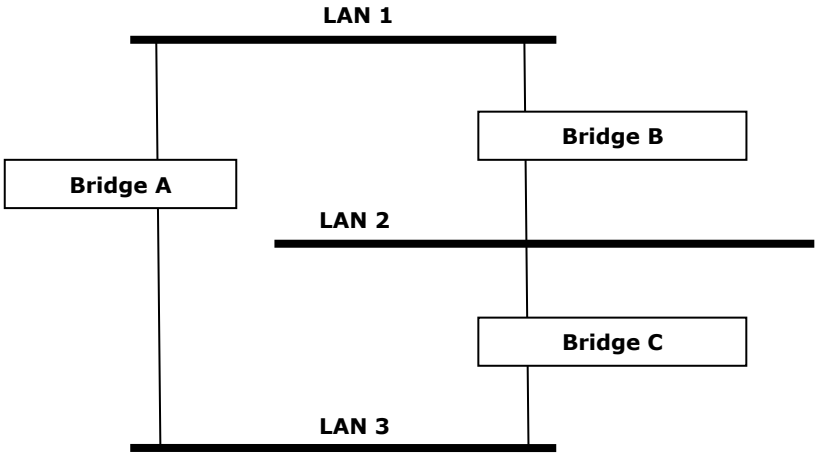
The STP protocol is part of the IEEE Std 802.1D, 2004 Edition bridge specification. The following explanation uses "bridge" instead of "switch."

What is STP?

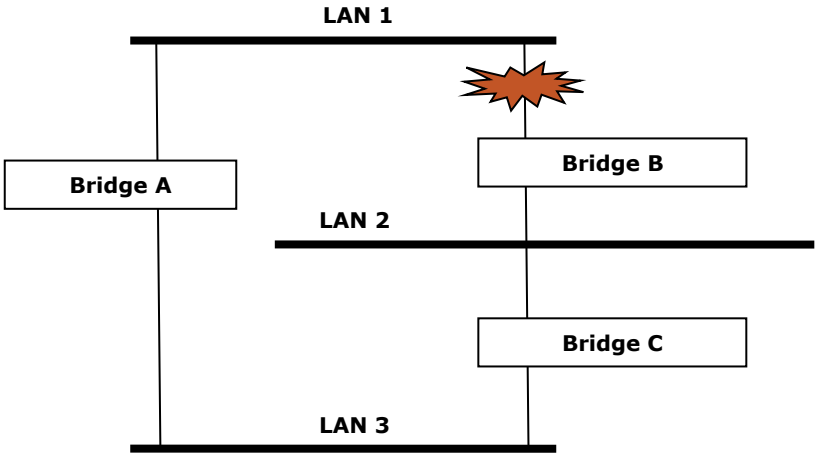
STP (802.1D) is a bridge-based system that is used to implement parallel paths for network traffic. STP uses a loop-detection process to:

- 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.

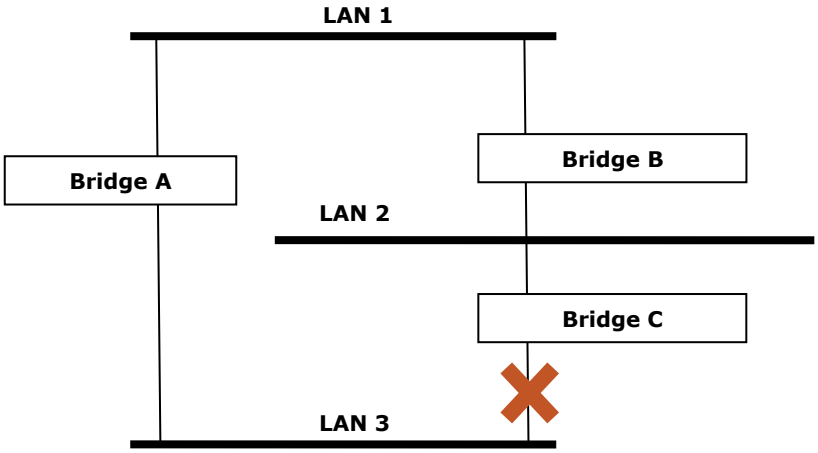
The figure below shows a network made up of three LANs separated by three bridges. Each segment uses at most two paths to communicate with the other segments. Since this configuration can give rise to loops, the network will overload if STP is NOT enabled.



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):

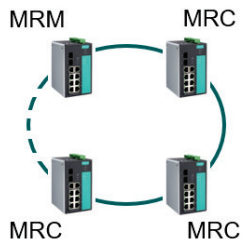
Also known as the Ring Manager, is a node that observes and controls the ring topology in order to react to network faults. There is only one MRM in the network. In the event of a Link Down scenario, the MRM diagnoses the issue and notifies all MRCs (Media Redundancy Clients) to clear their FDB (Filtering 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.



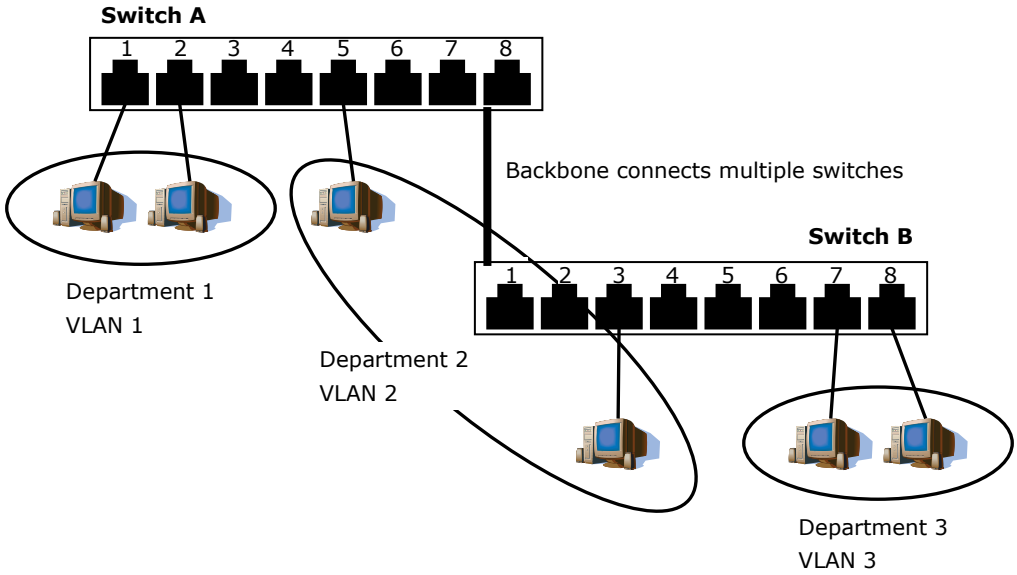
One of the ring ports on MRM will be in a blocking state, while the other port will be in a forwarding state. The path connected to the blocking port is the redundant path. Similarly, MRCs require two ports, both of which would be in a forwarding state.

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.

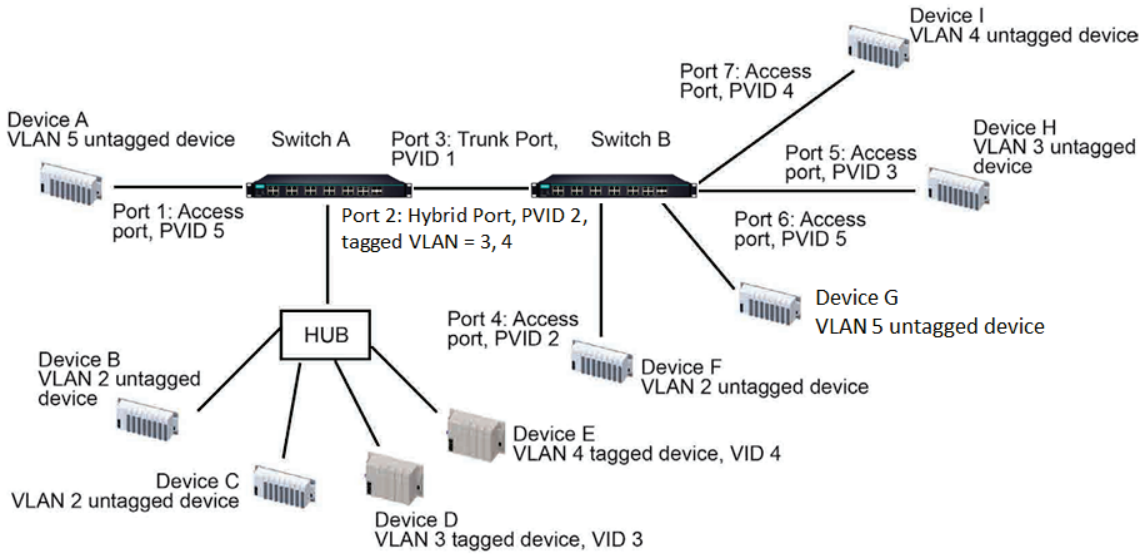
To carry multiple VLANs across a single physical link (backbone, trunk), each packet must be tagged with a VLAN identifier so that the switches can identify which packets belong in which VLAN. To communicate between VLANs, a router must be used.

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.