Moxa Managed Ethernet Switch
User Manual

Version 9.9, August 2023

www.moxa.com/products

© 2023 Moxa Inc. All rights reserved.

Moxa Managed Ethernet Switch User Manual

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

Copyright Notice

© 2023 Moxa Inc. All rights reserved.

Trademarks

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

Disclaimer

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

Technical Support Contact Information

www.moxa.com/support

Table of Contents

1. About this Manual 5
2. Getting Started 6
Serial Console Configuration (115200, None, 8, 1, VT100) 6
Configuration by Telnet Console 8
Configuration by Web Browser 10
Disabling Telnet and Browser Access 12
3. Featured Functions 13
Configuring Basic Settings 13
System Identification 13
Password 15
Password Login Policy 16
Accessible IP List 16
Port Settings 17
Network Parameters 19
GARP Timer Parameters 21
System Time Settings 21
IEEE 1588 PTP 23
Turbo Ring DIP Switch 28
System File Update 29
Restart 30
Reset to Factory Default 31
Loop Protection 31
Using Port Trunking 31
The Port Trunking Concept 32
Port Trunking Settings 32
Configuring SNMP 34
SNMP Read/Write Settings 35
Trap Settings 36
Private MIB Information 37
Using PoE (PoE Models Only) 37
Type 1 37
Type 2 41
Using Traffic Prioritization 50
The Traffic Prioritization Concept 50
Configuring Traffic Prioritization 52
Using Virtual LAN 56
The Virtual LAN (VLAN) Concept 56
Sample Applications of VLANs Using Moxa Switches 58
Configuring Virtual LAN 59
QinQ Setting 62
VLAN Table 63
Using Multicast Filtering 63
The Concept of Multicast Filtering 63
Configuring IGMP Snooping 67
Current Active IGMP Streams 69
Static Multicast MAC Addresses 70
Configuring GMRP 71
GMRP Table 71
Multicast Filtering Behavior 72
Using Bandwidth Management 72
Configuring Bandwidth Management 72
Security 76
Management Interface 76
User Login Authentication – User Login Settings 77
User Login Authentication – Auth Server Setting 77
Authentication Certificate 78
SSL Certificate Management 79
Using Port Access Control 79

Static Port Lock 79
IEEE 802.1X 79
Configuring Static Port Lock 80
Configuring IEEE 802.1X 81
Using Auto Warning 84
Configuring Email Warning 84
Configuring Relay Warning 87
Using Line-Swap-Fast-Recovery 89
Configuring Line-Swap Fast Recovery 89
Using Set Device IP 90
Configuring Set Device IP 91
Configuring DHCP Relay Agent 91
Using Diagnosis 93
Mirror Port 93
Ping 95
LLDP Function 95
Using Monitor 96
Monitor by Switch 96
Monitor by Port 97
Monitor by SFP 97
Using the MAC Address Table 98
Using Access Control List 98
The ACL Concept 99
Access Control List Configuration and Setup 100
Using Event Log 104
Using Syslog 105
Using Industrial Protocols 105
Using HTTPS/SSL 106
4. EDS Configurator GUI 107
Starting EDS Configurator 107
Broadcast Search 108
Search by IP Address 109
Upgrade Firmware 109
Modify IP Address 110
Export Configuration 111
Import Configuration 112
Unlock Server 113
A. MIB Groups 115

1. About this Manual

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

The following two chapters are covered in this user manual:

- **Chapter 2: Getting Started**

  This chapter explains the initial installation process for Moxa switches. There are three ways to access a Moxa switch's configuration settings: serial console, Telnet console, and web console.

- **Chapter 3: Featured Functions**

  This chapter explains how to access a Moxa switch's various configuration, monitoring, and administration functions. These functions can be accessed by serial, Telnet, or web console. The web console is the most user-friendly way to configure a Moxa switch. In this chapter, we use the web console interface to introduce the functions.

2. Getting Started

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

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

NOTE

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

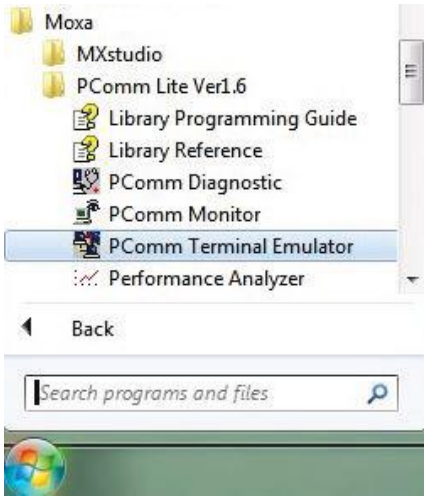
NOTE

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

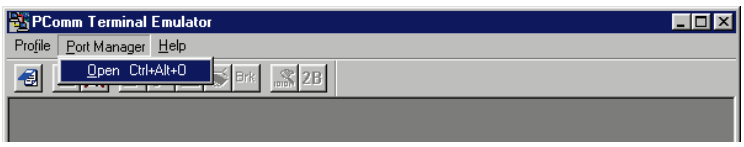
Before running PComm Terminal Emulator, use an RJ45 to DB9-F (or RJ45 to DB25-F) cable to connect the Moxa switch's console port to your PC's COM port (generally COM1 or COM2, depending on how your system is set up).

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

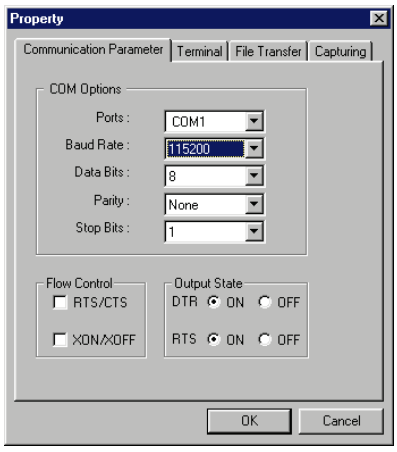
1. From the Windows desktop, click **Start > Moxa > PComm Lite Ver1.6 > Terminal Emulator**.



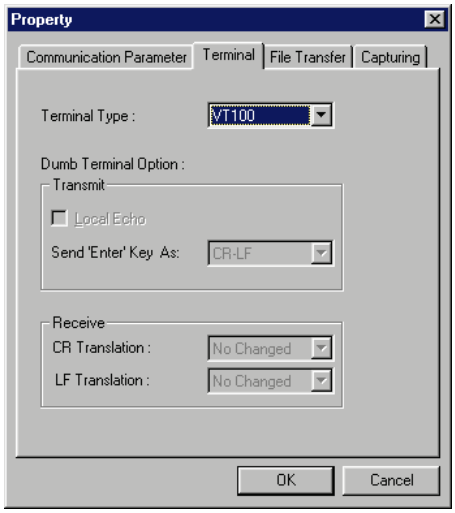
2. Select **Open** under the **Port Manager** menu to open a new connection.



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



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



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

```
MOXA EtherDevice Switch  IKS-6726
Console terminal type (1: ansi/vt100, 2: vt52) : 1
```

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

```
Model :              IKS-6726-T
Name :               Managed Redundant Switch 02678
Location :           Switch Location

Firmware Version :   V2.6
Serial No :          02678
IP :                 192.168.127.253
MAC Address :        00-90-E8-1B-55-24
                      +-------+
 +--------------------| admin |-+
 | Account  : [admin] | user  | |
 | Password :         +-------+ |
 +------------------------------+
```

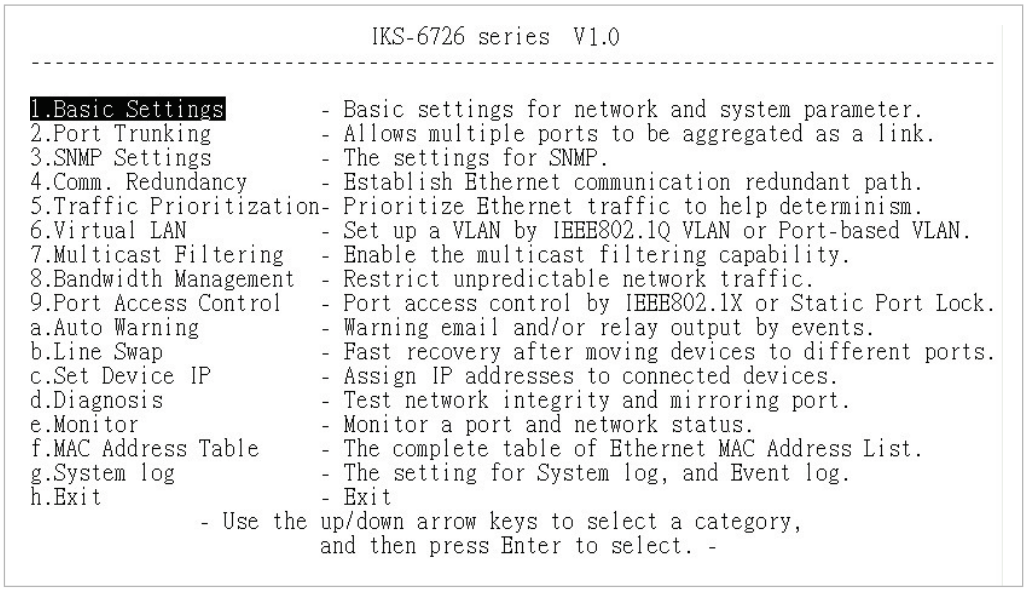
NOTE

In firmware v3.9 or above on EDS-400A Series (except for the EDS-405A Series and EDS-408A Series), EDS-500A Series, and EDS-P500A Series:

1. The default password assigned to the Moxa switch is moxa. Be sure to change the default password after you first log in to help enhance security.
2. The password cannot be blank and please choose a strong password to enhance security.
3. When updating the firmware from v3.9 or below with the password set as blank, the console will prompt you to set up a new password that has at least four characters.

The above measures also apply to the EDS-405A Series and EDS-408A Series in firmware v3.10 or later.

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



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

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

Configuration by Telnet Console

Opening the Moxa switch's Telnet or web console over a network requires that the PC host and Moxa switch are on the same logical subnet. You may need to adjust your PC host's IP address and subnet mask. By default, the Moxa switch's IP address is 192.168.127.253 and the Moxa switch's subnet mask is 255.255.255.0 (referred to as a Class B network). Your PC's IP address must be set to 192.168.xxx.xxx if the subnet mask is 255.255.0.0, or to 192.168.127.xxx if the subnet mask is 255.255.255.0.

NOTE

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

NOTE

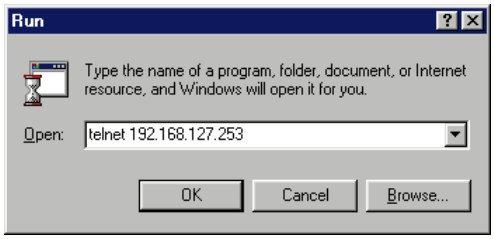
When connecting to the Moxa switch's Telnet or web console, first connect one of the Moxa switch's Ethernet ports to your Ethernet LAN, or directly to your PC's Ethernet port. You may use either a straight-through or cross-over Ethernet cable.

NOTE

The Moxa switch's default IP address is 192.168.127.253.

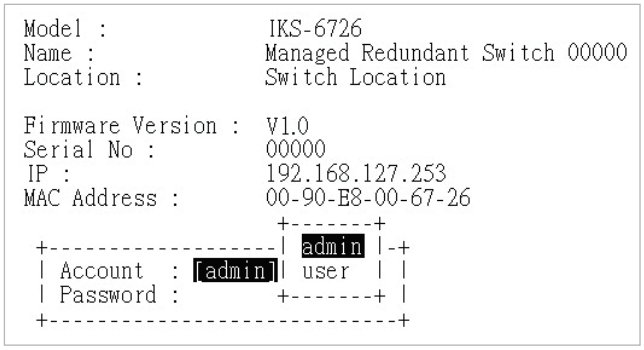
After making sure that the Moxa switch is connected to the same LAN and logical subnet as your PC, open the Moxa switch's Telnet console as follows:

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



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

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



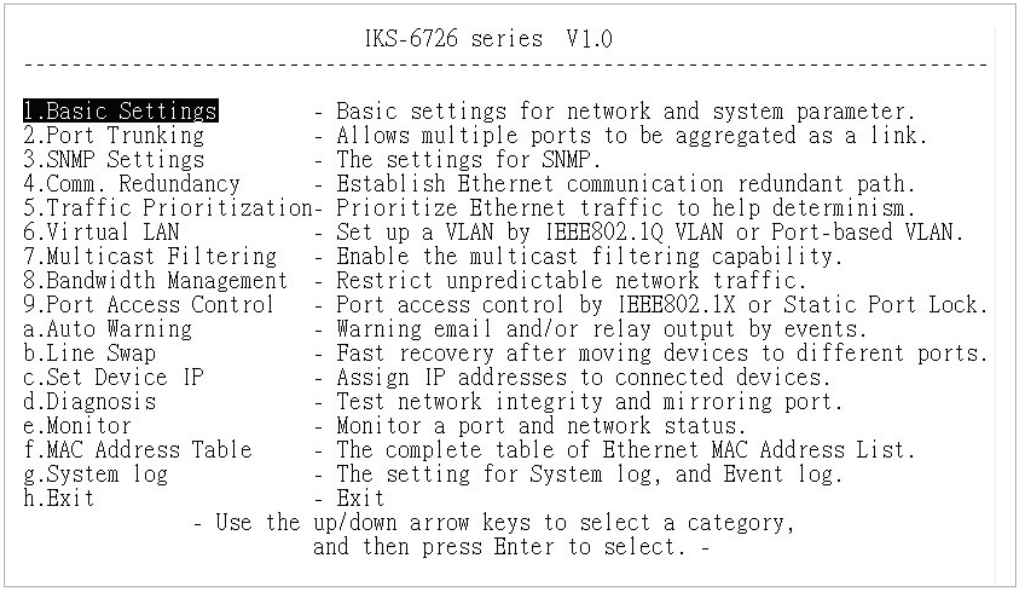
NOTE

In firmware v3.9 or above on EDS-400A Series (except for the EDS-405A Series and EDS-408A Series), EDS-500A Series, and EDS-P500A Series:

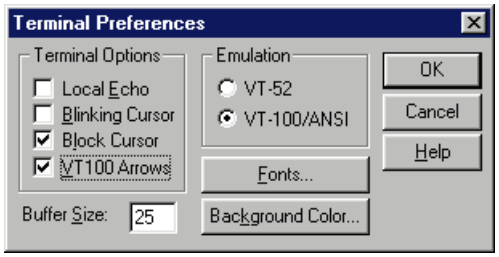
1. The default password assigned to the Moxa switch is moxa. Be sure to change the default password after you first log in to help enhance security.
2. The password cannot be blank and please choose a strong password to enhance security.
3. When updating the firmware from v3.9 or below with the password set as blank, the console will prompt you to set up a new password that has at least four characters.

The above measures also apply to the EDS-405A Series and EDS-408A Series in firmware v3.10 or later.

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



5. In the terminal window, select **Preferences...** from the **Terminal** menu on the menu bar.
6. The **Terminal Preferences** window should appear. Make sure that **VT100 Arrows** is checked.



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

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

NOTE

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

Configuration by Web Browser

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

NOTE

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

NOTE

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

NOTE

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

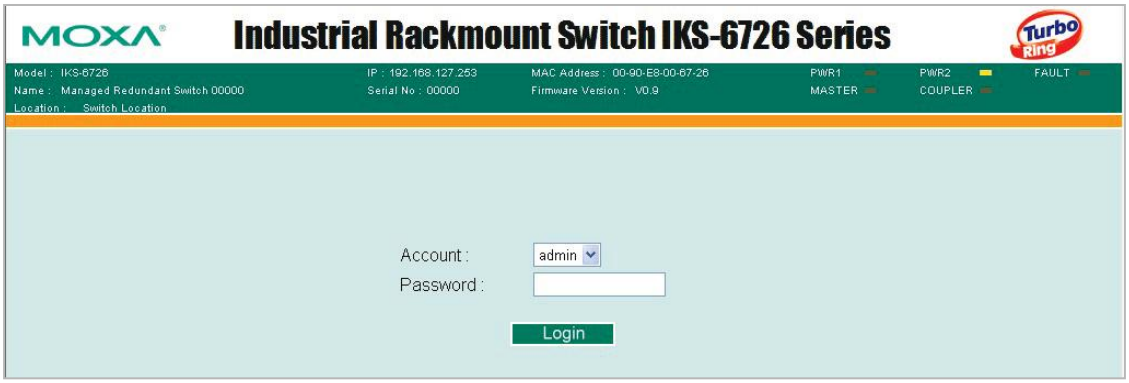
NOTE

The Moxa switch's default IP address is 192.168.127.253.

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

1. Connect your web browser to the Moxa switch's IP address by entering it in the **Address** or **URL** field.

2. The Moxa switch's web console will open, and you will be prompted to log in. Select the login account (admin or user) and enter the **Password**. This password will be required to access any of the consoles (web, serial, Telnet).



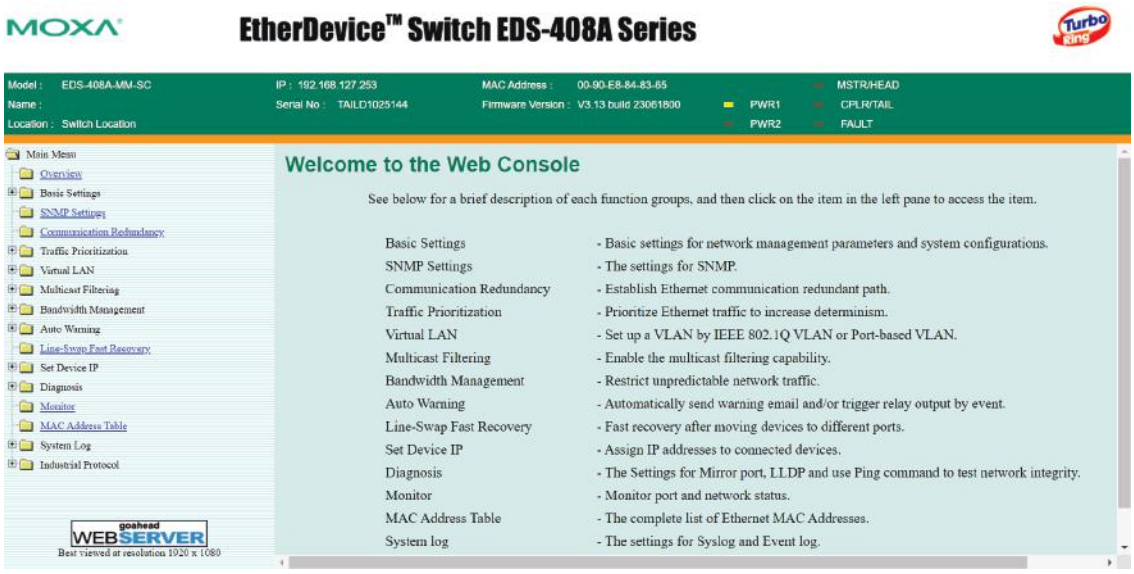
NOTE

In firmware v3.9 or above on EDS-400A Series (except for the EDS-405A Series and EDS-408A Series), EDS-500A Series, and EDS-P500A Series:

1. The default password assigned to the Moxa switch is moxa. Be sure to change the default password after you first log in to help enhance security.
2. The password cannot be blank and please choose a strong password to enhance security.
3. When updating the firmware from v3.9 or below with the password set as blank, the console will prompt you to set up a new password that has at least four characters.

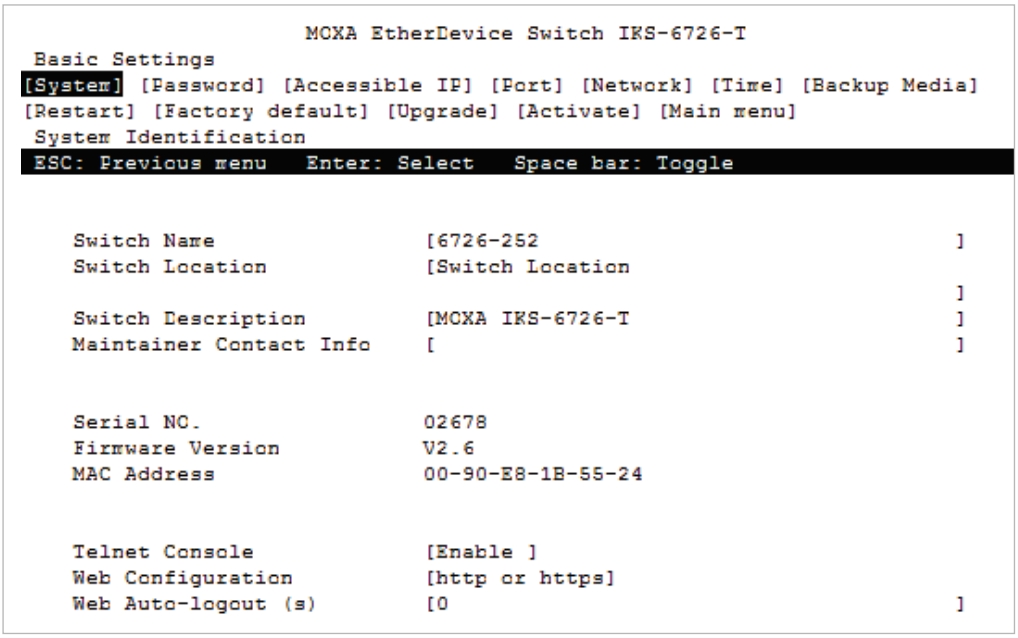
The above measures also apply to the EDS-405A Series and EDS-408A Series in firmware v3.10 or later.

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



Disabling Telnet and Browser Access

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



3. Featured Functions

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

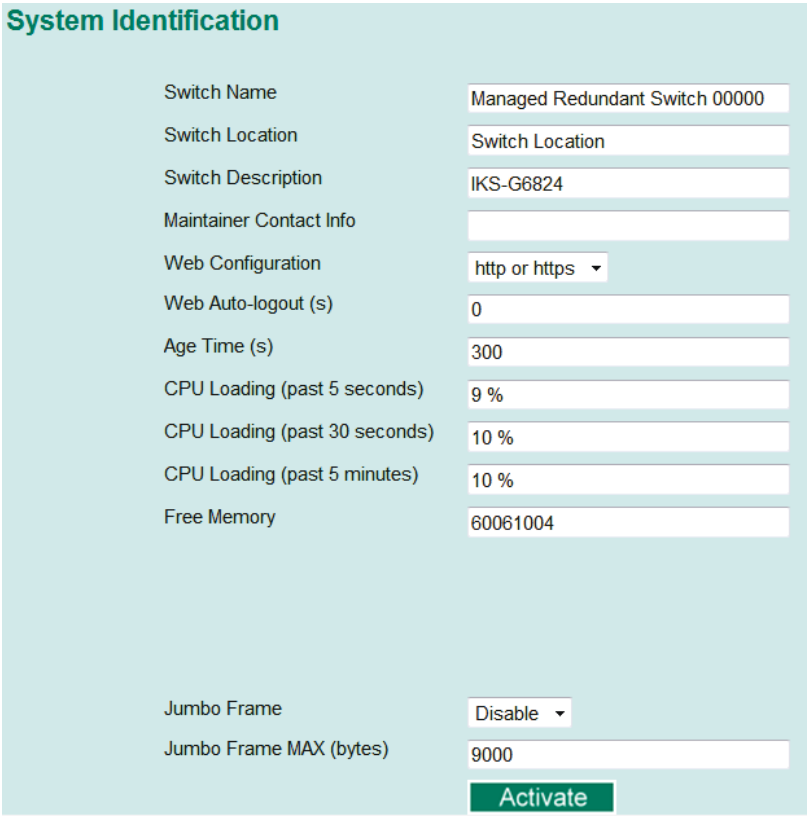
The web console is the most user-friendly interface for configuring a Moxa switch. In this chapter, we use the web console interface to introduce the functions. There are only a few differences between the web console, serial console, and Telnet console.

Configuring Basic Settings

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

System Identification

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



Switch Name

Setting	Description	Factory Default
Max. 30 characters	This option is useful for differentiating between the roles or applications of different units. Example: Factory Switch 1.	Managed Redundant Switch [Serial no. of this switch]

Switch Location

Setting	Description	Factory Default
Max. 80 characters	This option is useful for differentiating between the locations of different units. Example: production line 1.	Switch Location

Switch Description

Setting	Description	Factory Default
Max. 30 characters	This option is useful for recording a more detailed description of the unit.	None

Maintainer Contact Info

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

Web Configuration

Setting	Description	Factory default
Disable	No web service allowed	https or http
https or http	Web connection via https or http	
https only	Web connection via https only	

Web Auto-logout (S)

Setting	Description	Factory Default
60 to 86400 (seconds)	Disable or extend the auto-logout time for the web management console.	0 (disabled)

Age Time (S)

Setting	Description	Factory Default
15 to 3825 (seconds)	The length of time that a MAC address entry can remain in the Moxa switch. When an entry reaches its aging time, it "ages out" and is purged from the switch, effectively cancelling frame forwarding to that specific port.	300

CPU Loading

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

Free Memory

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

Jumbo Frame

Setting	Description	Factory Default
Enable	Enables the Moxa switch to support the Jumbo Frame function	Disabled
Disable	Disables the Jumbo Frame function	

Jumbo Frame MAX (bytes)

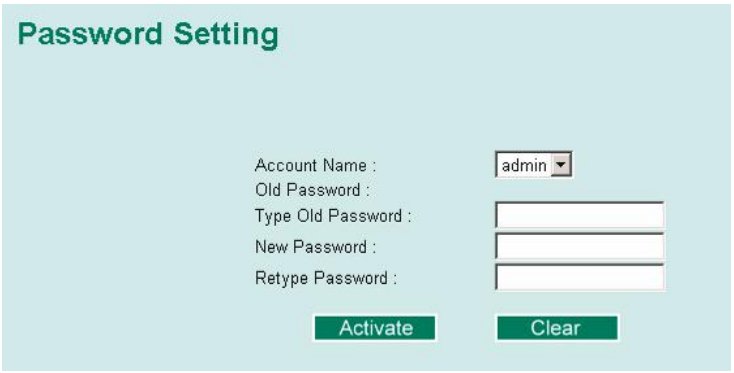
Setting	Description	Factory Default
1522 to 9000	The maximum length supported by the Jumbo Frame function	9000

NOTE

"Jumbo Frame" is supported by the IKS-G6000 series and the ICS-G7000 Series.

Password

The Moxa switch provides two levels of configuration access. The **admin** account has read/write access of all configuration parameters, and the **user** account has read access only. A **user** account can view the configuration, but will not be able to make modifications.



ATTENTION

In firmware v3.9 or above on EDS-400A Series (except for the EDS-405A Series and EDS-408A Series), EDS-500A Series, and EDS-P500A Series:

1. The default password assigned to the Moxa switch is moxa. Be sure to change the default password after you first log in to help enhance security.
2. The password cannot be blank and please choose a strong password to enhance security.
3. When updating the firmware from v3.9 or below with the password set as blank, the console will prompt you to set up a new password that has at least four characters.

The above measures also apply to the EDS-405A Series and EDS-408A Series in firmware v3.10 or later.

Account

Setting	Description	Factory Default
Admin	This account can modify the Moxa switch's configuration.	admin
User	This account can only view the Moxa switch's configurations.	

Password

Setting	Description	Factory Default
Old password (max. 16 characters)	Enter the current password	None
New password (Max. 16 characters)	Enter the desired new password.	None
Retype password (Max. 16 characters)	Enter the desired new password again.	None

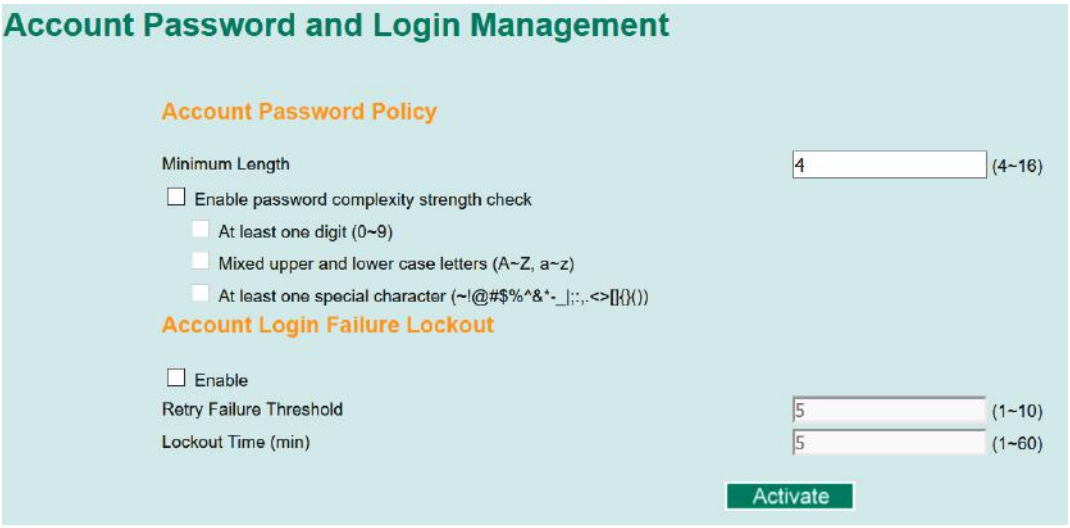
NOTE

The valid special characters are (~!@#$%^&*-_|;:,.<>[]{}()).

Password Login Policy

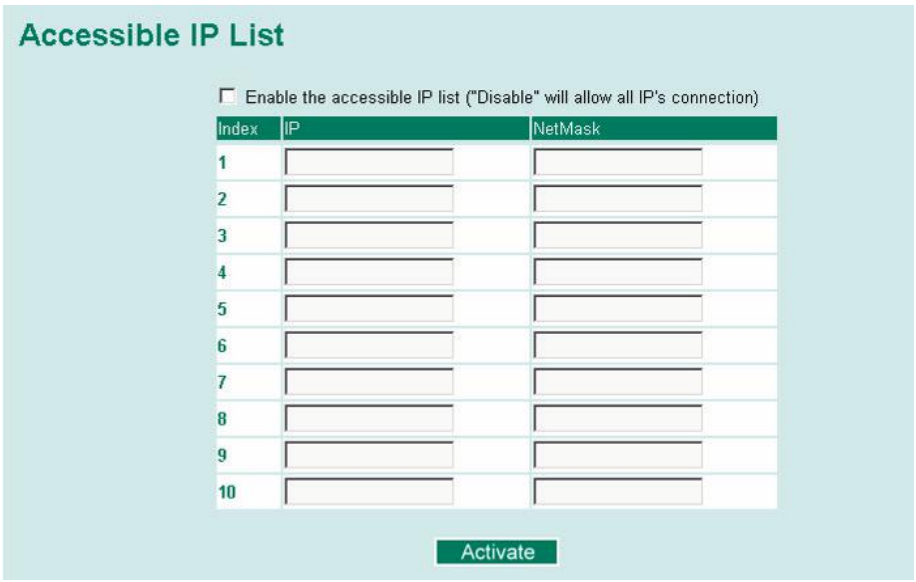
This function only applies to the following: EDS-405A/408A, EDS-505A/508A/510A/516A/518A, EDS-608/611/616/619, and EDS-P510, EDS-P510A Series.

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



Accessible IP List

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



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

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

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

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

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

- **Grant access to all hosts**

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

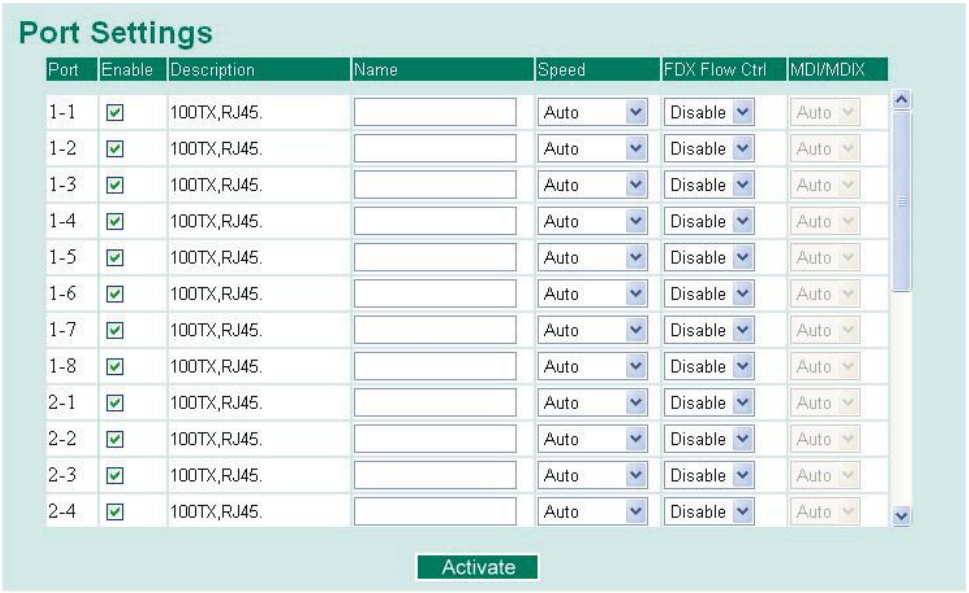
The following table shows additional configuration examples:

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

Port Settings

Ethernet Port Settings

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



Enable

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

ATTENTION

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

Description

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

Name

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

Speed

Setting	Description	Factory Default
Auto	Allows the port to use the IEEE 802.3u protocol to negotiate with connected devices. The port and connected devices will determine the best speed for that connection.	Auto
1G-Full	Choose one of these fixed speed options if the connected Ethernet device has trouble auto-negotiating for line speed.	
100M-Full		
100M-Half		
10M-Full		
10M-Half		

FDX Flow Ctrl

This setting enables or disables flow control for the port when the port's Speed is set to Auto. The final result will be determined by the Auto process between the Moxa switch and connected devices. Flow control should be enabled on both the ingress and egress ports of the Moxa switch as well as being enabled between both ends of the Moxa switch and the connected devices.

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

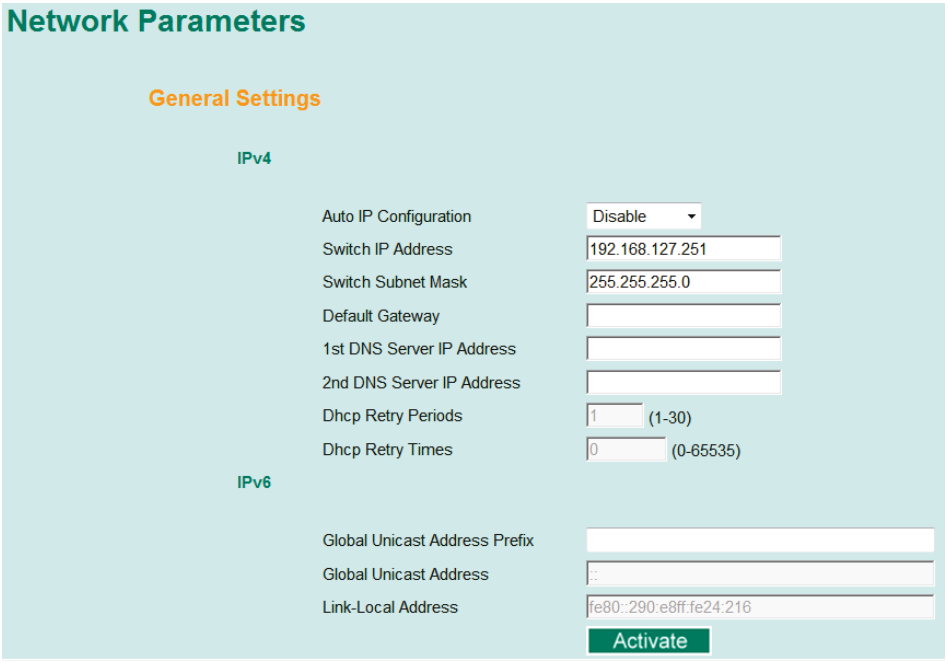
MDI/MDIX

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

Network Parameters

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

A brief explanation of each configuration item is given below.



IPv4

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

Auto IP Configuration

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

Switch IP Address

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

Switch Subnet Mask

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

Default Gateway

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

DNS IP Address

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

DHCP Retry Periods

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

DHCP Retry Times

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

IPv6

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

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

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

Global Unicast Address

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

Link-Local Address

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

Neighbor Cache

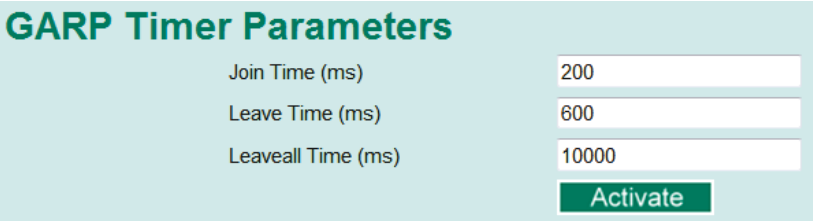
Setting	Description	Factory Default
None	The information in the neighbor cache that includes the neighboring node's IPv6 address, the corresponding Link-Layer address, and the current state of the entry.	None

GARP Timer Parameters

Generic Attribute Registration Protocol (GARP) was defined by the IEEE 802.1 working group to provide a generic framework. GARP defines the architecture, rules of operation, state machines, and variables for the registration and de-registration of attribute values.

The GARP Timer parameters are exchanged by creating the applications via GVRP (GARP VLAN Registration Protocol) to set the attributes of Timer.

Note that you need to set the same GARP timer values on all Layer 2 switches to ensure that the system works successfully.



Join Time

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

Leave Time

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

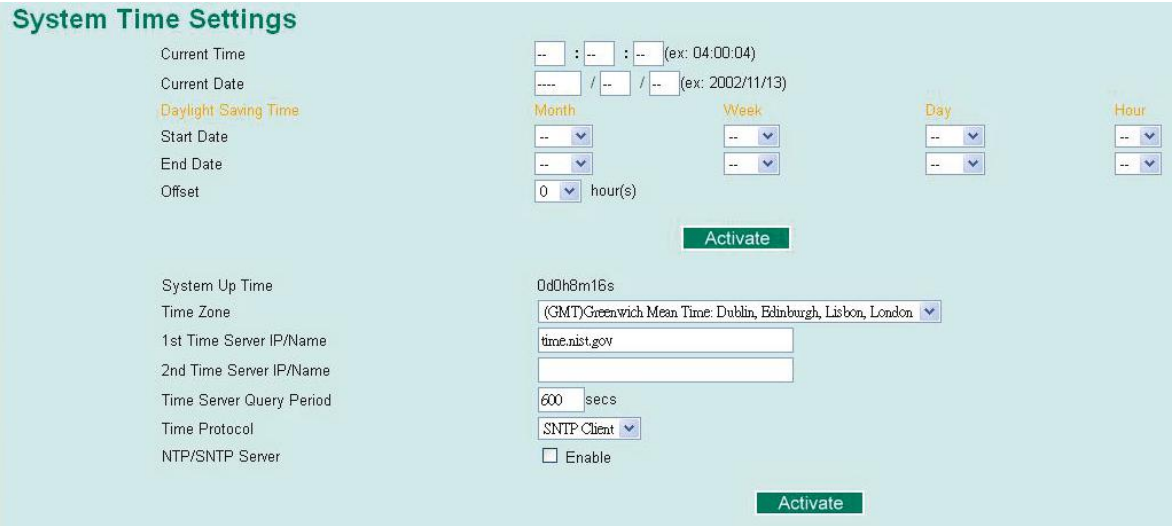
Leaveall Time

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

NOTE

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

System Time Settings



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

The list of models support real-time clock as shown in the table below:

Type	Models Supported
With real-time clock	EDS-405A-PTP, EDS-600/700/800 series, EDS-P510/P510A-8PoE, EDS-G509, IKS-6726/6726-8PoE/6728, IKS-G6524/G6824, ICS-G7000 series
Without real-time clock	EDS-400A series (except EDS-405A-PTP), EDS-505A/508A/510A/516A/518A, EDS-P506A-4PoE

NOTE

The user must update the Current Time and Current Date after rebooting the switch (even models with real-time clock will lose time information if shut down for a few days). The user must pay particular attention to this when there is no NTP server, LAN, or Internet connection.

Current Time

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

Current Date

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

Daylight Saving Time

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

Start Date

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

End Date

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

Offset

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

System Up Time

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

Time Zone

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

NOTE

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

Time Server IP/Name

Setting	Description	Factory Default
IP address or name of time server	The IP or domain address (e.g., 192.168.1.1, time.stdtime.gov.tw, or time.nist.gov).	None
IP address or name of secondary time server	The Moxa switch will try to locate the secondary NTP server if the first NTP server fails to connect.	

Time Server Query Period

Setting	Description	Factory Default
Time Server Query Period	Define the time period to query NTP server	600 sec

Time Protocol

Setting	Description	Factory Default
NTP	NTP (Network Time Protocol) is used to synchronize time with multiple time servers. The time accuracy is up to 50 ms.	-
SNTP	SNTP stands for Simple Network Time Protocol). The synchronization process of SNTP is simpler than NTP. The time accuracy is up to 1 second, which is suitable for low time accuracy requirements.	-

Enable NTP/SNTP Server

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

IEEE 1588 PTP

NOTE

IEEE 1588 PTP only supported in PTP models.

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

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

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

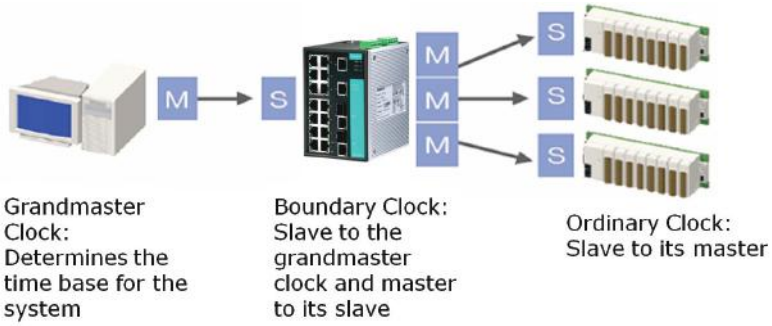
How does an Ethernet switch affect 1588 synchronization?

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

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

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

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



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

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

NOTE

If the CM-600-4TX-PTP module is not installed, then the EDS-600 only supports software-based IEEE 1588.

Configuring PTP

IEEE 1588/PTP Operation

Operation

Setting	Description	Factory Default
Enable PTP	Globally disables or enables IEEE 1588 operation.	Disabled

IEEE 1588/PTP Configuration

Clock Mode (sets the switch's clock mode)

Setting	Description	Factory Default
v1 BC	Operates as an IEEE 1588 v1 boundary clock.	v1 BC
v2 E2E 2-step TC	Operates as an edge-to-edge IEEE 1588 v2 transparent clock with 2-step method.	
v2 P2P 2-step TC	Operates as a peer-to-peer IEEE 1588 v2 transparent clock with 2-step method.	
v2 E2E BC	Operates as an edge-to-edge IEEE 1588 v2 boundary clock	
v2 P2P BC	Operates as a peer-to-peer IEEE 1588 v2 boundary clock	

logSyncInterval (sets the synchronization message time interval)

Setting	Description	Factory Default
0, 1, 2, 3, or 4	0 (1 s), 1 (2 s), 2 (4 s), 3 (8 s), or 4 (16 s). Supported in IEEE 1588 V1.	0
-3, -2, -1, 0, or 1	-3 (128 ms), -2 (256 ms), -1 (512 ms), 0 (1 s), or 1 (2 s). Supported in IEEE 1588 V2.	

logAnnounceInterval (sets the announce message interval)

Setting	Description	Factory Default
0, 1, 2, 3, or 4	0 (1 s), 1 (2 s), 2 (4 s), 3 (8 s), or 4 (16 s)	1 (2 s)

announceReceiptTimeout

Setting	Description	Factory Default
2, 3, 4, 5, 6, 7, 8, 9, or 10	The multiple of announce message receipt timeout by the announce message interval.	3

logMinDelayReqInterval

Setting	Description	Factory Default
0, 1, 2, 3, 4, or 5	Minimum delay request message interval	0 (1 sec.)

logMinPdelayReqInterval

Setting	Description	Factory Default
1, 0, 1, 2, 3, or 4	Minimal delay request message interval: -1 (512 ms), 0 (1 s), 1 (2 s), 2 (4 s), 3 (8 s), or 4 (32 s) (Available in Clock Mode: v2 P2P 2-step TC, and v2 P2P BC)	0 (1 sec)

Domain Number

Setting	Description	Factory Default
_DFLT (0), _ALT(1), _ALT(2), or _ALT(3)	Subdomain name (IEEE 1588-2002) or the domain Number (IEEE 1588-2008) fields in PTP messages	_DFLT (0)

Transport of PTP (transport protocol of an IEEE 1588 PTP message)

Setting	Description	Factory Default
IPv4 or 802.3/Ethernet	• IEEE 1588 PTP V1 supports IPv4 only • IEEE 1588 PTP V2 supports both IPv4 and IPv6.	IPv4

priority1

Setting	Description	Factory Default
0 to 255	Set first priority value; 0 = highest priority, 255 = lowest priority.	128

priority2

Setting	Description	Factory Default
0 to 255	Set second priority value; 0 = highest priority, 255 = lowest priority.	128

clockClass

Setting	Description	Factory Default
0 to 255	The clockClass attribute denotes the traceability of the time or frequency distributed by the grandmaster clock.	248

clockAccuracy

Setting	Description	Factory Default
0x21	The clockAccuracy characterizes a clock for the purpose of the best master clock (BMC) algorithm. This value is fixed at 0x21, which means the time of the EDS switch is accurate to within 100 ns.	0x21

Timescale

Setting	Description	Factory Default
PTP or ARB	• PTP timescale: In normal operation, the epoch is the PTP epoch and the timescale is continuous. The time unit is SI seconds, as realized on the rotating geoid (SI: International System). • ARB timescale: In normal operation, the epoch is set by an administrative procedure. The epoch can be reset during normal operation. Between invocations of the administrative procedure, the timescale is continuous. Additional invocations of the administrative procedure may introduce discontinuities in the overall timescale.	PTP

ARB Time

Setting	Description	Factory Default
0 to 255	The geoid of the PTP clock reference time (seconds).	0

Leap59

Setting	Description	Factory Default
True or False	The last minute of the current UTC day contains 59 seconds. If the epoch is not PTP, the value will be set to FALSE.	False

Leap61

Setting	Description	Factory Default
True or False	The last minute of the current UTC day contains 61 seconds. If the epoch is not PTP, the value will be set to FALSE.	False

UTC Offset Valid

Setting	Description	Factory Default
True or False	The initialization value will be TRUE if the value of the current UTC offset is known to be correct; otherwise, it will be FALSE.	False

UTC Offset

Setting	Description	Factory Default
0 to 255	The known UTC offset (seconds).	0

Status

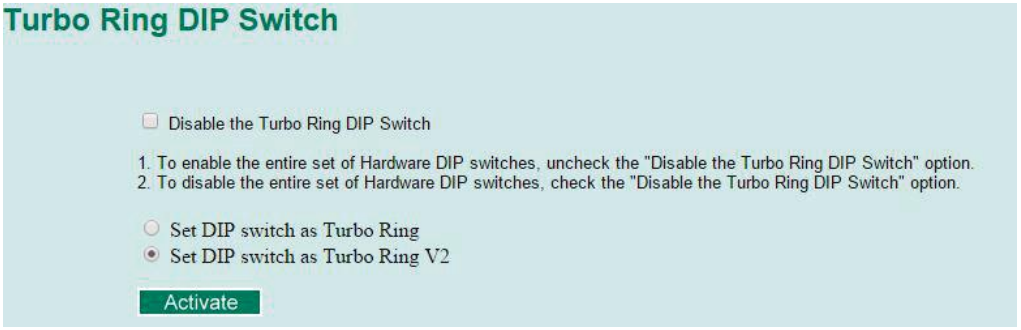
Setting	Description	Factory Default
N/A	Shows the current IEEE 1588 PTP status.	N/A

PTP Port Settings

Shows the current switch PTP port settings.

Turbo Ring DIP Switch

The **Turbo Ring DIP Switch** page allows users to disable the 4th DIP switch located on the EDS's outer casing. The default is enabled with Turbo Ring v2 protocol. Once the user changes the 4th hardware DIP switch configuration to **ON**, the switch will start to initiate the Turbo Ring redundancy protocol based on the configuration. The detailed description is given below:



Setting	Description	Factory Default
Disable the Turbo Ring DIP switch	**Unchecked:** The Turbo Ring protocol will be activated automatically when the 4th DIP switch is moved to the ON position.	unchecked
	Checked: The Turbo Ring protocol will not be activated automatically, regardless of the position of the 4th DIP switch.	
Set DIP switch as Turbo Ring	If the DIP switch is enabled, Turbo Ring protocol will be enabled when the DIP switch is moved to the ON position.	Set DIP switch as Turbo Ring v2
Set DIP switch as Turbo Ring v2	If the DIP switch is enabled, Turbo Ring v2 protocol will be enabled when the DIP switch is moved to the ON position.	

NOTE

If the 4th DIP switch (Turbo Ring) is configured to ON, you will not be able to disable the Turbo Ring DIP switch from the web interface, console, or Telnet.

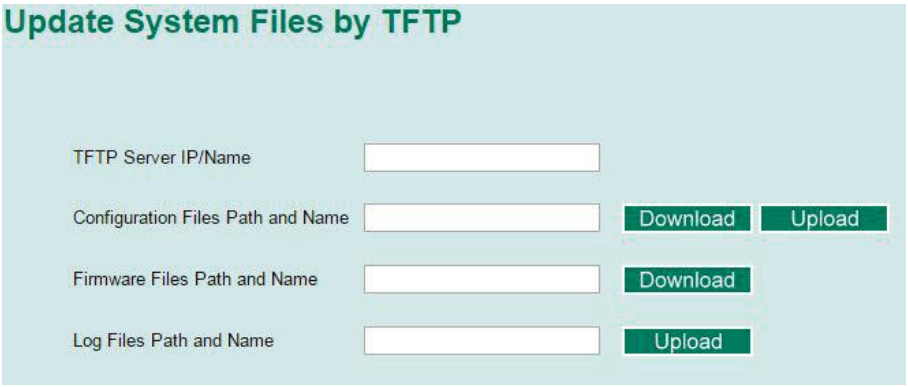
NOTE

If you would like to enable VLAN and/or port trunking on any of the last four ports, do not use the fourth DIP switch to activate Turbo Ring. In this case, you should use the Web, Telnet, or Serial console to activate Turbo Ring.

System File Update

Update System Files by Remote TFTP

The Moxa switch supports saving your configuration or log file to a remote TFTP server or local host. Other Moxa switches can also load the configuration at a later time. The Moxa switch also supports loading firmware or configuration files from the TFTP server or a local host.



TFTP Server IP/Name

Setting	Description	Factory Default
IP address of TFTP server	Specifies the IP address or name of the remote TFTP server. Must be specified before downloading or uploading files.	None

Configuration Files Path and Name

Setting	Description	Factory Default
Max. 40 characters	Specifies the path and file name of the Moxa switch's configuration file on the TFTP server.	None

Firmware Files Path and Name

Setting	Description	Factory Default
Max. 40 characters	Specifies the path and file name of the Moxa switch's firmware file.	None

Log Files Path and Name

Setting	Description	Factory Default
Max. 40 characters	Specifies the path and file name of the Moxa switch's log file.	None

After setting the desired paths and file names, click **Download** to download the prepared file from the remote TFTP server, or click **Upload** to upload the desired file to the remote TFTP server.

Update System Files from Local PC

Configuration File

Click **Export** to save the Moxa switch's configuration file to the local host.

Log File

Click **Export** to save the Moxa switch's log file to the local host.

> **NOTE**
>
> Some operating systems will open the configuration file and log file directly in the web page. In such cases, right click the Export button to save the file.

Upgrade Firmware

To import a new firmware file into the Moxa switch, click **Browse** to select the firmware file that is saved on your computer. The upgrade procedure will proceed automatically after clicking **Import**.

Upload Configure Data

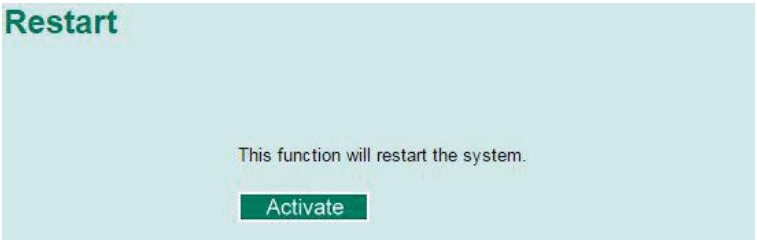
To import a configuration file into the Moxa switch, click **Browse** to select the configuration file already saved on your computer. The upgrade procedure will proceed automatically after clicking **Import**.

ABC (Auto-Backup Configurator) Configuration

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

Restart

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



Reset to Factory Default

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

NOTE

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

Loop Protection

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

Check the Enable box and click Activate to enable the Loop protection.

Enable Loop Protection

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

Using Port Trunking

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

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

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

The Port Trunking Concept

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

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

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

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

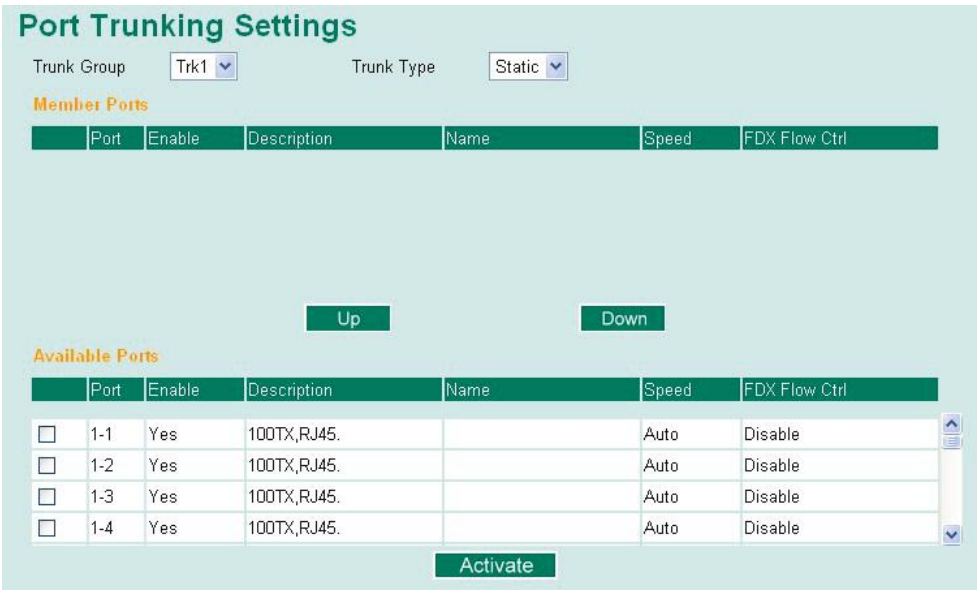
Each Moxa switch can set a maximum of 4 port trunking groups. When you activate port trunking, certain settings on each port will be reset to factory default values or disabled:

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

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

Port Trunking Settings

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



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

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

Step 3: Select the desired ports under **Available Ports** and click **Up** to add to the Trunk Group.

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

Trunk Group (maximum of 4 trunk groups)

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

The EDS 400A series does not support Port Trunking. The number of Trunk Groups for other models are listed in the following table:

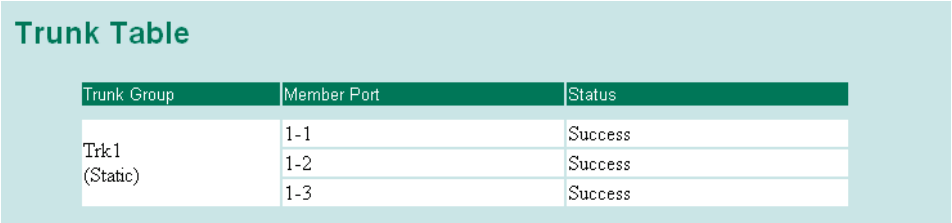
No. of Trunk Groups	Model
2	EDS-505A, EDS-P506A-4PoE, EDS-516A
3	EDS-518A
4	For other models

Trunk Type

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

Available Ports/Member Ports

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



Trunk Table

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

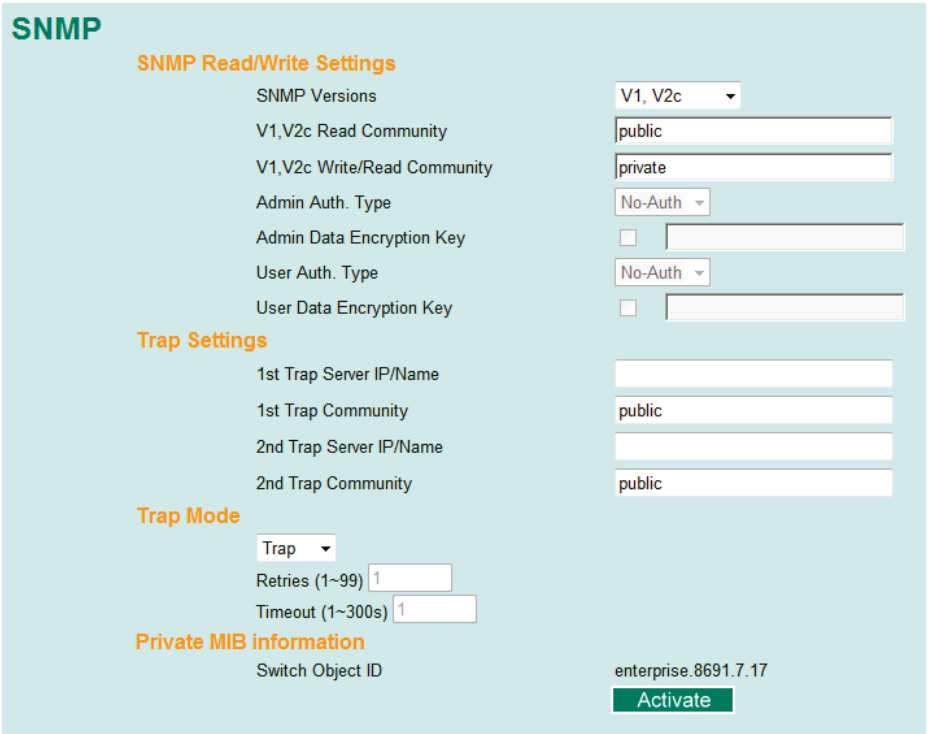
Configuring SNMP

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

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

Protocol Version	UI Setting	Authentication	Encryption	Method
SNMP V1, V2c	V1, V2c Read Community	Community string	No	Uses a community string match for authentication.
	V1, V2c Write/Read Community	Community string	No	Uses a community string match for authentication.
SNMP V3	No-Auth	No	No	Uses an account with admin or user to access objects
	MD5 or SHA	Authentication based on MD5 or SHA	No	Provides authentication based on HMAC-MD5, or HMAC-SHA algorithms. 8-character passwords are the minimum requirement for authentication.
	MD5 or SHA	Authentication based on MD5 or SHA	Data encryption key	Provides authentication based on HMAC-MD5 or HMAC-SHA algorithms, and data encryption key. 8-character passwords and a data encryption key are the minimum requirements for authentication .and encryption.

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



SNMP Read/Write Settings

SNMP Versions

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

V1, V2c Read Community

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

V1, V2c Write/Read Community

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

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

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

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

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

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

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

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

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

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

NOTE

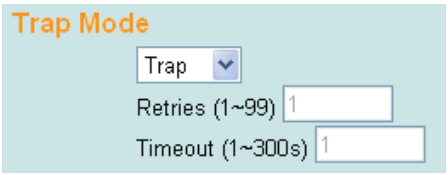
When changing the SNMP version, the data encryption key information will be cleared. Therefore, when changing to SNMP V3, the data encryption key should be entered again.

Trap Settings

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

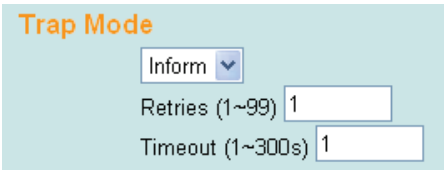
SNMP Trap Mode—Trap

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



SNMP Trap Mode—Inform

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



1st Trap Server IP/Name

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

1st Trap Community

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

2nd Trap Server IP/Name

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

2nd Trap Community

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

Private MIB Information

Switch Object ID

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

NOTE

The Switch Object ID cannot be changed.

Using PoE (PoE Models Only)

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

Power over Ethernet can be used with:

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

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

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

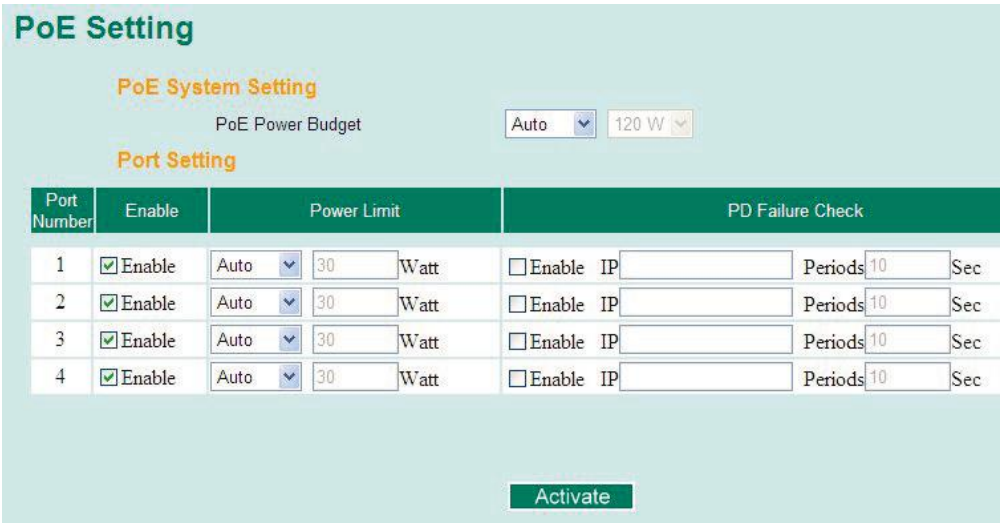
Type	Models Supported
Type 1	EDS-P510, EDS-P506A-4PoE, IKS-6726-8PoE
Type 2	EDS-P510A-8PoE, IKS-6728-8PoE-4GTXSFP

Type 1

PoE Setting

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

An explanation of each configuration item follows:



PoE Power Budget

Indicates the PoE power that can be supplied by the system

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

Port Setting

Enable

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

Power Limit

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

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

PD Failure Check

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

IP

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

Period

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

PoE Timetabling

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

Port

Setting	Description	Factory Default
Port	Enable a dedicated port	Port 1

Enable

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

Weekly Timetabling

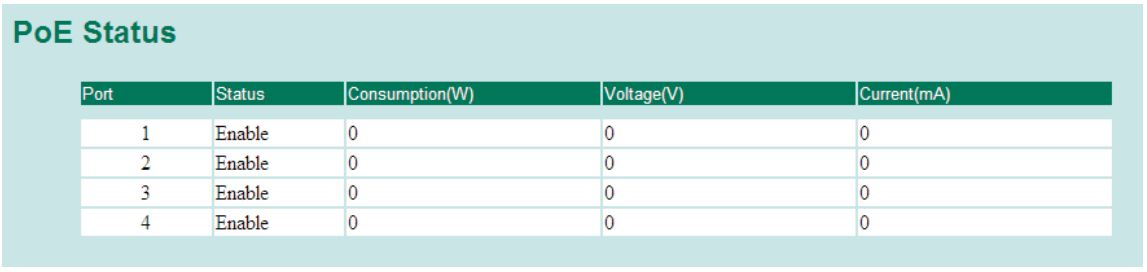
Day

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

Start/End Time

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

PoE Status



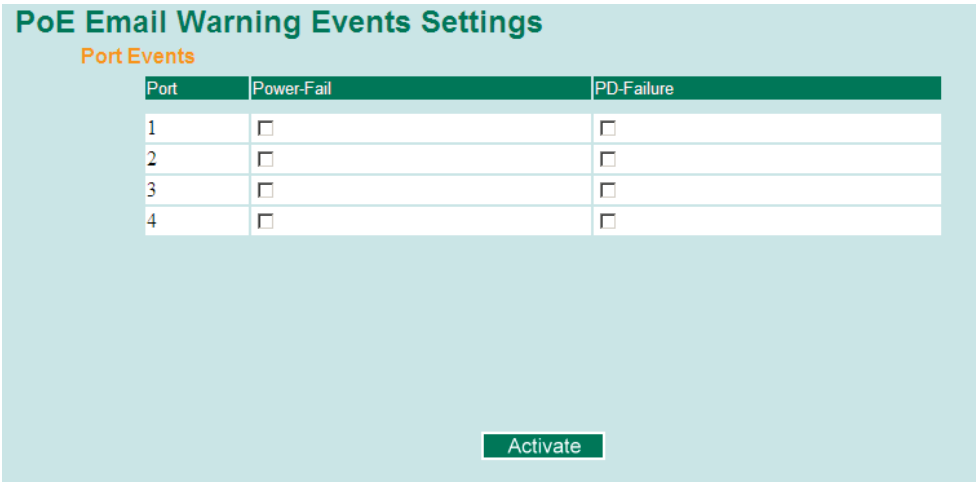
Item	Description
Enable/Disable	Indicates the PoE port status
Consumption (W)	Indicates the actual Power consumed value for PoE port
Voltage (V)	Indicates the actual Voltage consumed value for PoE port
Current (mA)	Indicates the actual Current consumed value for PoE port

PoE Email Warning Events Settings

Since industrial Ethernet devices are often located at the endpoints of a system, these devices do not always know what is happening elsewhere on the network. This means that a PoE port connected to a PD must provide system administrators with real-time alarm messages. Even when control engineers are out of the control room for an extended period of time, they can still be informed of the status of the PD almost instantaneously when exceptions occur. The PoE Ethernet switch supports different methods for warning

engineers automatically, such as email and relay output. It also supports two digital inputs to integrate sensors into your system to automate alarms using email and relay output.

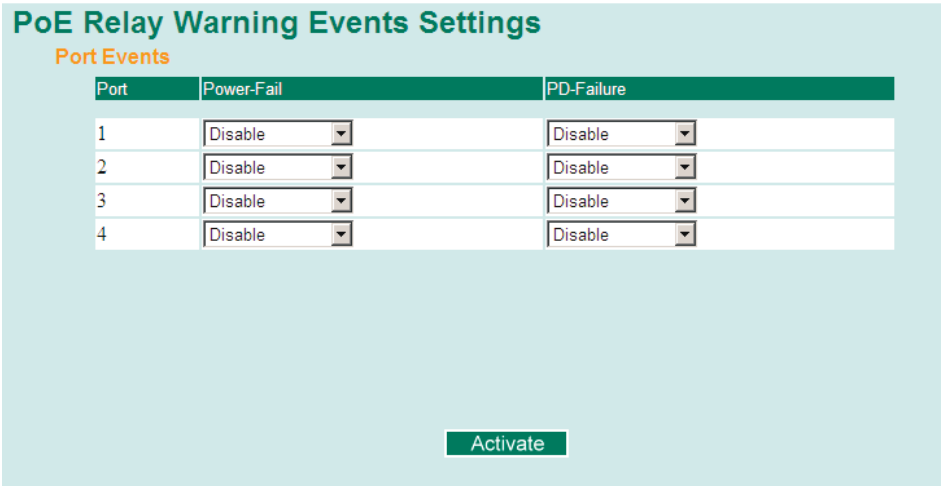
Email Warning Event Types can be divided into two basic groups: Power-Fail and PD-Failure.



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

PoE Relay Warning Events Settings

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



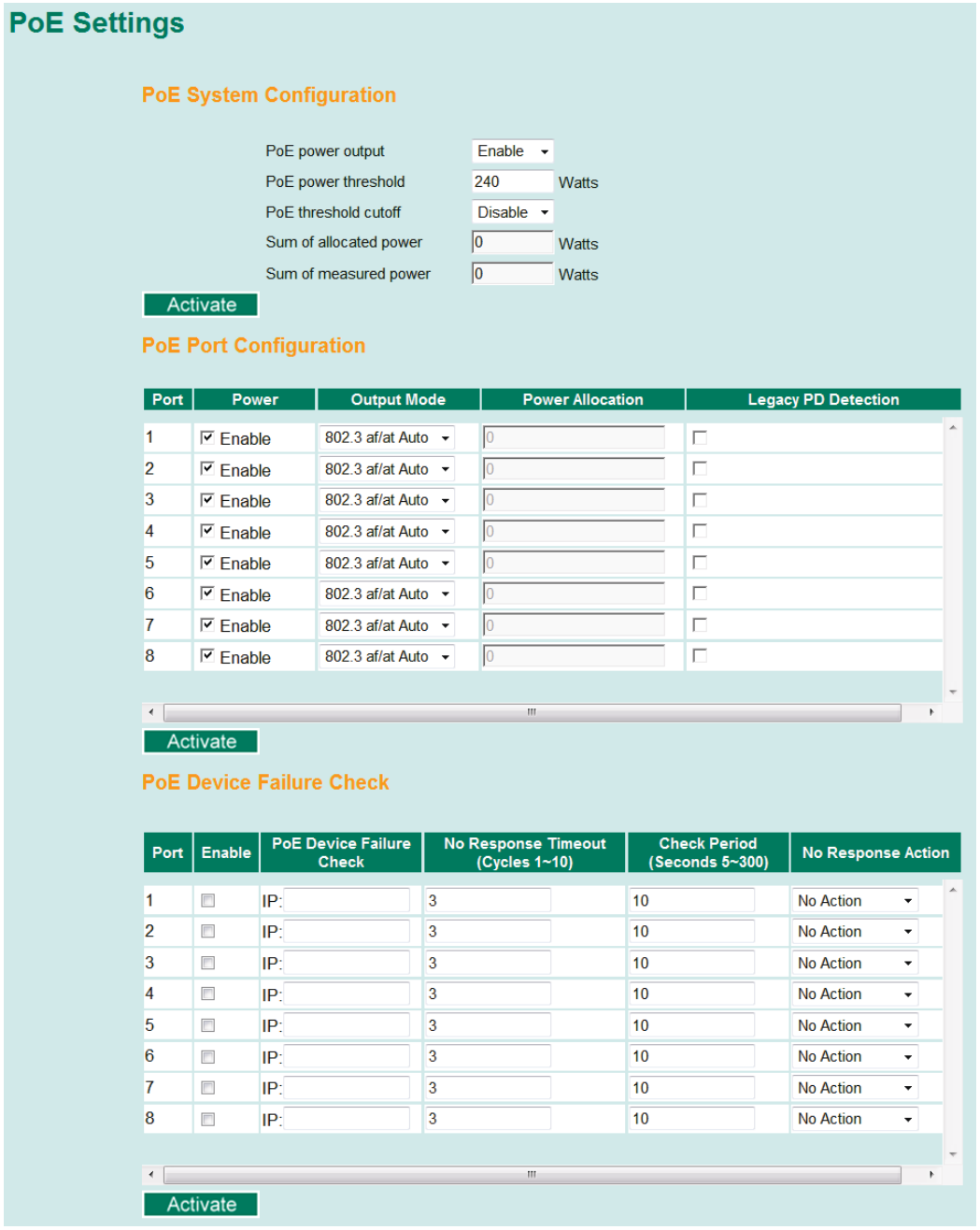
Port Events	Warning e-mail is sent when...
Power-Fail	When actual PD power consumption exceeds related PD power limit settings.
PD-Failure	When the switch cannot receive a PD response after the defined period.

Type 2

PoE Setting

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

An explanation of each configuration item follows:



PoE System Configuration

PoE power output

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

PoE power threshold

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

PoE threshold cutoff

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

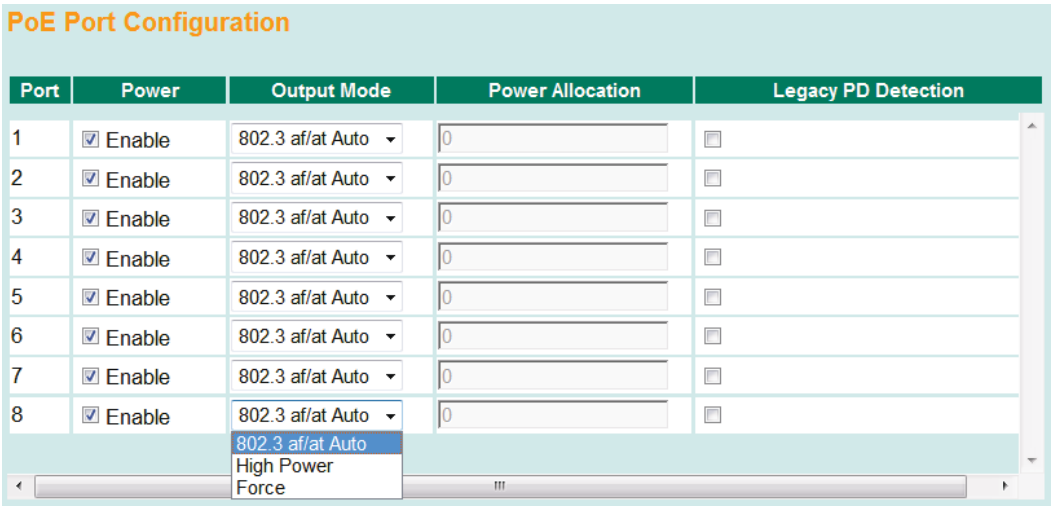
Sum of allocated power

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

Sum of measured power

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

PoE Port Configuration



Power

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

Output Mode

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

Power Allocation

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

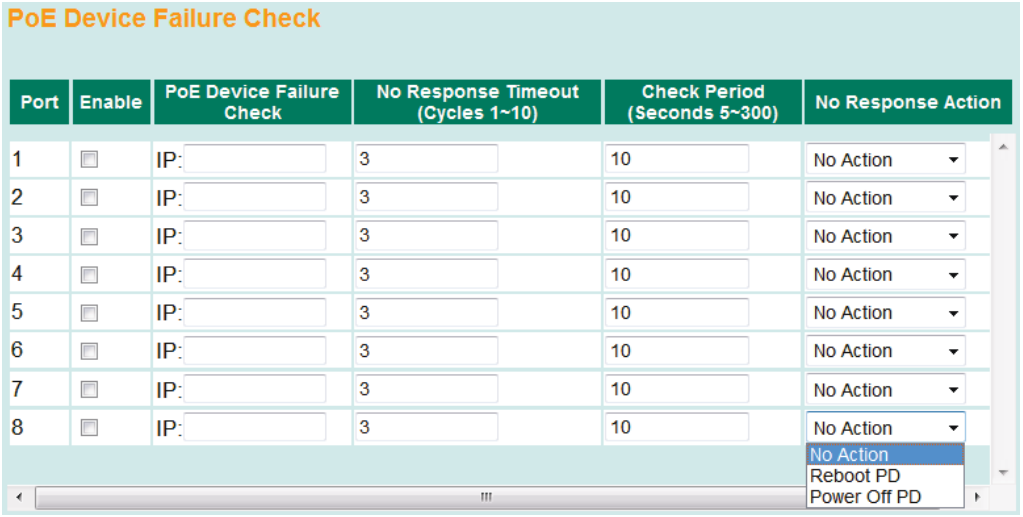
Legacy PD Detection

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

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

PoE Device Failure Check

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



Enable

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

PoE Device IP Address

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

No Response Timeout

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

Check Period

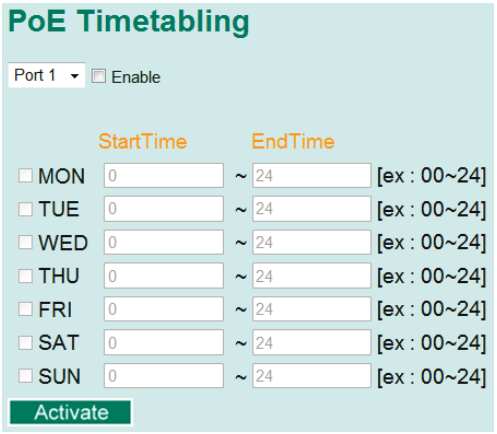
Setting	Description	Factory Default
5 to 300	Enter the time span for IP checking period	10

No Response Action

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

PoE Timetabling

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



Port

Setting	Description	Factory Default
Port	Enable a dedicated port	Port 1

Enable

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

Weekly Timetabling

Day

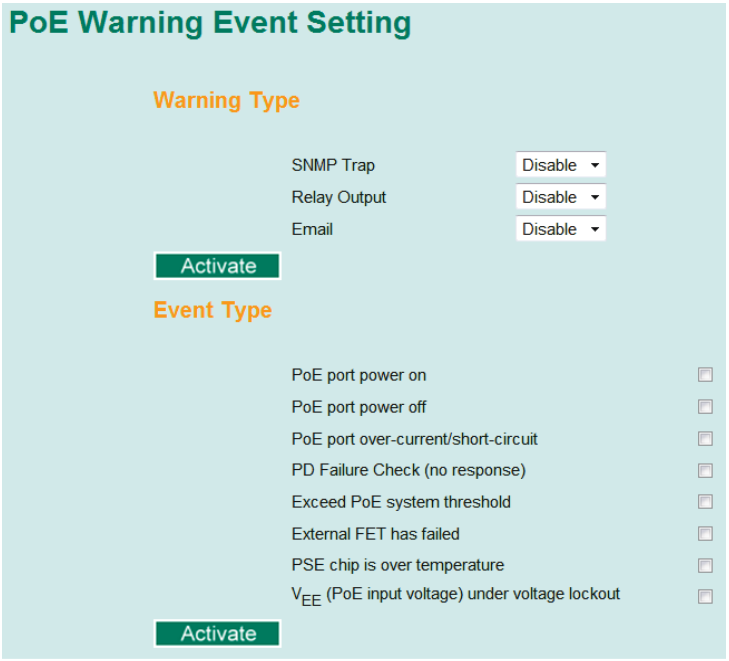
Setting	Description	Factory Default
Checked	Enables the port for a defined number of days	Disable
Unchecked	Disables the port for a defined number of days	

Start/End Time

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

PoE Warning Event Setting

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



Warning Type

SNMP Trap

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

Relay Output

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

Email

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

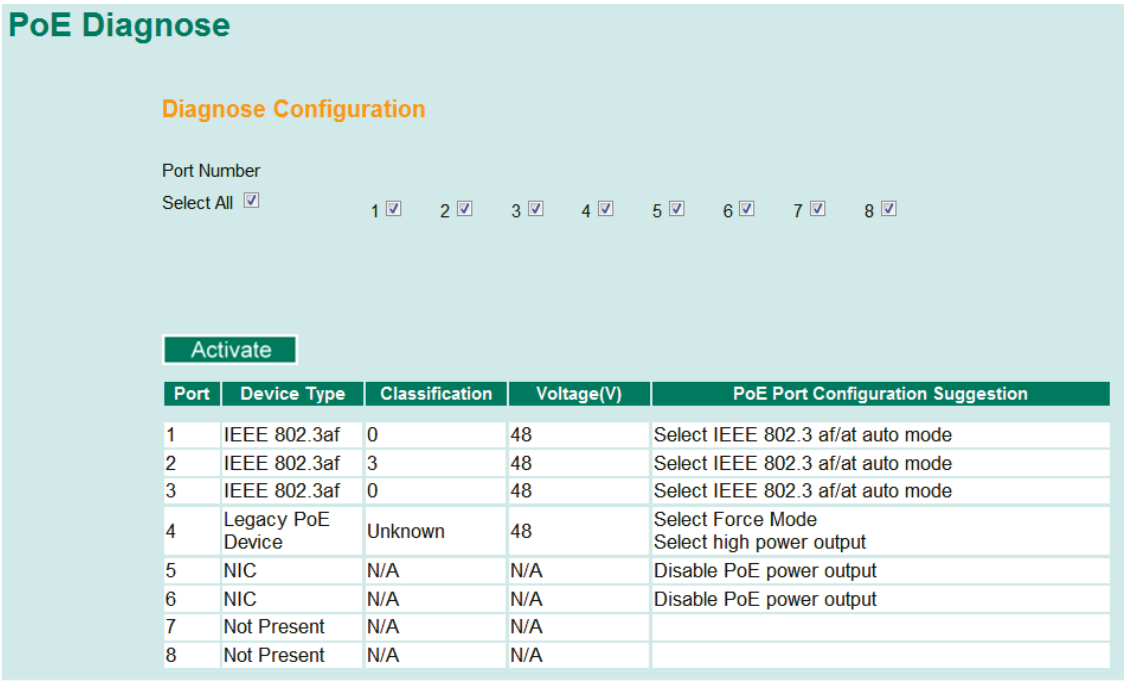
Event Type

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

NOTE

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

PoE Diagnose



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

Following steps help users to diagnose the PD conditions:

Step 1: Check the port numbers which will be diagnosed

Step 2: Click Activate

Step 3: The system shows the selected PD conditions

Diagnose Configuration

Port Number

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

Device Type

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

Classification

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

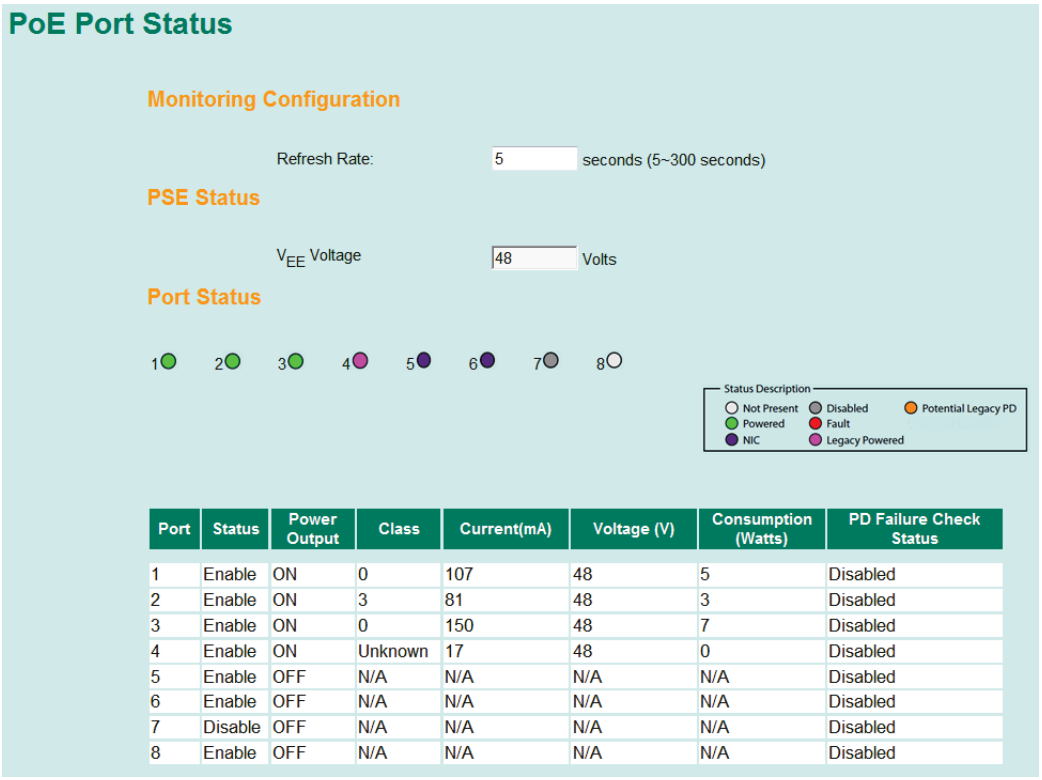
Voltage (V)

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

PoE Port Configuration Suggestion

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

PoE Port Status



Port	Status	Power Output	Class	Current(mA)	Voltage (V)	Consumption (Watts)	PD Failure Check Status
1	Enable	ON	0	107	48	5	Disabled
2	Enable	ON	3	81	48	3	Disabled
3	Enable	ON	0	150	48	7	Disabled
4	Enable	ON	Unknown	17	48	0	Disabled
5	Enable	OFF	N/A	N/A	N/A	N/A	Disabled
6	Enable	OFF	N/A	N/A	N/A	N/A	Disabled
7	Disable	OFF	N/A	N/A	N/A	N/A	Disabled
8	Enable	OFF	N/A	N/A	N/A	N/A	Disabled

Monitoring Configuration

Refresh Rate

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

PSE Status

VEE Voltage

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

Port Status

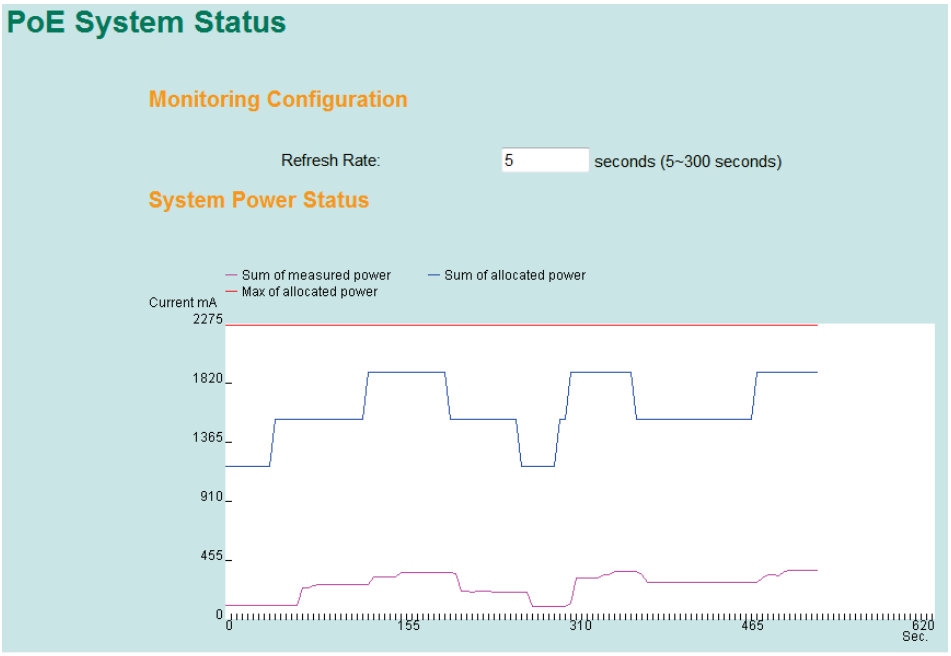
Status Description

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

Port Description

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

PoE System Status



Monitoring Configuration

Refresh Rate

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

System Power Status

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

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

Using Traffic Prioritization

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

The Traffic Prioritization Concept

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

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

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

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

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

IEEE 802.1D Traffic Marking

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

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

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

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

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

Differentiated Services (DiffServ) Traffic Marking

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

The advantages of DiffServ over IEEE 802.1D are:

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

Traffic Prioritization

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

- 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.

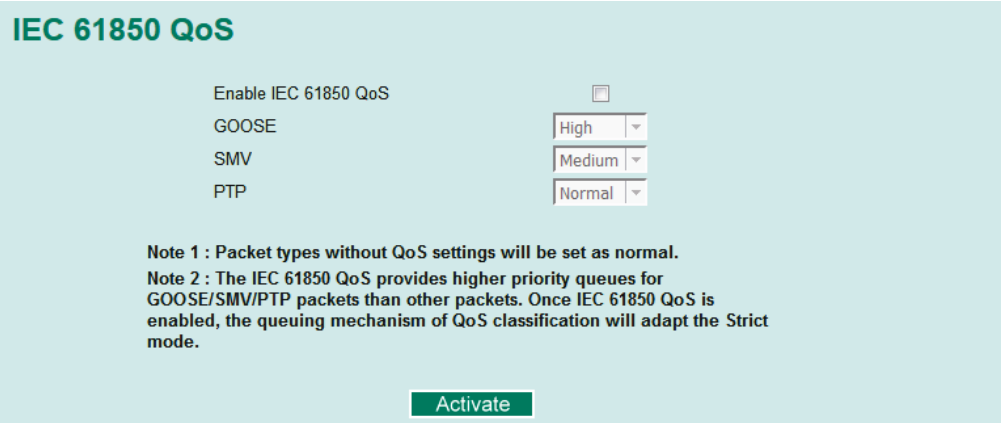
Configuring Traffic Prioritization

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

IEC 61850 QoS

IEC 61850 QoS (Quality of Service) is an application-based communications prioritization function that can prioritize critical messages, which are sent with the GOOSE/SMV/PTP protocols in power substations. In comparison, **QoS Classification** can only use port-based message prioritization.

Supported Models
PT-7728 Series, PT-7828 Series, PT-7728-PTP Series (Firmware V3.4)



Enable Packet Priority

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

GOOSE

Setting	Description	Factory Default
High/Medium/Normal/Low	The priority sequence is High>Medium>Normal>Low. We recommend setting GOOSE packets to high priority.	High

SMV

Setting	Description	Factory Default
High/Medium/Normal/Low	The priority sequence is High>Medium>Normal>Low. We recommend setting SMV packets to high priority.	Medium

PTP

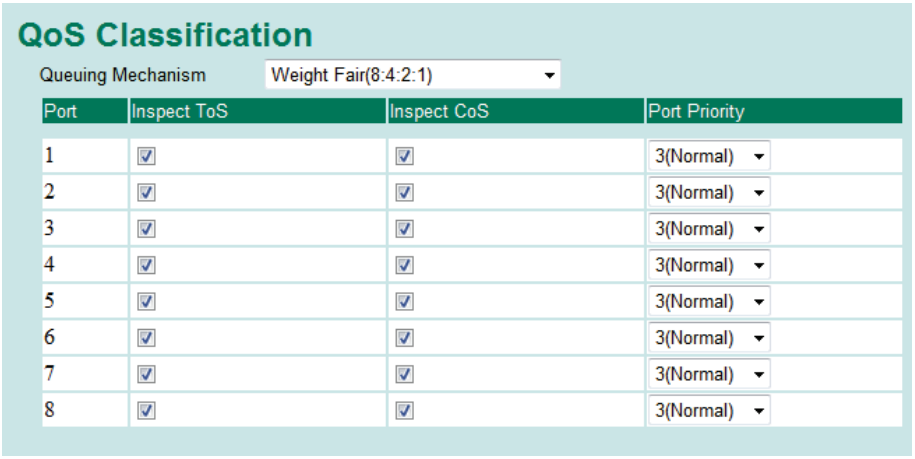
Setting	Description	Factory Default
High/Medium/Normal/Low	The priority sequence is High>Medium>Normal>Low.	Normal

QoS Classification

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

Type	Models Supported
Type 1	EDS-400A Series, EDS-505A/508A/510A/G509, EDS-P506A-4PoE/P510/P510A-8PoE, EDS-600 Series, IKS-G6524/G6824, ICS-G7000 Series, PT-508, PT-510, PT-7710 Series
Type 2	EDS-516A/518A, EDS-728/828, IKS-6726/6726-8PoE/6728, PT-7528, PT-7728, PT-7828, PT-7728-PTP

Type 1



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

Queuing Mechanism

Setting	Description	Factory Default
Weight Fair	The Moxa switch has 4 priority queues. In the weight fair scheme, an 8, 4, 2, 1 weighting is applied to the four priorities. This approach prevents the lower priority frames from being starved of opportunity for transmission with only a slight delay to the higher priority frames.	Weight Fair
Strict	In the Strict-priority scheme, all top-priority frames egress a port until that priority's queue is empty, and then the next lower priority queue's frames egress. This approach can cause the lower priorities to be starved of opportunity for transmitting any frames but ensures that all high priority frames will egress the switch as soon as possible.	

Inspect TOS

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

Inspect COS

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

Inspect Port Priority

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

NOTE

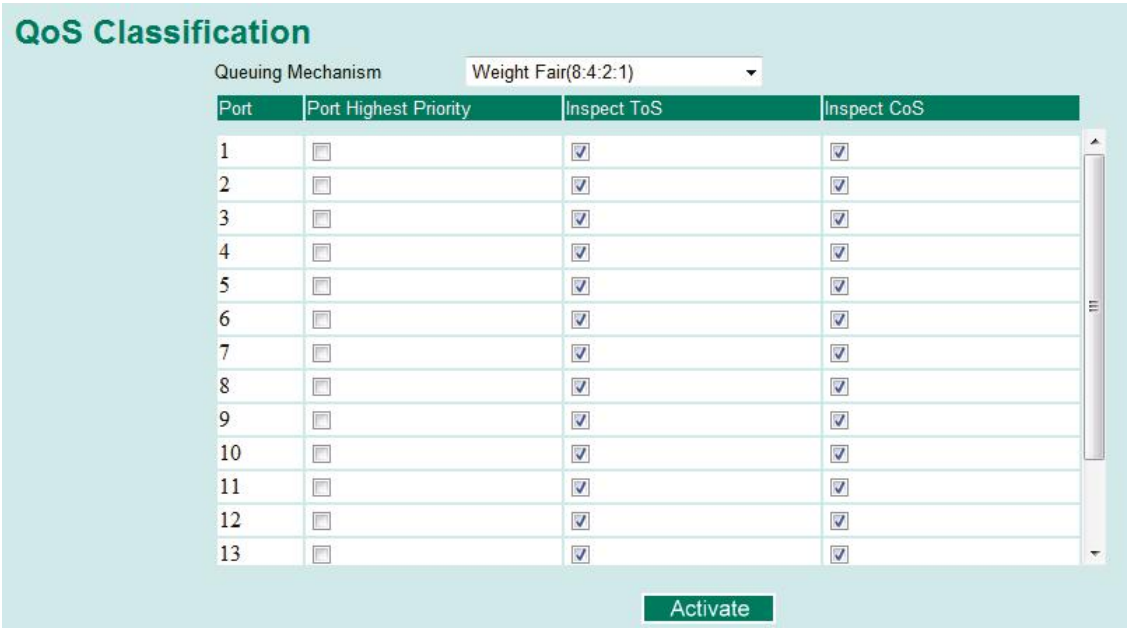
The priority of an ingress frame is determined in the following order:

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

NOTE

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

Type 2



Queuing Mechanism

Setting	Description	Factory Default
Weight Fair	The Moxa switch has 4 priority queues. In the weight fair scheme, an 8, 4, 2, 1 weighting is applied to the four priorities. This approach prevents the lower priority frames from being starved of opportunity for transmission with only a slight delay to the higher priority frames.	Weight Fair
Strict	In the Strict-priority scheme, all top-priority frames egress a port until that priority's queue is empty, and then the next lower priority queue's frames egress. This approach can cause the lower priorities to be starved of opportunity for transmitting any frames but ensures that all high priority frames will egress the switch as soon as possible.	

Inspect Port Highest Priority

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

Inspect TOS

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

Inspect COS

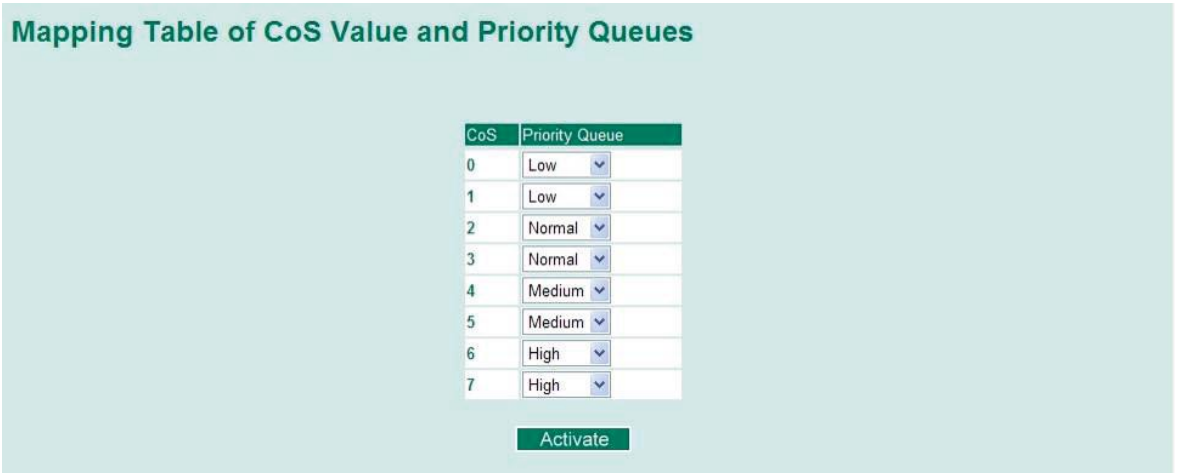
Setting	Description	Factory Default
Enable/Disable	Enables or disables the Moxa switch for inspecting 802.1p COS tags in the MAC frame to determine the priority of each frame.	Enabled

NOTE

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

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

CoS Mapping



CoS Value and Priority Queues

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

TOS/DiffServ Mapping

ToS (DSCP) Value and Priority Queues

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

Using Virtual LAN

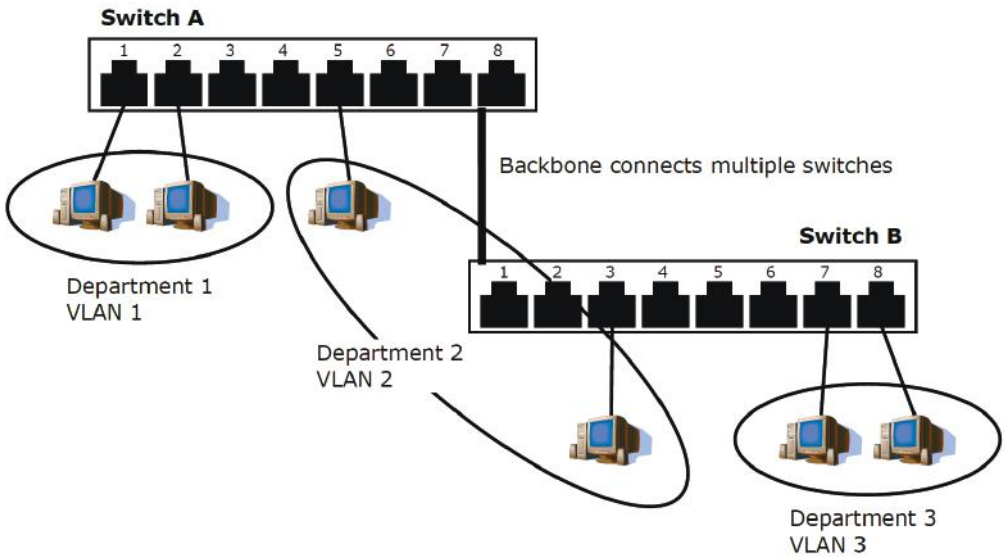
Setting up Virtual LANs (VLANs) on your Moxa switch increases the efficiency of your network by dividing the LAN into logical segments, as opposed to physical segments. In general, VLANs are easier to manage.

The Virtual LAN (VLAN) Concept

What is a VLAN?

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

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



Benefits of VLANs

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

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

VLANs and the Rackmount switch

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

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

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

Managing a VLAN

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

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

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

Communication Between VLANs

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

VLANs: Tagged and Untagged Membership

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

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

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

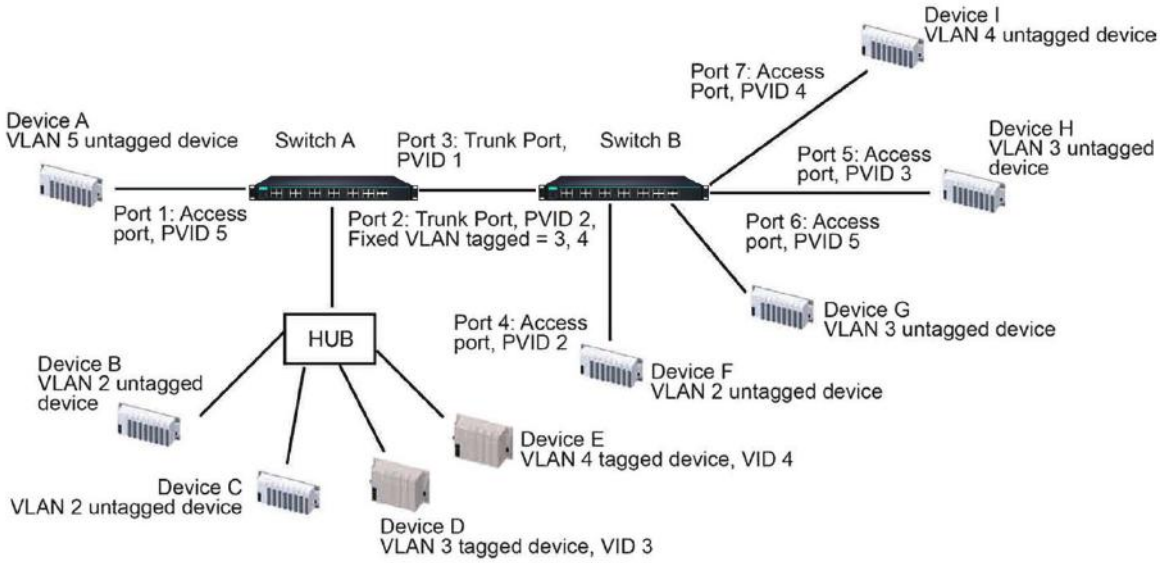
To carry multiple VLANs across a single physical link (backbone, trunk), each packet must be tagged with a VLAN identifier so that the switches can identify which packets belong in which VLAN. To communicate between VLANs, a router must be used.

The Moxa switch supports three types of VLAN port settings:

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

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

Sample Applications of VLANs Using Moxa Switches



In this application,

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

After the application is properly configured:

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

Configuring Virtual LAN

VLAN Settings

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

VLAN Mode

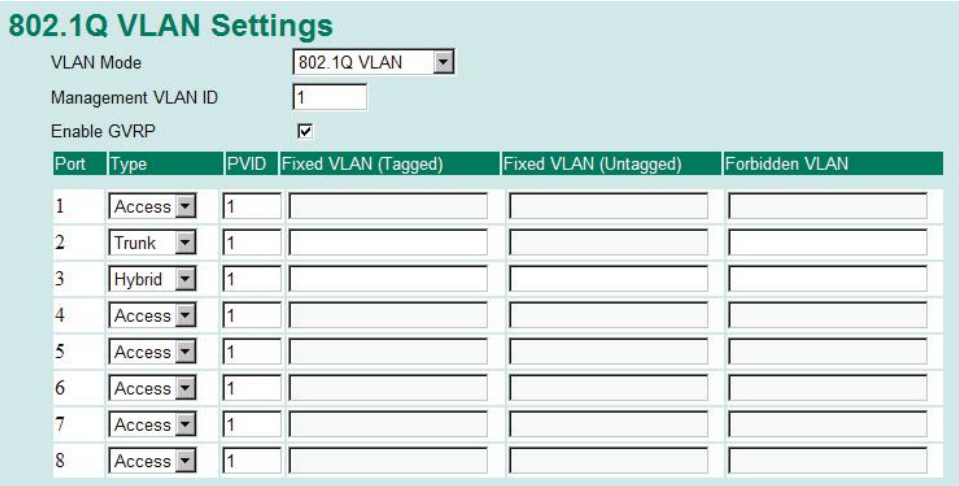
Setting	Description	Factory Default
802.1Q VLAN	Set VLAN mode to 802.1Q VLAN	802.1Q VLAN
Port-based VLAN	Set VLAN mode to Port-based VLAN	
Unaware VLAN	Set VLAN mode to Unaware VLAN	

NOTE

The following models support the Unaware VLAN function.

- EDS-728
- IKS-6726/6728
- PT-508/510, PT-7710, PT-G7509, PT-7728, PT-7528

802.1Q VLAN Settings



Management VLAN ID

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

Port Type

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

ATTENTION

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

Port PVID

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

Fixed VLAN List (Tagged)

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

Fixed VLAN List (Untagged)

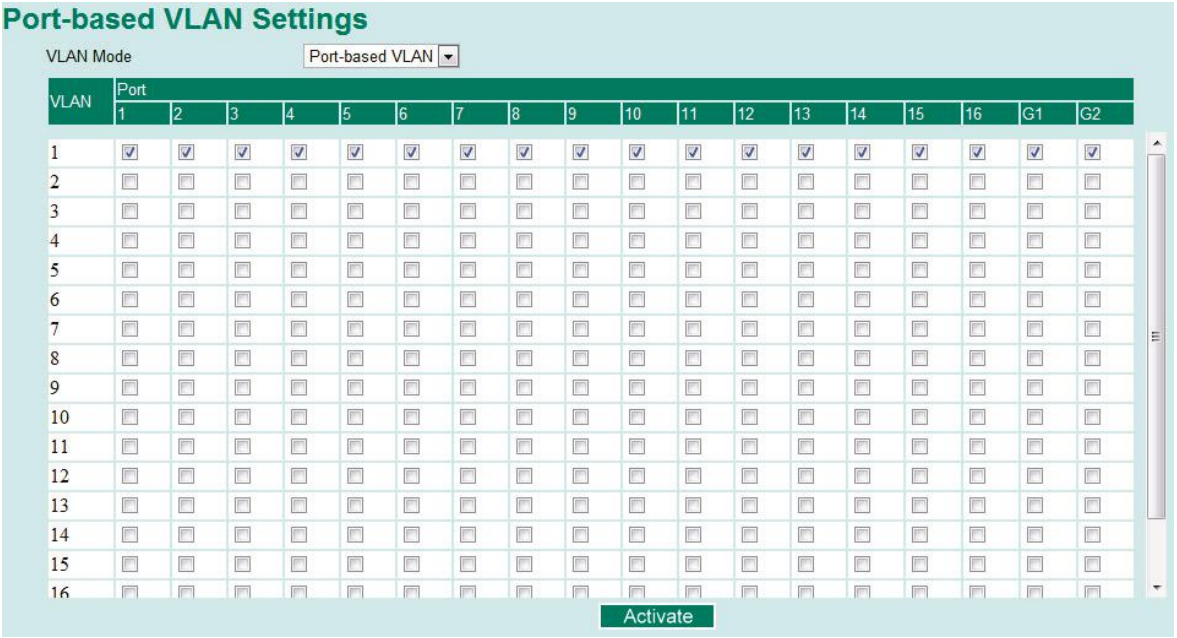
Setting	Description	Factory Default
VID range from 1 to 4094	This field will be active only when selecting the Hybrid port type. Set the other VLAN ID for tagged devices that connect to the port and tags that need to be removed in egress packets. Use commas to separate different VIDs.	None

Forbidden VLAN List

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

Port-Based VLAN Settings

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



NOTE

Port-Based VLAN is supported by:

- EDS series switches (not including the EDS-728/828)
- IKS-6726A/6728A

Port-Based VLAN is NOT supported by:

- EDS-728/828
- IKS-G6524A/G6824A
- ICS series switches

NOTE

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

Unaware VLAN Settings

The **Unaware VLAN** function provides users a flexible operation in a VLAN network. Switches which are set on **Unaware VLAN** mode do not check the VLAN tags of input Ethernet frame. All of VLAN tags can always in and out of the **Unaware VLAN** switch, and the switch won't affect the VLAN tags of Ethernet frames.

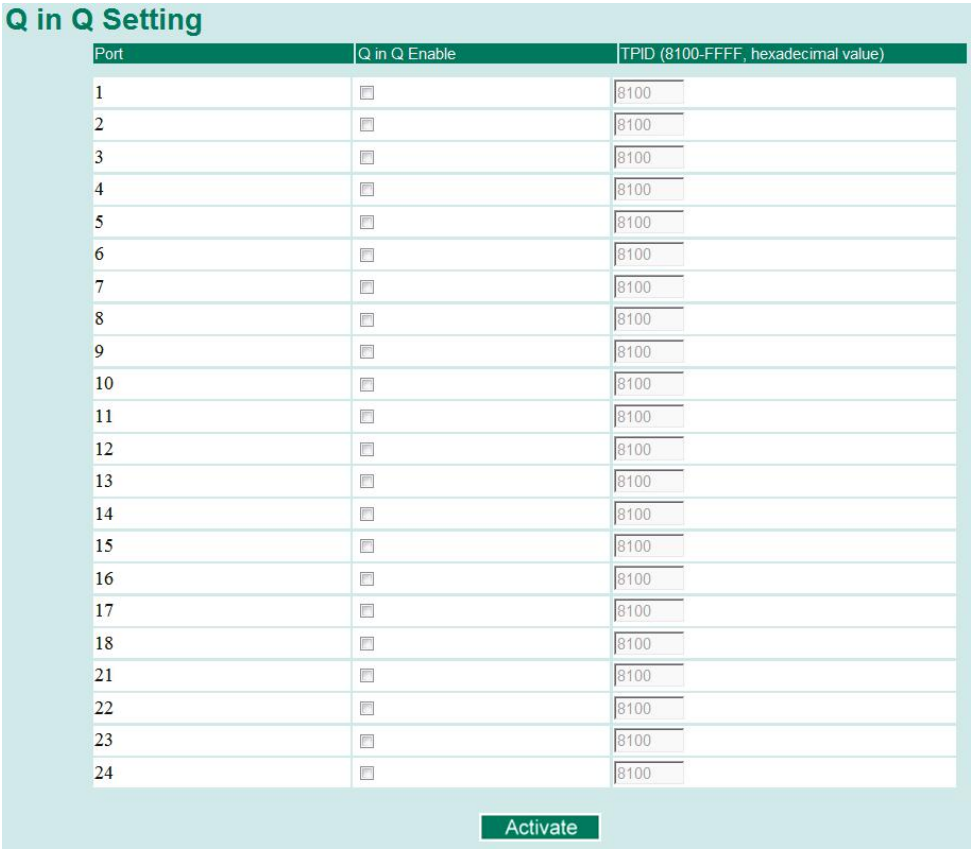
NOTE

When users enable Unaware VLAN function, all of ports are set as unaware VLAN ports.

QinQ Setting

NOTE

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



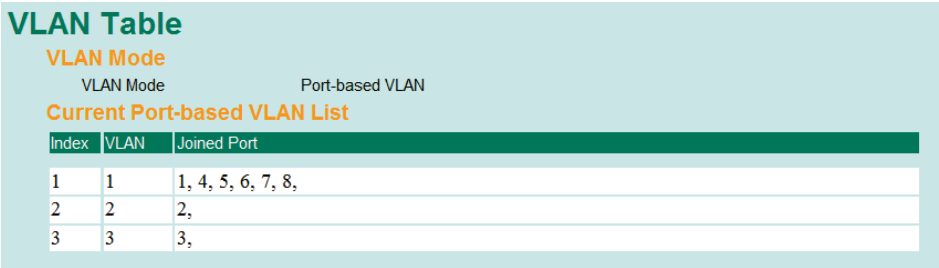
QinQ Enable

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

TPID

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

VLAN Table



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

NOTE

Most Moxa managed switches have a maximum of 64 VLAN settings. However, the IKS-G6524/G6824 and ICS-G7000 series support up to 256 VLAN settings.

Using Multicast Filtering

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

The Concept of Multicast Filtering

What is an IP Multicast?

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

Benefits of Multicast

The benefits of using IP multicast are:

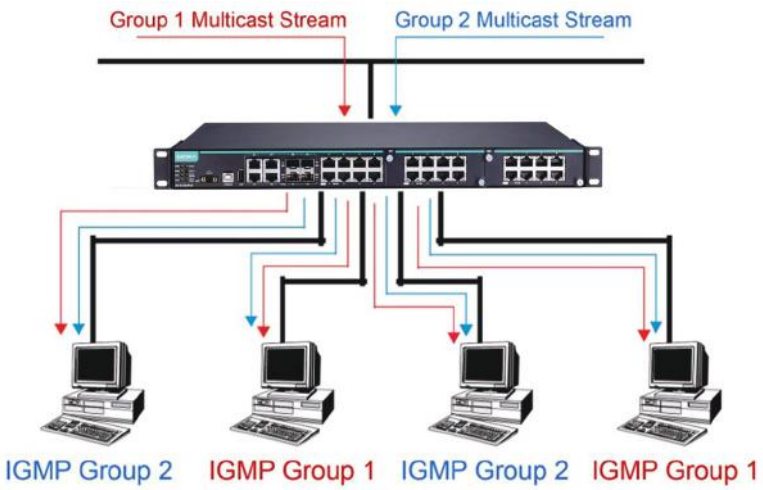
- It uses the most efficient, sensible method to deliver the same information to many receivers with only one transmission.
- It reduces the load on the source (for example, a server) since it will not need to produce several copies of the same data.
- It makes efficient use of network bandwidth and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

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

Multicast Filtering

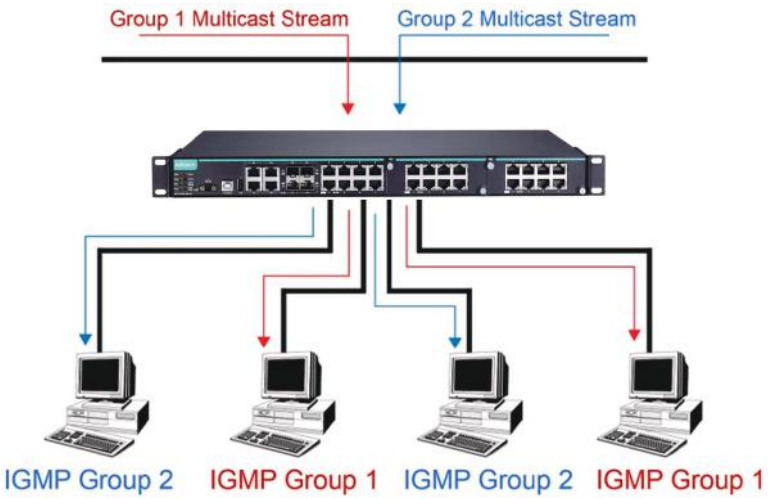
Multicast filtering ensures that only end-stations that have joined certain groups receive multicast traffic. With multicast filtering, network devices only forward multicast traffic to the ports that are connected to registered end-stations. The following two figures illustrate how a network behaves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

Network without multicast filtering



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

Network with multicast filtering



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

Multicast Filtering and Moxa's Industrial Rackmount Switches

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

Snooping Mode

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

IGMP Snooping Enhanced Mode

Snooping Enhanced Mode allows your switch to forward multicast packets to the Moxa switch's member port only. If you disable Enhanced Mode, data streams will run to the querier port as well as the member port.

Query Mode

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

NOTE

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

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

NOTE

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

IGMP Multicast Filtering

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

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

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

IGMP version comparison

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

GMRP (GARP Multicast Registration Protocol)

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

Static Multicast MAC

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

Enabling Multicast Filtering

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

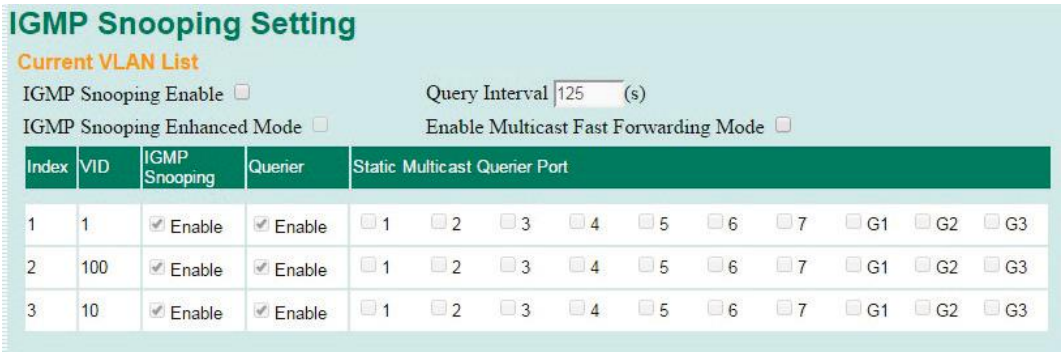
Configuring IGMP Snooping

NOTE

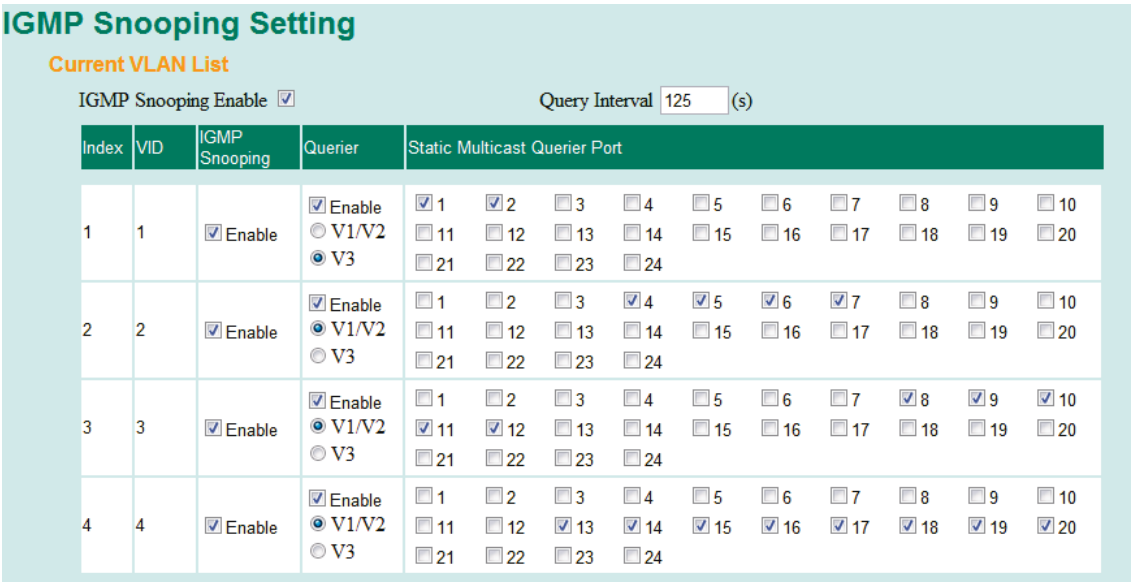
IGMP Snooping will be disabled when Port-Based VLAN is enabled.

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

Layer 2 switch setting page



Layer 3 switch setting page



IGMP Snooping Enable

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

NOTE

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

Query Interval

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

Enable Multicast Fast Forwarding Mode

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

IGMP Snooping Enhanced Mode

Setting	Description	Factory Default
Enable	IGMP Multicast packets will be forwarded to: Auto-Learned Multicast Querier Ports Member Ports	Disable
Disable	IGMP Multicast packets will be forwarded to: Auto-Learned Multicast Router Ports Static Multicast Querier Ports Querier Connected Ports Member Ports	

NOTE

IGMP Snooping Enhanced Mode in networks composed entirely of Moxa switches

IGMP Snooping

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

Querier

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

Static Multicast Querier Port

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

NOTE

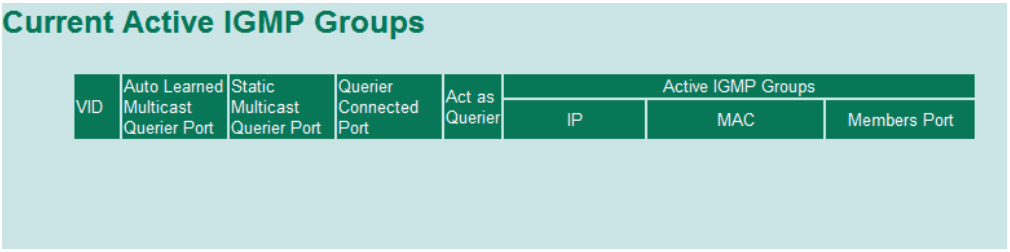
If a router or layer 3 switch is connected to the network, it will act as the Querier, and consequently this Querier option will be disabled on all Moxa layer 2 switches.

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

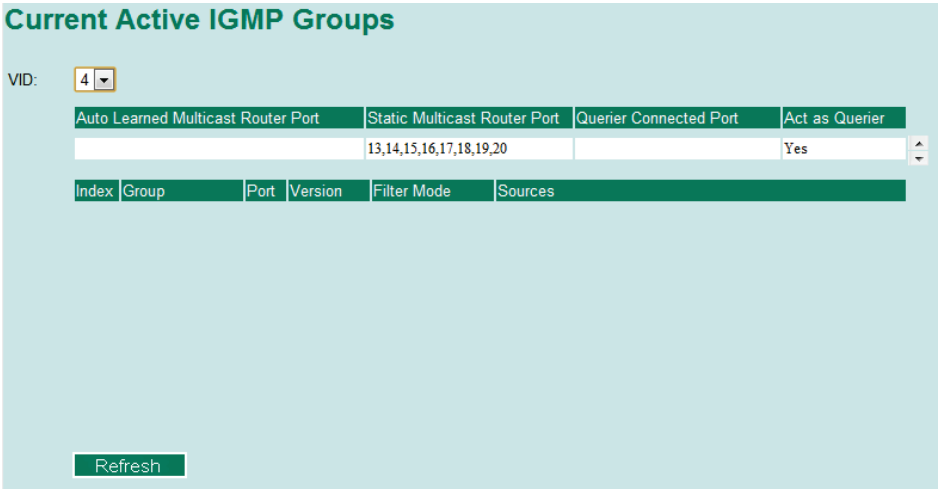
IGMP Table

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

Layer 2 switch page



Layer 3 switch page

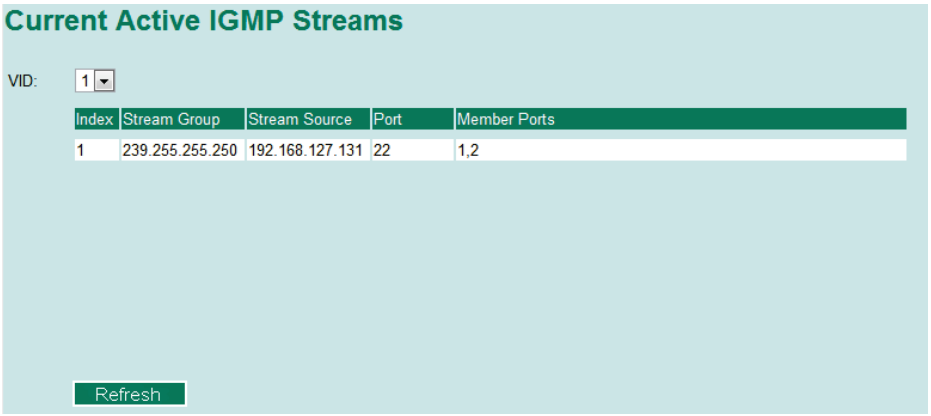


The information shown in the table includes:

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

Current Active IGMP Streams

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



Stream Group: Multicast group IP address

Stream Source: Multicast source IP address

Port: Which port receives the multicast stream

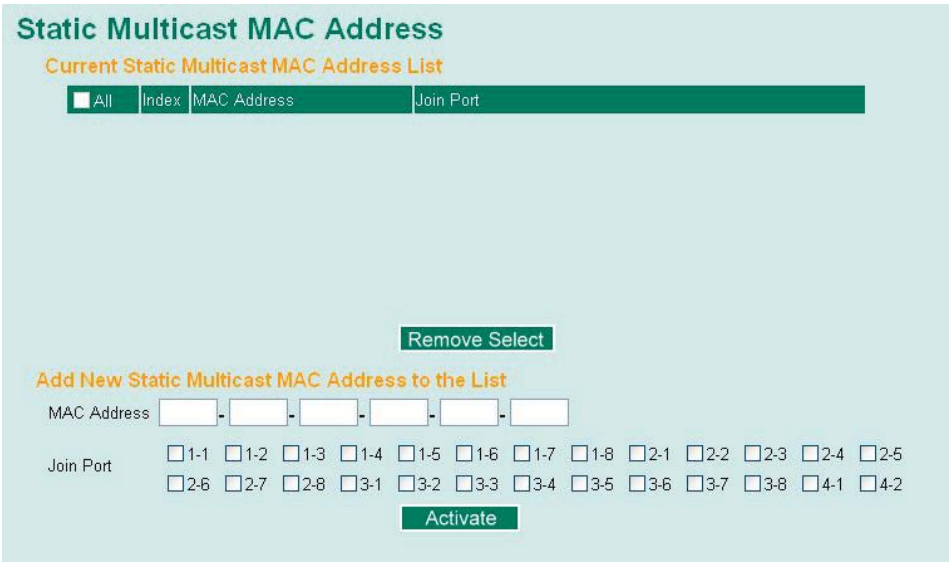
Member ports: Ports the multicast stream is forwarded to.

NOTE

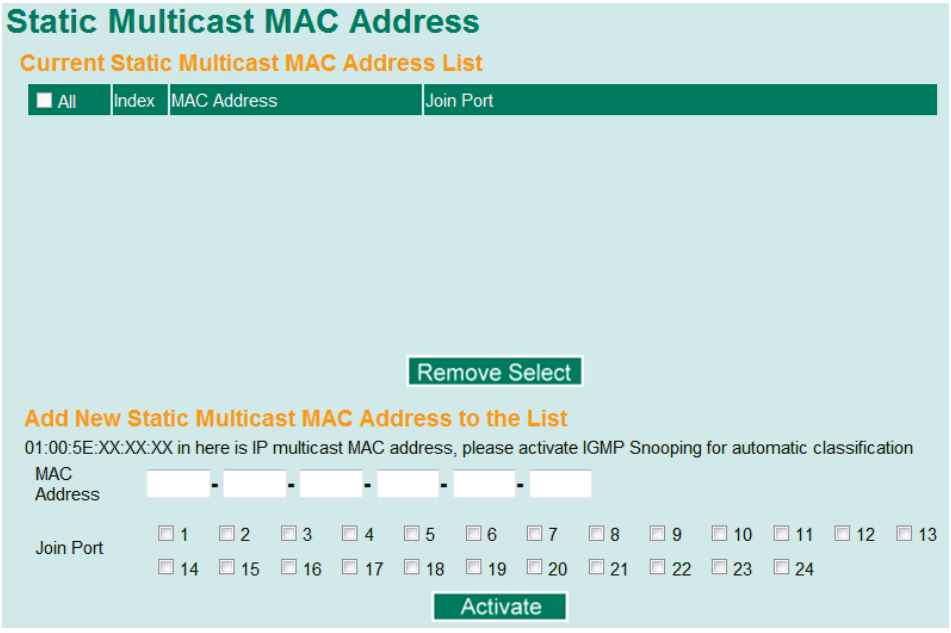
The IGMP stream table is supported only in Layer 3 switches

Static Multicast MAC Addresses

Layer 2 switch page



Layer 3 switch page



NOTE

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

Add New Static Multicast Address to the List

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

MAC Address

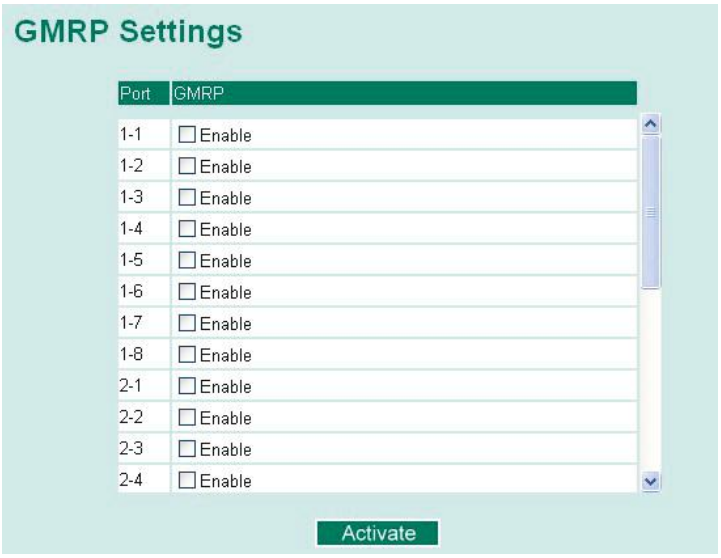
Setting	Description	Factory Default
Integer	Input the number of the VLAN that the host with this MAC address belongs to.	None

Join Port

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

Configuring GMRP

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

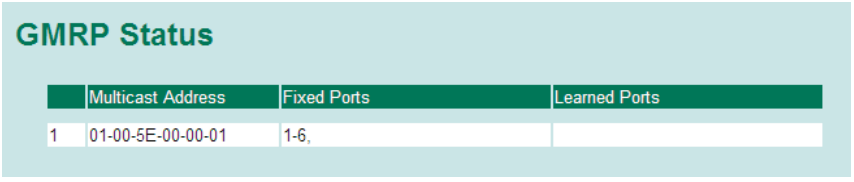


GMRP enable

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

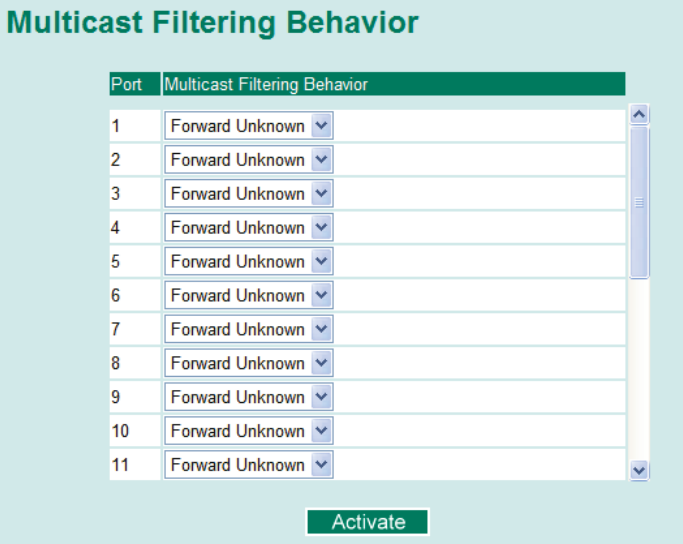
GMRP Table

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



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

Multicast Filtering Behavior



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

Using Bandwidth Management

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

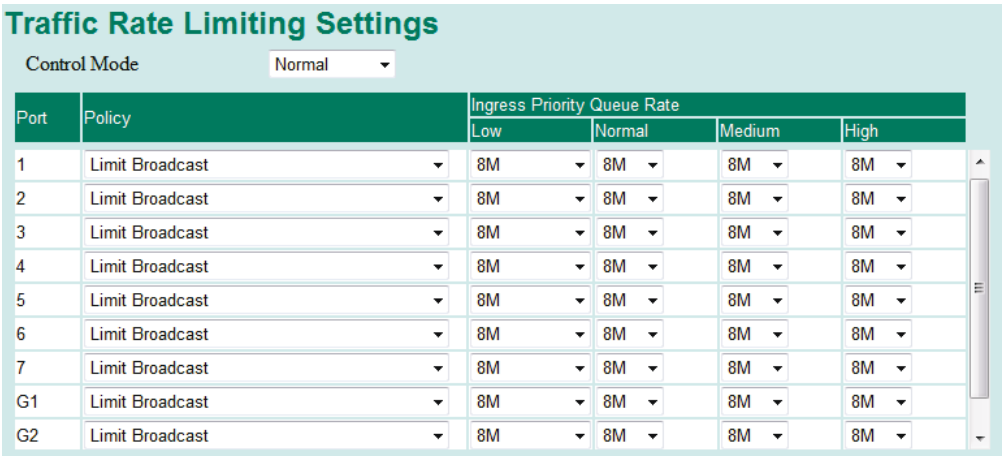
Configuring Bandwidth Management

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

Type	Models Supported
Type 1	EDS-400A Series, EDS-505A/508A/510A/G509, EDS-P506A-4PoE/P510/P510A-8PoE, EDS-600 Series, IKS-G6524/G6824, ICS-G7000 Series, PT-508, PT-510, PT-7710 Series
Type 2	EDS-516A/518A, EDS-728/828, IKS-6726/6726-8PoE/6728, PT-7728, PT-7828, PT-7728-PTP

Type 1

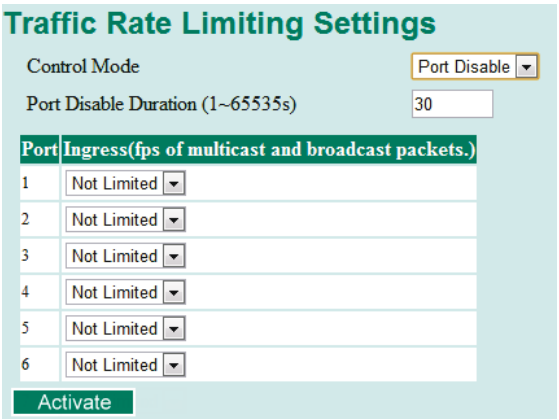
Traffic Rate Limiting Settings



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

Ingress Rate Limit - Normal

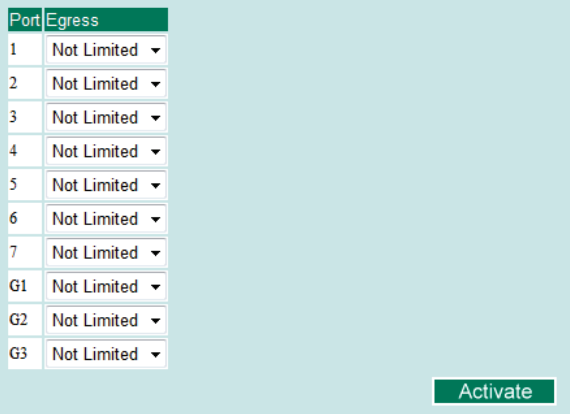
Policy	Description	Factory Default
Limit All	Select the ingress rate limit for different packet types from the following options: Not Limited, 128K, 256K, 512K, 1M, 2M, 4M, 8M	Limit Broadcast 8M
Limit Broadcast, Multicast, Flooded Unicast		
Limit Broadcast, Multicast		
Limit Broadcast		



Ingress Rate Limit – Port Disable

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

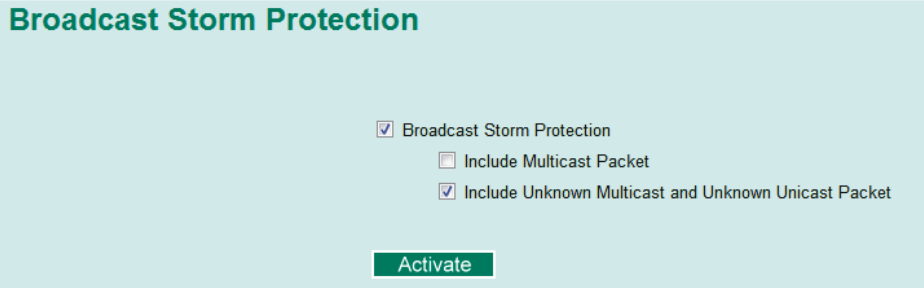
Egress Rate Limit



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

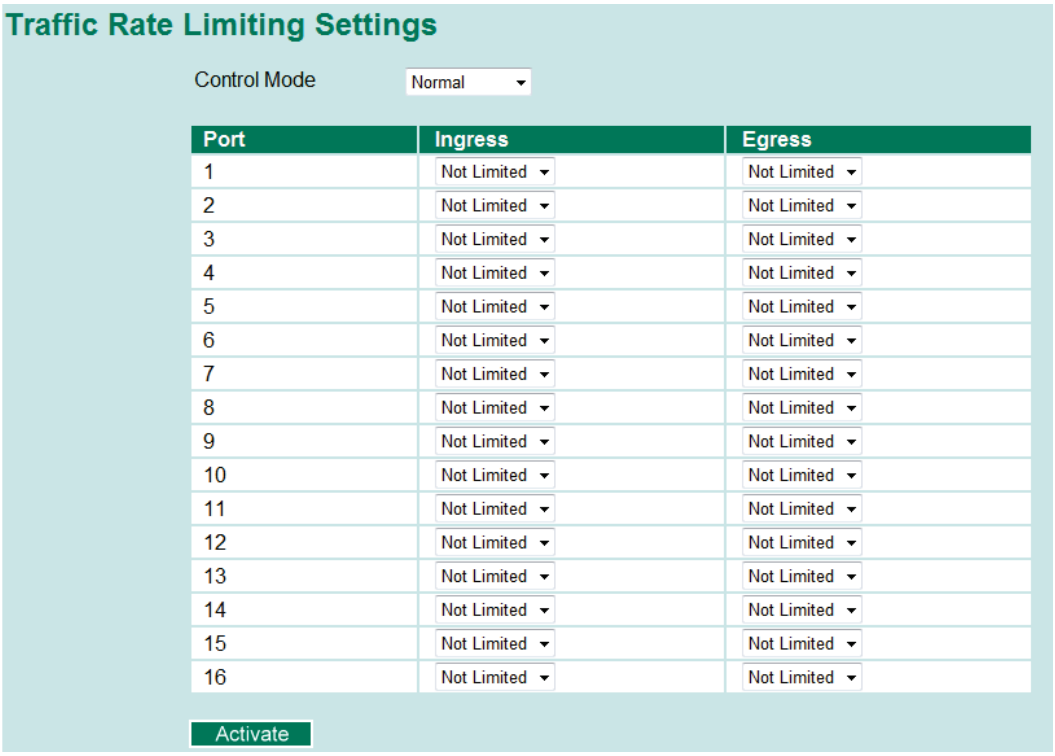
Type 2

Broadcast Storm Protection



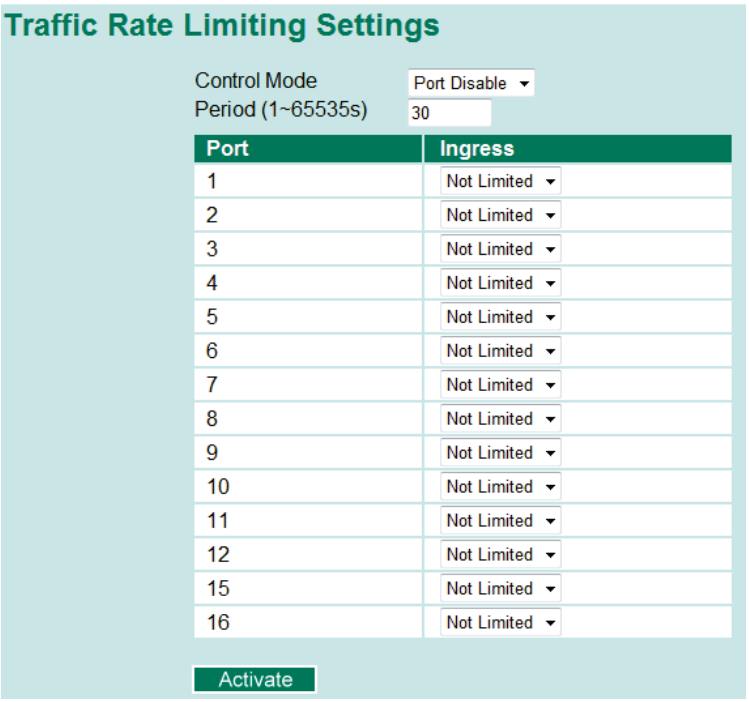
Setting	Description	Factory Default
Enable/Disable	This enables or disables Broadcast Storm Protection for unknown broadcast packet globally	Enable
	This enables or disables Broadcast Storm Protection for unknown multicast packets and unicast packets globally	Disable

Traffic Rate Limiting Settings



Ingress and Egress Rate Limit - Normal

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



Ingress Rate Limit – Port Disable

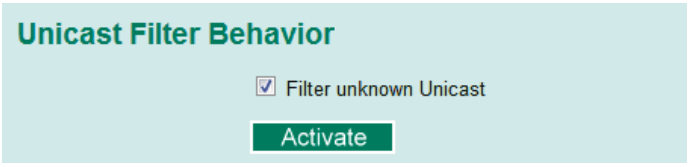
Setting	Description	Factory Default
Period (1~65535 seconds)	When the ingress packets exceed the ingress rate limit, the port will be disabled for a certain period.	30 seconds
Ingress (frame per second)	Select the ingress rate (fps) limit for all packets from the following options: Not Limited, 4464,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

Unicast Filter Behavior

NOTE

These functions are supported in the EDS-728/828 and rackmount switches.

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

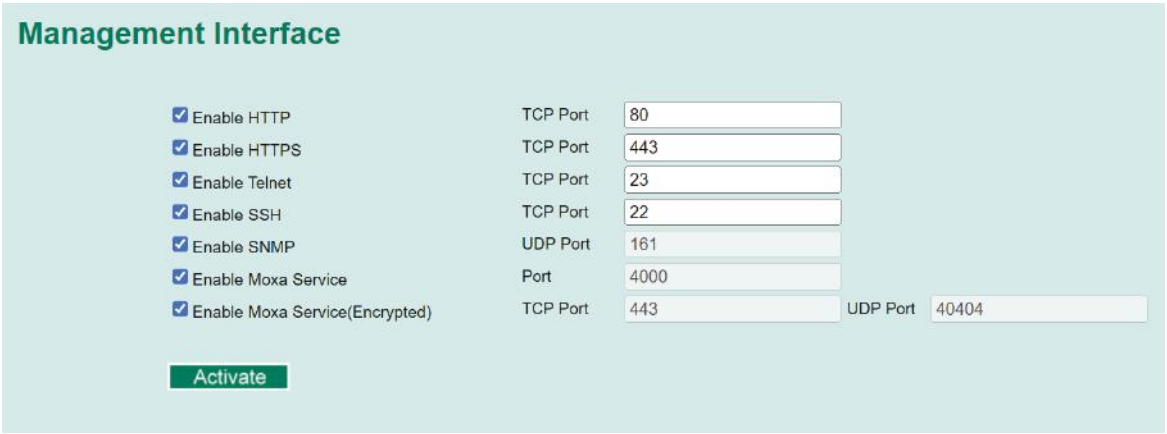


Setting	Description	Factory Default
Enable Filter unknown Unicast	Enable this function to prevent unknown unicast packets from flooding to all ports in the VLAN	Disable

Security

Security can be categorized in two levels: the user name/password level, and the port access level. For user name/password level security, Moxa switches provide two different user login options: Terminal Access Controller Access-Control System Plus (TACACS+) and Remote Authentication Dial In User Service (RADIUS). The TACACS+ and RADIUS mechanism is a centralized "AAA" (Authentication, Authorization and Accounting) system for connecting to network services. The fundamental purpose of both TACACS+ and RADIUS is to provide an efficient and secure mechanism for user account management.

Management Interface



Enable HTTP

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

Enable HTTPS

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

Enable Telnet

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

Enable SSH

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

Enable SNMP

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

Enable Moxa Service

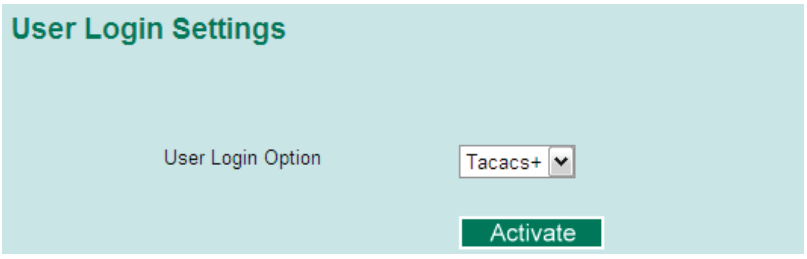
Setting	Description	Factory Default
Select/Deselect	Select the appropriate checkboxes to enable Moxa Service. NOTE: Moxa Service is only for Moxa network management software suite.	Port: 4000

Enable Moxa Service (Encrypted)

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

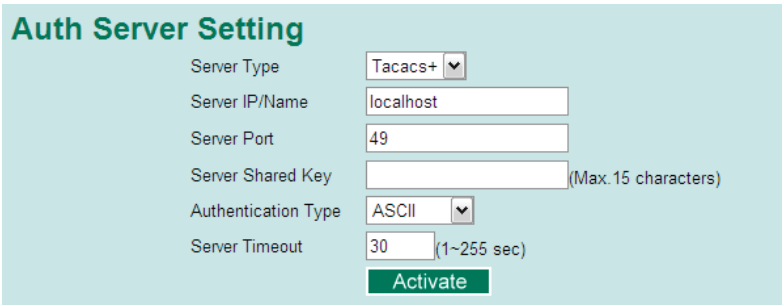
User Login Authentication – User Login Settings

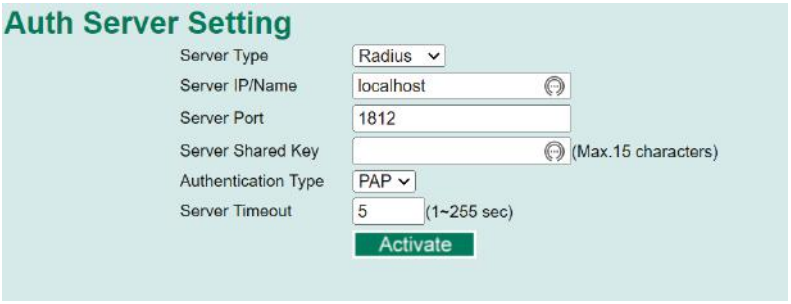
Both TACAS+ and RADIUS are options here.



User Login Authentication – Auth Server Setting

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





NOTE

When changing the login authentication method, the shared key information for RADIUS and TACACS+ will be cleared. Therefore, when changing to RADIUS or TACACS+, the shared key should be entered again.

Setting	Description	Factory Default
Server Type	Authentication server types selection	TACACS+
Server IP/Name	Set IP address of an external TACACS+/RADIUS server as the authentication database	Localhost
Server Port	Set communication port of an external TACACS+/RADIUS server as the authentication database	TACACS+ : 49 RADIUS : 1812
Server Shared Key	Set specific characters for server authentication verification	None
Authentication Type	The authentication mechanism. ASCII is for TACACS+; PAP is for RADIUS.	ASCII for TACACS+
Server Timeout	The timeout period to wait for a server response	TACACS+ : 30 RADIUS : 5

Authentication Certificate

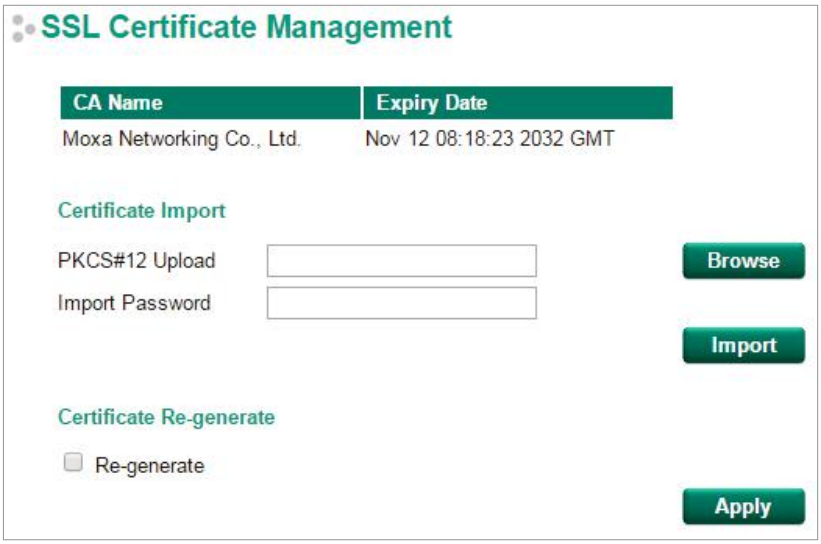
The switch offers two methods to encrypt the communication: SSL Certificate and SSH Key. You can only use one of the encryption types at the same time. SSL (Secure Socket Layer) is mainly for web communication security. It secures the data between two application points. SSH (Secure Shell) is a security protocol based on the Application Layer and Transport Layer. It encrypts the data for security.

NOTE

The switch only supports one type of Authentication Certificate at a time.

Check the Authentication Certificate, and then click Activate to complete.

SSL Certificate Management



Certificate Import

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

Regenerate SSL Certificate

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

Using Port Access Control

NOTE

Port Access Control functions not supported in EDS-400A series (except EDS-405A-PTP).

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

Static Port Lock

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

IEEE 802.1X

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

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

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

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

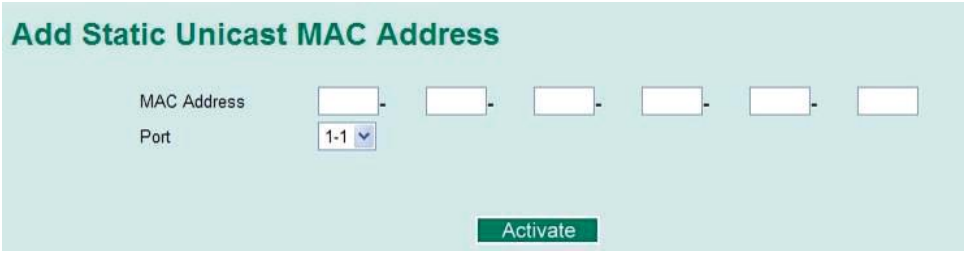
Authenticator: Edge switch or wireless access point that acts as a proxy between the supplicant and the authentication server, requesting identity information from the supplicant, verifying the information with the authentication server, and relaying a response to the supplicant.

The Moxa switch acts as an authenticator in the 802.1X environment. A supplicant and an authenticator exchange EAPOL (Extensible Authentication Protocol over LAN) frames with each other. We can either use an external RADIUS server as the authentication server, or implement the authentication server in the Moxa switch by using a Local User Database as the authentication look-up table. When we use an external RADIUS server as the authentication server, the authenticator and the authentication server exchange EAP frames between each other.

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

Configuring Static Port Lock

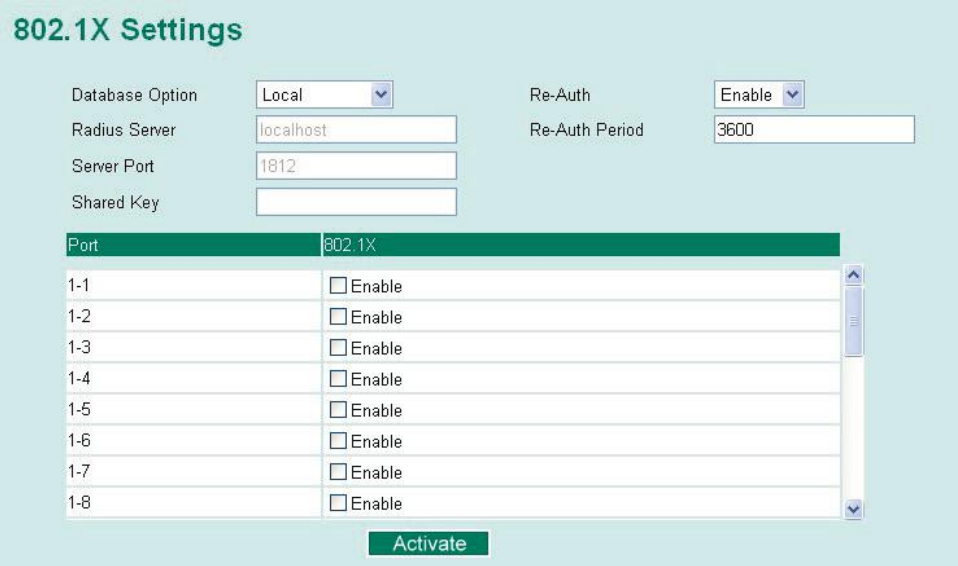
The Moxa switch supports adding unicast groups manually if required.



Static Unicast MAC Address

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

Configuring IEEE 802.1X



Database Option

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

Radius Server

Setting	Description	Factory Default
IP address or domain name	The IP address or domain name of the RADIUS server	local host

Server Port

Setting	Description	Factory Default
Numerical	The UDP port of the RADIUS server	1812

Shared Key

Setting	Description	Factory Default
alphanumeric (Max. of 40 characters)	A key to be shared between the external RADIUS server and Moxa switch. Both ends must be configured to use the same key.	None

Re-Auth

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

Re-Auth Period

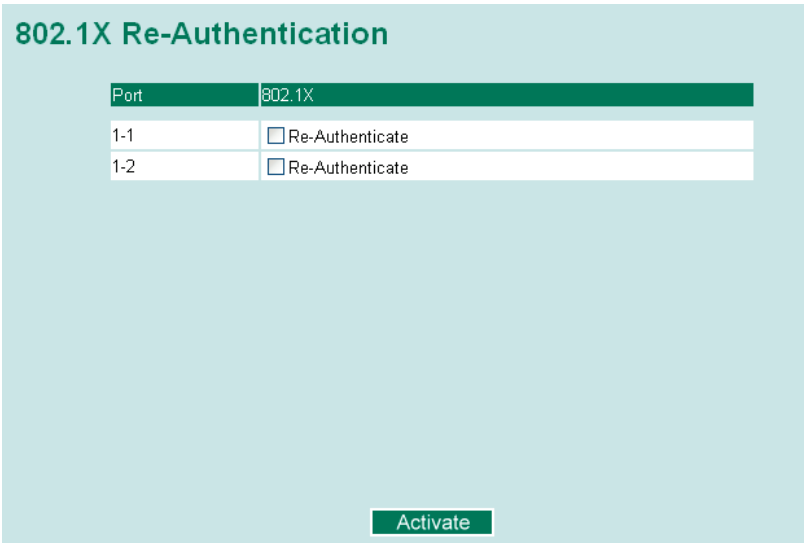
Setting	Description	Factory Default
Numerical (60 to 65535 sec.)	Specify how frequently the end stations need to reenter usernames and passwords in order to stay connected.	3600

802.1X

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

802.1X Re-Authentication

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

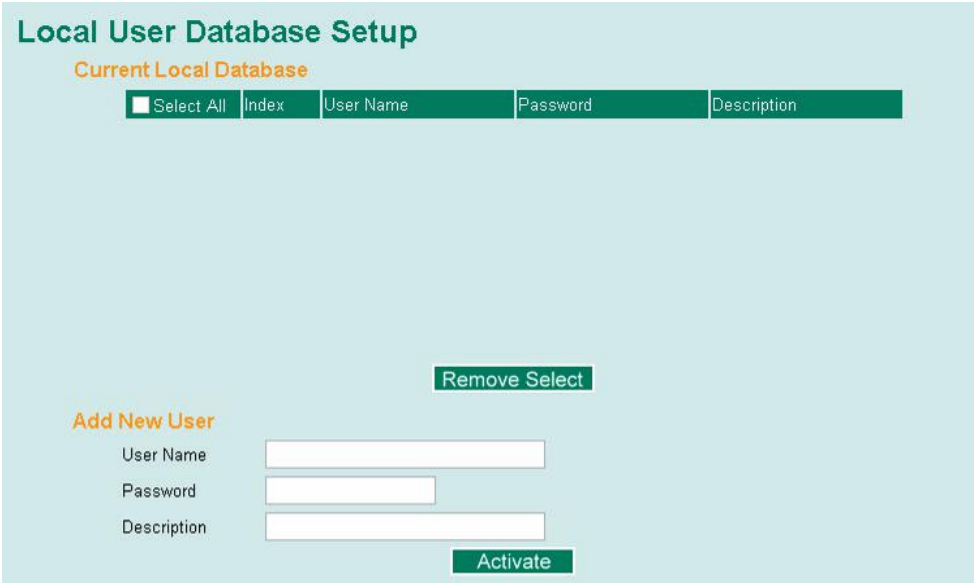


802.1X Re-Authentication

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

Local User Database Setup

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



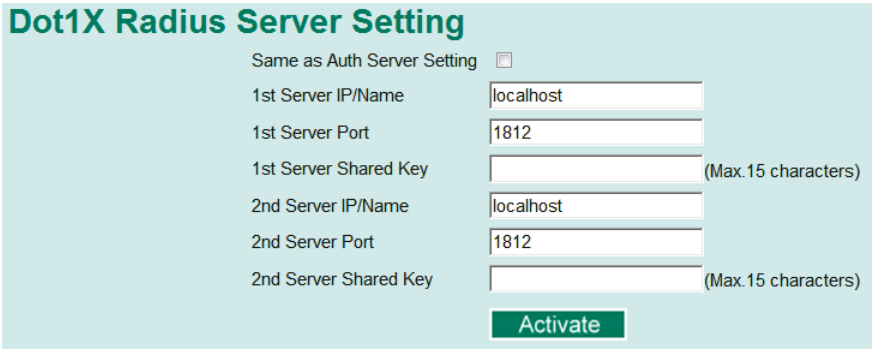
Local User Database Setup

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

NOTE

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

Dot1X Radius Server Setting



Same as Auth Server Setting

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

Server Setting

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

Port Access Control Table

The port status will show authorized or unauthorized.

Using Auto Warning

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

Configuring Email Warning

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

Configure Email Event Types

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

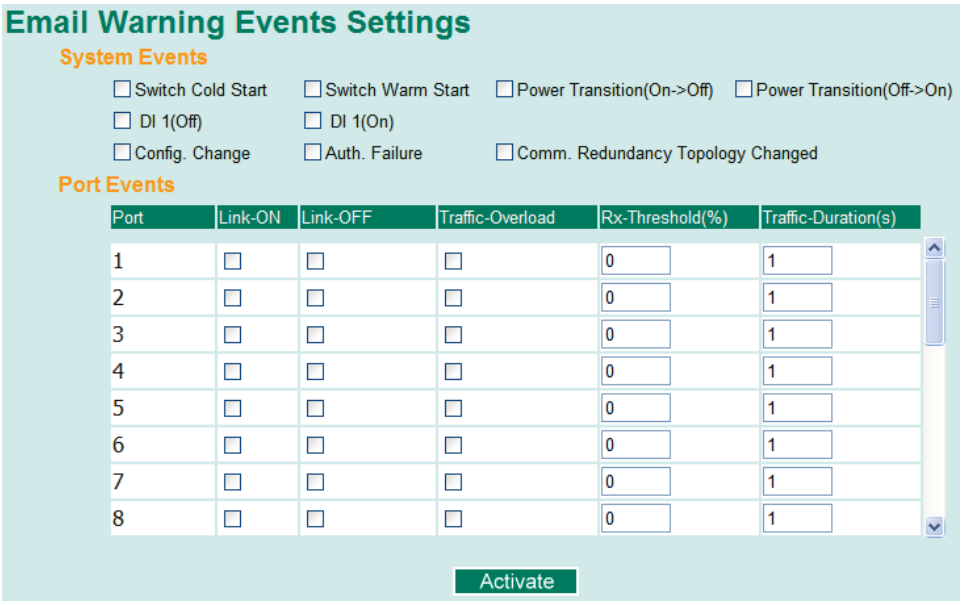
Configure Email Settings

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

Activate your settings and if necessary, test the email

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

Configuring Event Types



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

System Events	Warning e-mail is sent when...
Switch Cold Start	Power is cut off and then reconnected.
Switch Warm Start	Moxa switch is rebooted, such as when network parameters are changed (IP address, subnet mask, etc.).
Power Transition (On→Off)	Moxa switch is powered down.
Power Transition (Off→On)	Moxa switch is powered up.
DI1/DI2 (On→Off)	Digital Input 1/2 is triggered by on to off transition
DI1/DI2 (Off→On)	Digital Input 1/2 is triggered by off to on transition
Configuration Change Activated	Any configuration item has been changed.
Authentication Failure	An incorrect password was entered.
Comm. Redundancy Topology Changed	If any Spanning Tree Protocol switches have changed their position (applies only to the root of the tree). If the Master of the Turbo Ring has changed or the backup path is activated.

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

NOTE

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

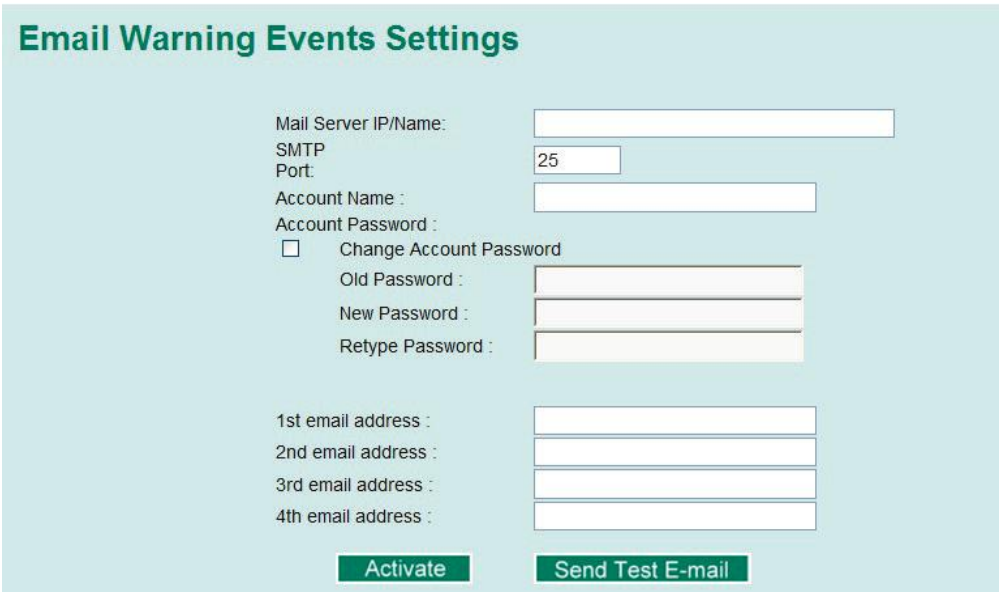
NOTE

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

Managed-Redundant-Switch-00000@Switch_Location

where Managed-Redundant-Switch-00000 is the default Switch Name, 00000 is the Moxa switch's serial number, and Switch_Location is the default Server Location. Refer to the Basic Settings section to see how to modify Switch Name and Switch Location.

Configuring Email Settings



Mail Server IP/Name

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

SMTP Port

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

Account Name

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

Password Setting

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

Email Address

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

Send Test Email

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

NOTE

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

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

Configuring Relay Warning

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

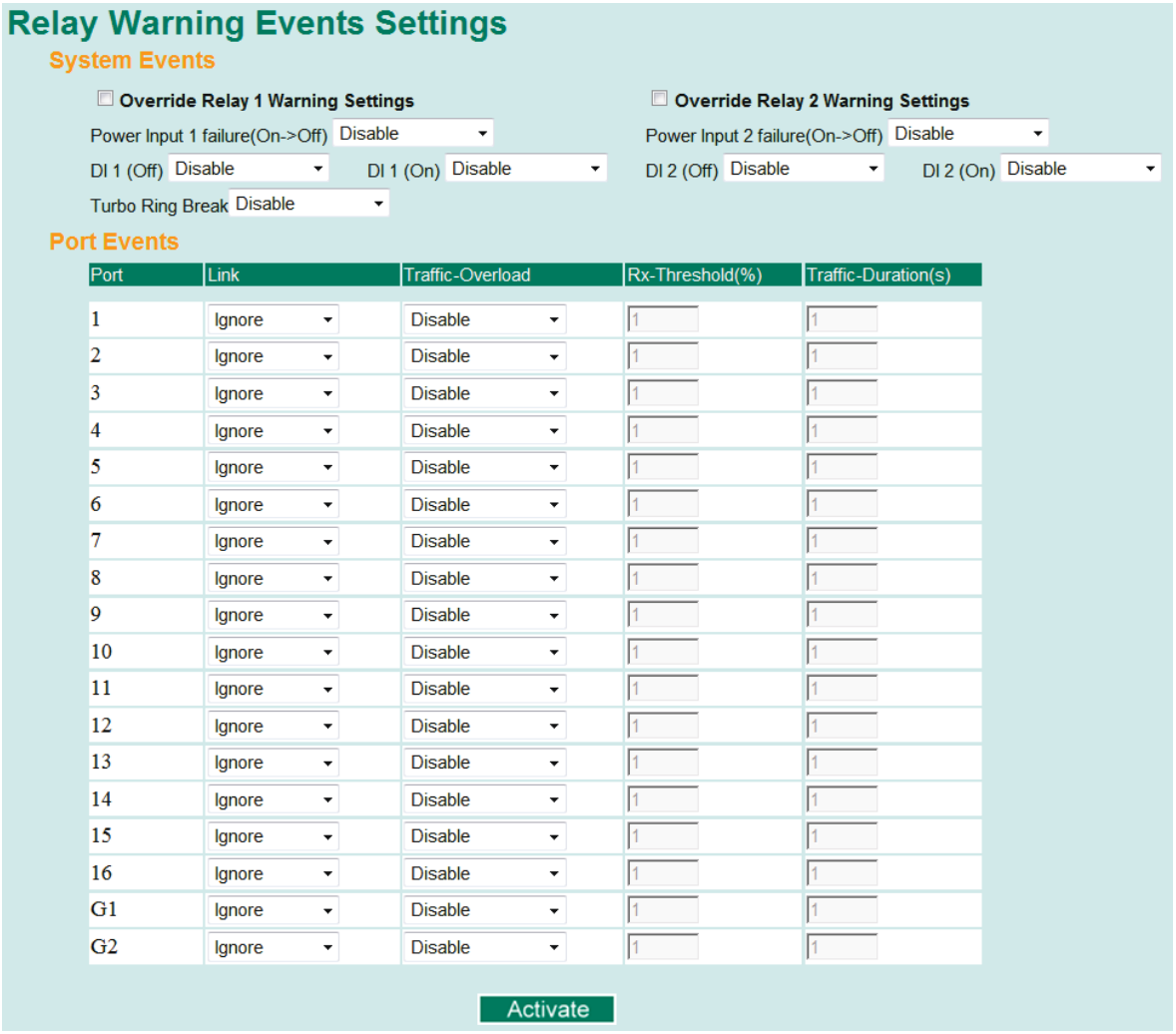
Configure Relay Event Types

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

Activate your settings

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

Configuring Event Types



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

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

System Events	Warning Relay output is triggered when...
Power Transition (On -> Off)	Moxa switch is powered down
Power Transition (Off -> On)	Moxa switch is powered up
DI1/DI2 (On -> Off)	Digital Input 1/2 is triggered by on to off transition
DI1/DI2 (Off -> On)	Digital Input 1/2 is triggered by off to on transition
Turbo Ring Break	The Turbo Ring is broken. Only the MASTER switch of Turbo Ring will output warning relay.

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

Override relay alarm settings

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

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

Warning List

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

Using Line-Swap-Fast-Recovery

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

Configuring Line-Swap Fast Recovery

Enable Line-Swap-Fast-Recovery

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

Using Set Device IP

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

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

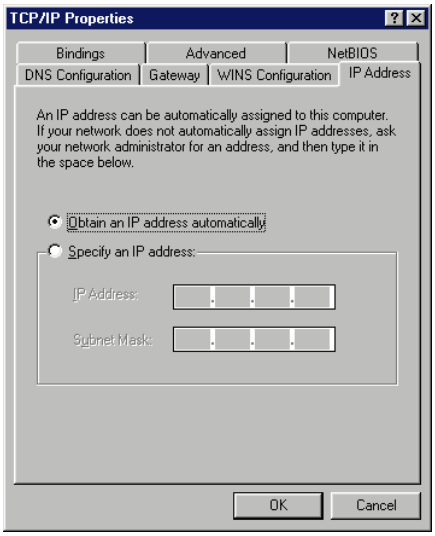
Take the following steps to use the **Set device IP** function:

STEP 1—*Set up the connected devices*

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

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

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



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

STEP 2

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

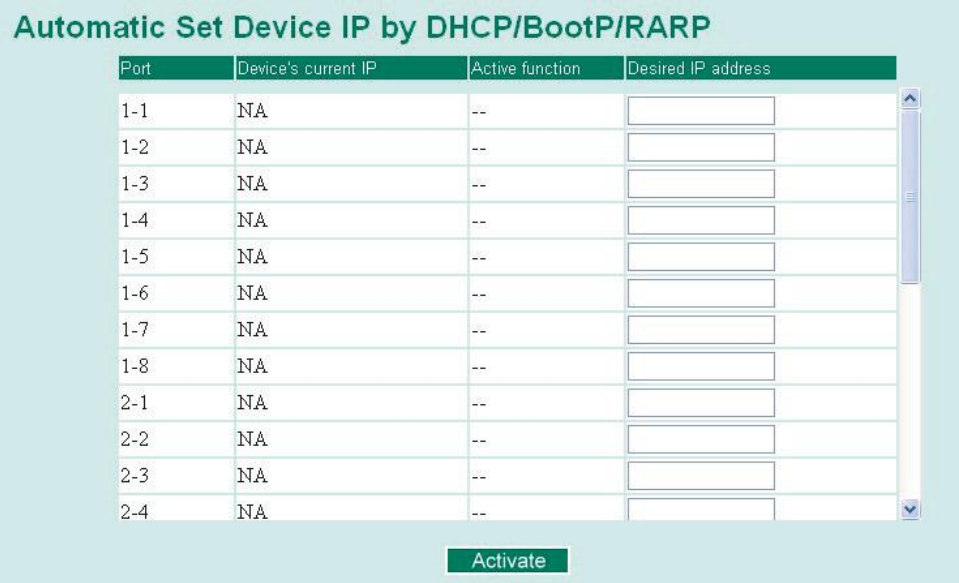
STEP 3

Be sure to activate your settings before exiting.

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

Configuring Set Device IP

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



Desired IP Address

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

Configuring DHCP Relay Agent

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

DHCP Relay Agent (Option 82)

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

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

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

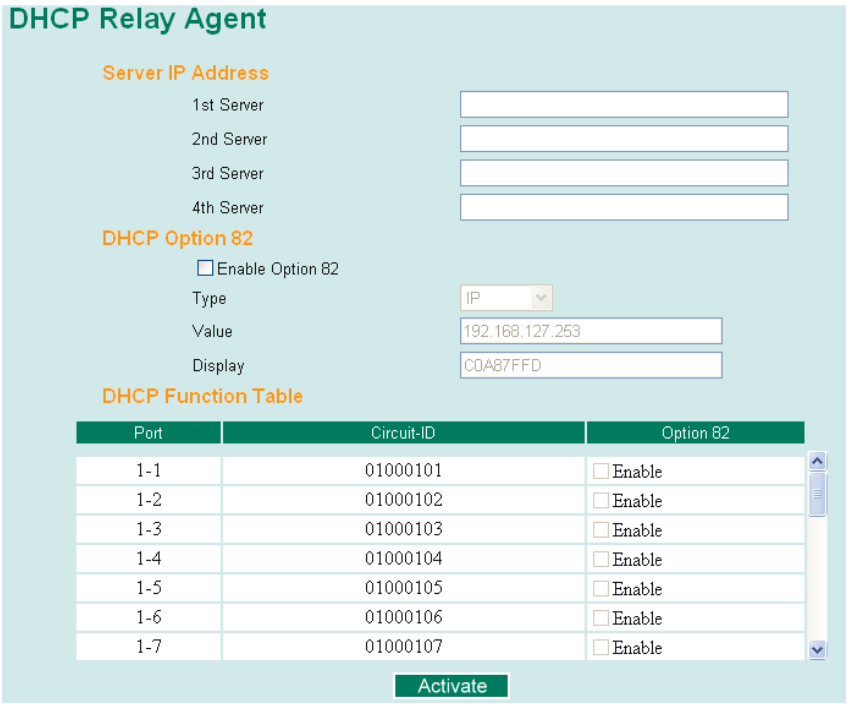
FF–VV–VV–PP

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

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

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

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



Server IP Address

1st Server

1st Server

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

2nd Server

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

3rd Server

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

4th Server

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

DHCP Option 82

Enable Option 82

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

Type

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

Value

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

Display

Setting	Description	Factory Default
read-only	The actual hexadecimal value configured in the DHCP server for the Remote-ID. This value is automatically generated according to the Value field. Users cannot modify it.	COA87FFD

DHCP Function Table

Enable

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

Using Diagnosis

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

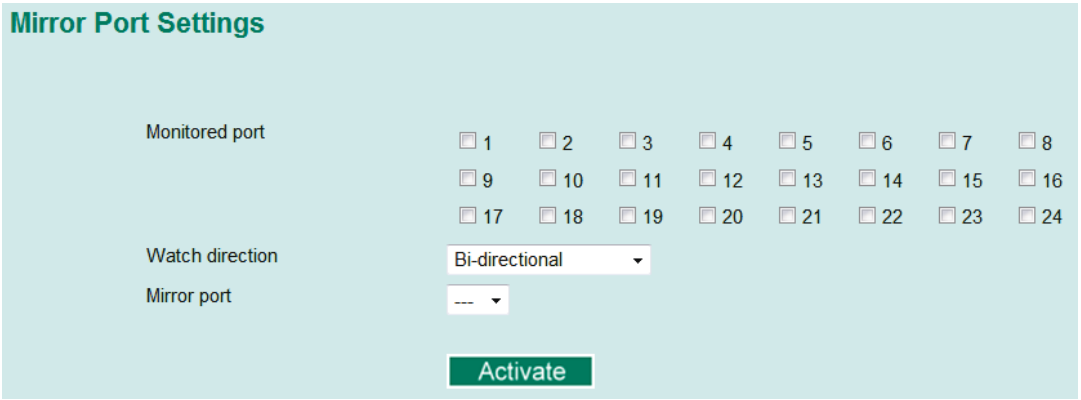
Mirror Port

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

Please note that two types of mirror port settings are available, depending on the specific model of switch. In Type 1, the switches support multi-to-one and one-to-one mirror function. In Type 2, the switches support only one-to-one mirror function.

Type	Models Supported
Type 1	EDS-728/828, IKS-6726/6726-8PoE/6728/G6524/G6824, ICS-G7000 Series, PT-7528, PT-7728, PT-7828, PT-7728-PTP Series
Type 2	EDS 400A/500A/600 Series, EDS-P506A-4PoE/P510/P510A-8PoE/G509, PT-508, PT-510, PT-7710 Series

Type 1



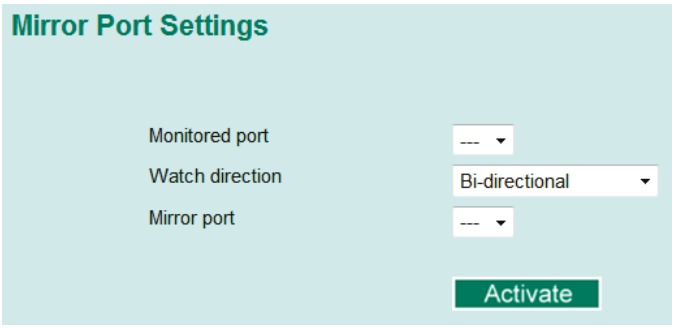
Mirror Port Settings

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

NOTE

In Type 1 settings, users can select multiple monitored ports for port mirror function.

Type 2



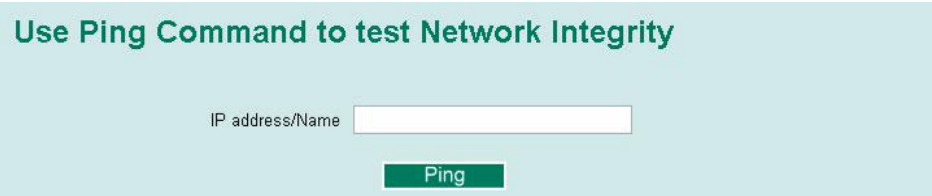
Mirror Port Settings

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

NOTE

In Type 2 settings, users can select only one monitored port for port mirror function.

Ping



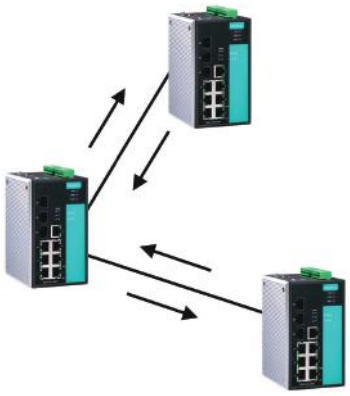
The **Ping** function uses the ping command to give users a simple but powerful tool for troubleshooting network problems. The function's most unique feature is that even though the ping command is entered from the user's PC keyboard, the actual ping command originates from the Moxa switch itself. In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

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

LLDP Function

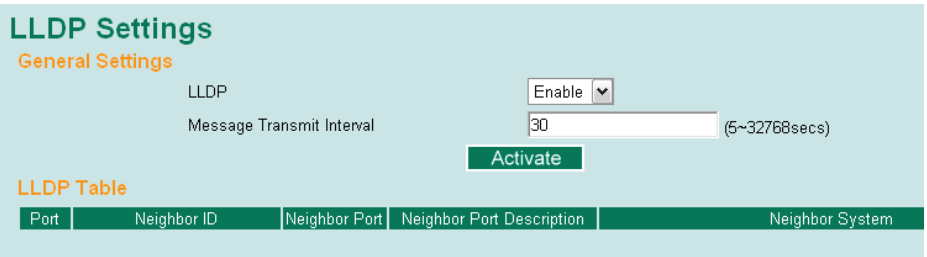
Overview

LLDP is an OSI Layer 2 protocol defined by IEEE 802.11AB. LLDP standardizes the self-identification advertisement method, and allows each networking device, such as a Moxa managed switch, to periodically send its system and configuration information to its neighbors. Because of this, all LLDP devices are kept informed of each other's status and configuration, and with SNMP, this information can be transferred to Moxa's MXview for auto-topology and network visualization.



From the switch's web interface, you can enable or disable LLDP, and set the LLDP transmit interval. In addition, you can view each switch's neighbor-list, which is reported by its network neighbors. Most importantly, enabling the LLDP function allows Moxa's MXview to automatically display the network's topology and system setup details, such as VLAN and Trunking, for the entire network.

Configuring LLDP Settings



General Settings

LLDP

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

Message Transmit Interval

Setting	Description	Factory Default
5 to 32768 sec.	Sets the transmit interval of LLDP messages, in seconds.	30 (seconds)

LLDP Table

The LLDP Table displays the following information:

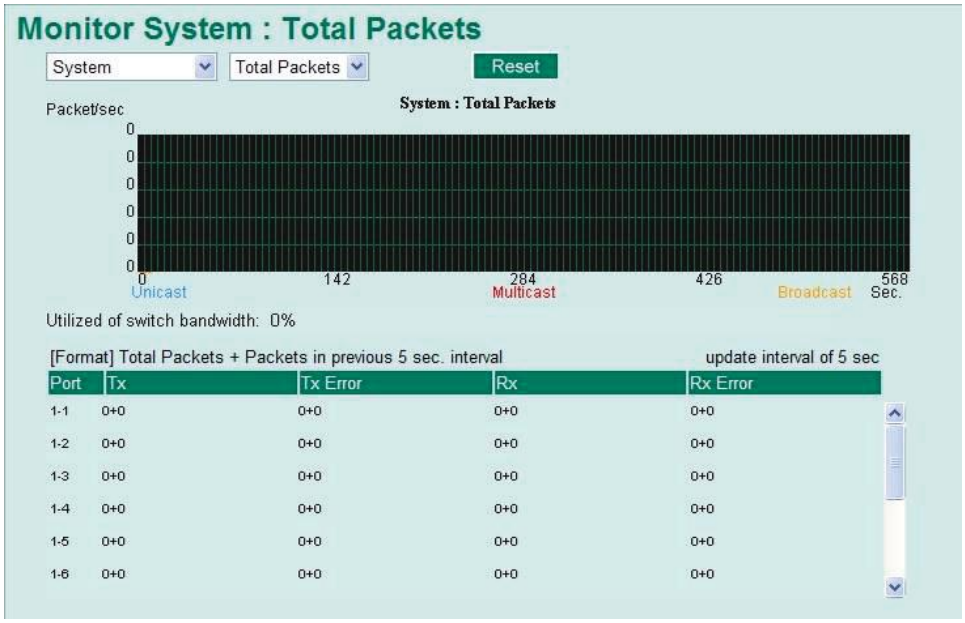
Port	The port number that connects to the neighbor device.
Neighbor ID	A unique entity (typically the MAC address) that identifies a neighbor device.
Neighbor Port	The port number of the neighbor device.
Neighbor Port Description	A textual description of the neighbor device's interface.
Neighbor System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

Using Monitor

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

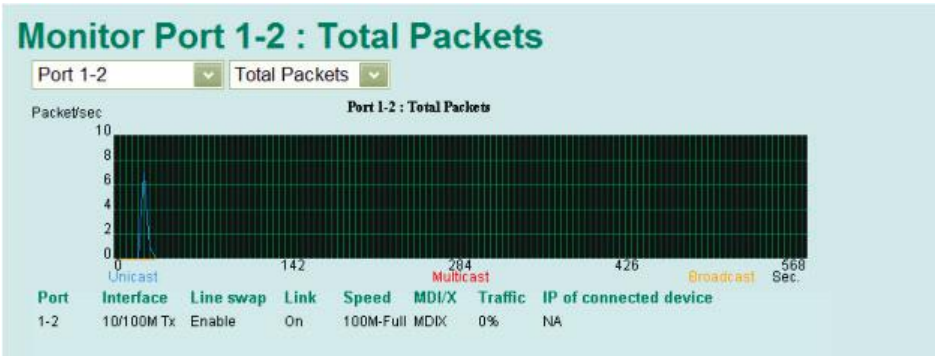
Monitor by Switch

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



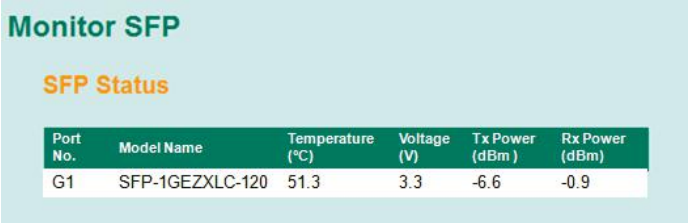
Monitor by Port

Access the Monitor by Port function by selecting **ALL 10/100M or 1G Ports** or **Port *i***, in which **i** = **1, 2, ...**, **G2**, from the left pull-down list. The **Port *i*** options are identical to the Monitor by System function discussed above, in that users can view graphs that show All Packets, TX Packets, RX Packets, or Error Packets activity, but in this case, only for an individual port. The **All Ports** option is essentially a graphical display of the individual port activity that can be viewed with the Console Monitor function discussed above. The All Ports option shows three vertical bars for each port. The height of the bar represents **Packets/s** for the type of packet, at the instant the bar is being viewed. That is, as time progresses, the height of the bar moves up or down so that the user can view the change in the rate of packet transmission. The blue colored bar shows **Uni-cast** packets, the red colored bar shows **Multi-cast** packets, and the orange colored bar shows **Broad-cast** packets. The graph is updated every few seconds, allowing the user to analyze data transmission activity in real-time.



Monitor by SFP

Optical fiber is commonly used for long distance data transmission. However, when link issues occur, it is very costly to trouble shoot the fiber cable and fiber transceiver at remote sites. To solve this problem, Moxa industrial Ethernet switches provide digital diagnostic and monitoring functions on Moxa SFP optical fiber links and allow users to measure optical parameters and its performance from center site. This function can greatly facilitate the trouble shooting process for optical fiber links and reduce costs for onsite debug.



Parameter	Description
Port No.	Switch port number with SFP plugged in
Model Name	Moxa SFP model name
Temperature (°C)	SFP casing temperature
Voltage (V)	Voltage supply to the SFP
Tx power (dBm)	The amount of light being transmitted into the fiber optic cable
Rx power (dBm)	The amount of light being received from the fiber optic cable

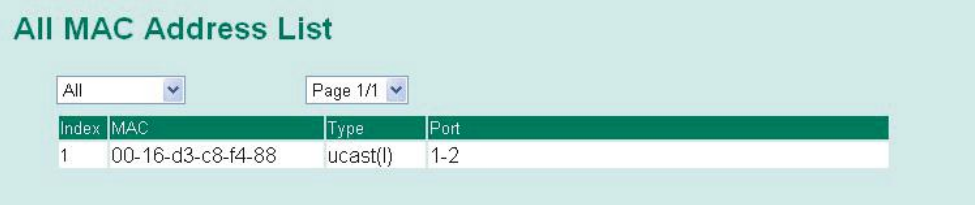
NOTE

Certain tolerances exist between real data and measured data.

Parameters	Tolerance
Temperature (°C)	± 3°C
Voltage (V)	± 0.1V
Tx power (dBm)	± 3dB
Rx power (dBm)	± 3dB

Using the MAC Address Table

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



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

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

The table displays the following information:

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

Using Access Control List

NOTE

Access Control Lists are available in Moxa Layer 3 switches.

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

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

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

The ACL Concept

What is ACL?

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

Benefits of ACL

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

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

How ACL works

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

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

- IP based
- MAC Based

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

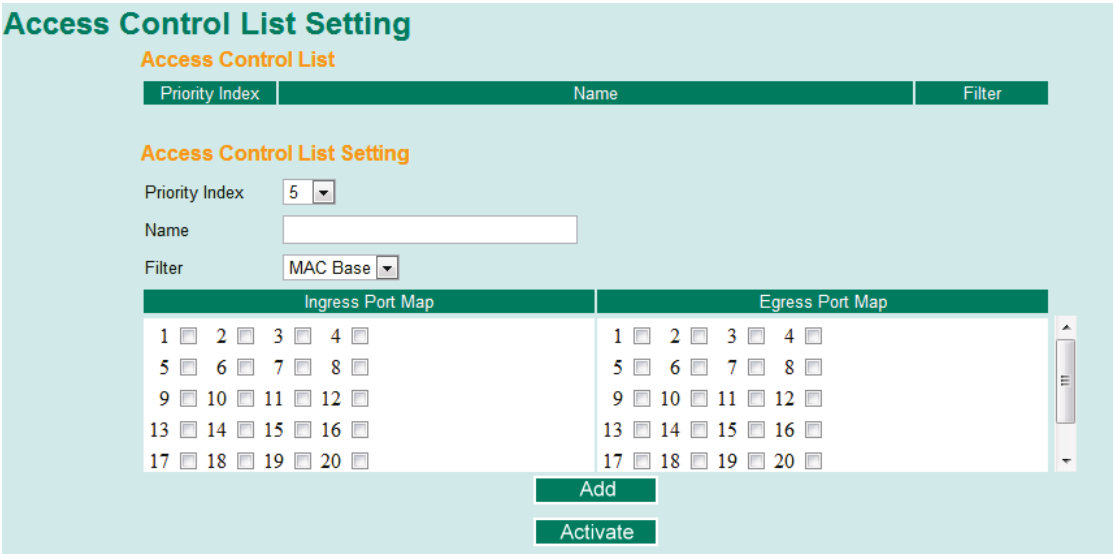
After adding a new access control list, you can also create new rules for the access control list. Each ACL group accepts 10 rules. Rules can filter packets by source and destination IP/MAC address, IP protocol, TCP/UDP Port, Ethernet Type, and VLAN ID.

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

Access Control List Configuration and Setup

Access Control List Settings

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



In this page, you can mainly configure two settings:

Add/Modify Access Control List

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

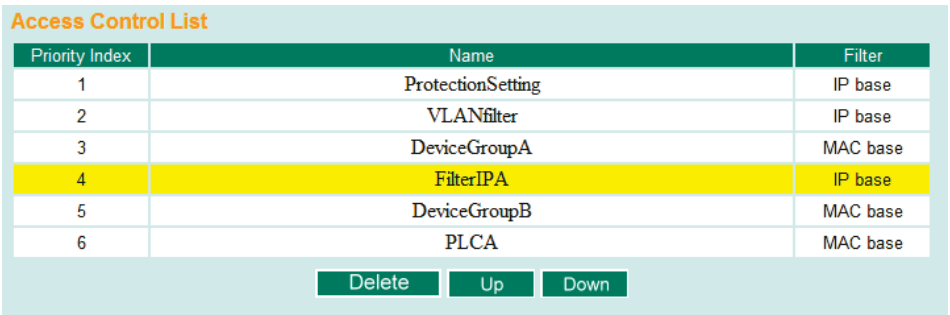
- **Priority Index:** ACL checking sequence is based on this index. Smaller index numbers have higher priority for packet filtering. If a packet is filtered by an access list with higher priority, those access lists with lower priority will not being executed.

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

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

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

Adjust ACL Priority Index



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

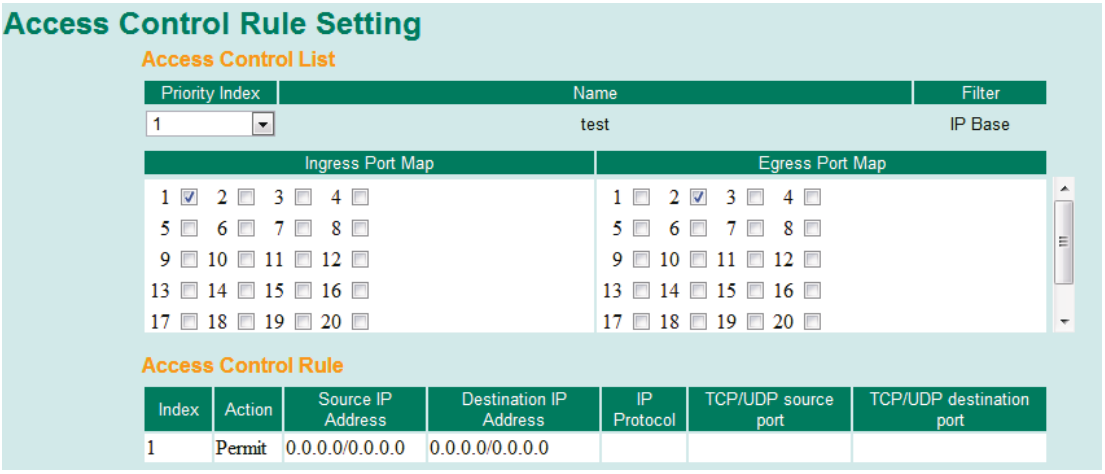
Step 1: Select the list

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

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

Access Control Rule Settings

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



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

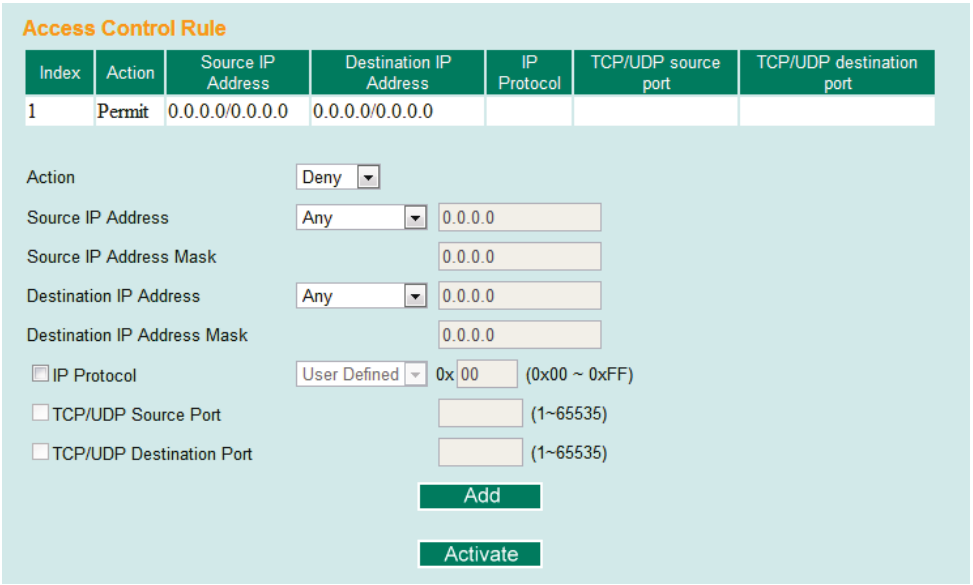
NOTE

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

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

IP-Based

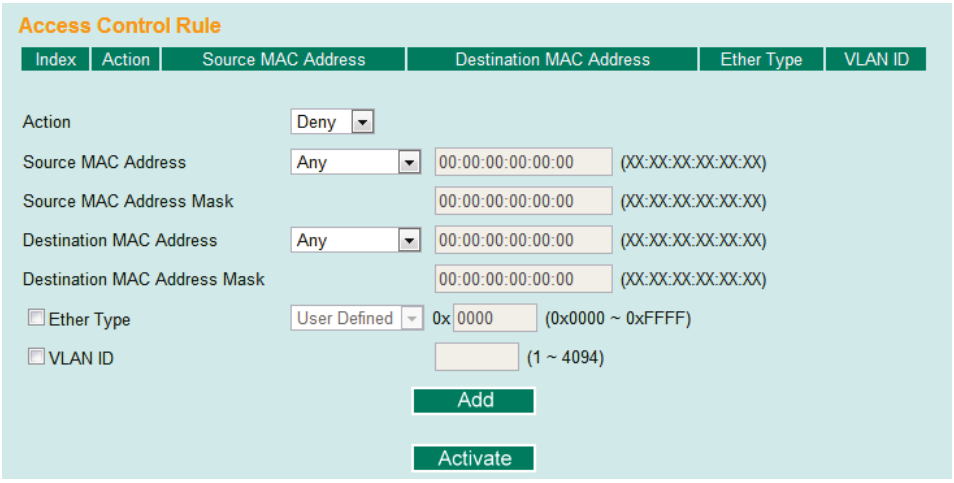
After configuring, click Add button to add the rule to the list. Then, click Activate to activate the settings.



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

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

MAC-Based

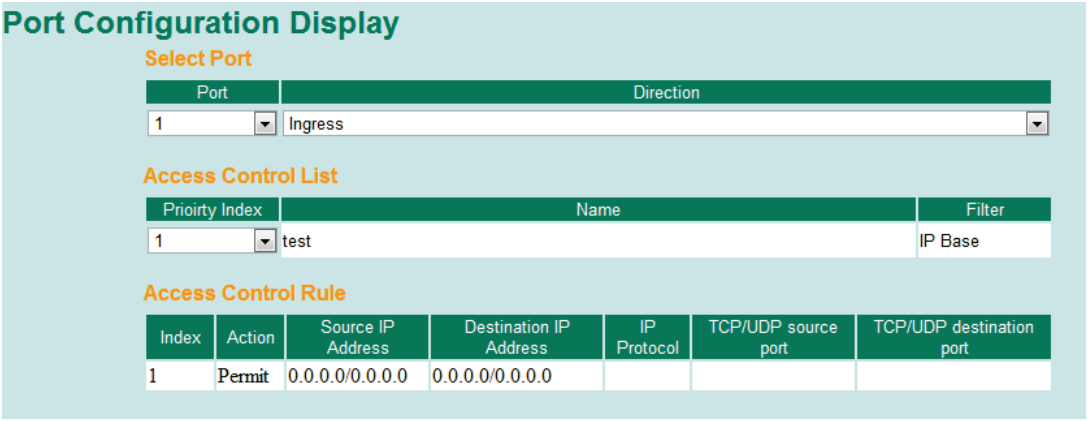


- **Action:** Whether to deny or permit access if the rule criterion is met.
- **Source MAC Address/Source MAC Address Mask:** Defines the MAC address rule. By using the mask, you can assign specific MAC address ranges to filter. It allows checking the source or destination of the packet. Choose **Any** if you do not need to use this criteria.
- **Ethernet Type:** Select the type of Ethernet protocol to filter. Options here are **IPv4, ARP, RARP, IEEE802.1Q, IPv6, IEE802.3, PROFIENT, LLDP,** and **IEEE1588.**
- **VLAN ID:** Enter a VLAN ID you would like to filter by.

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

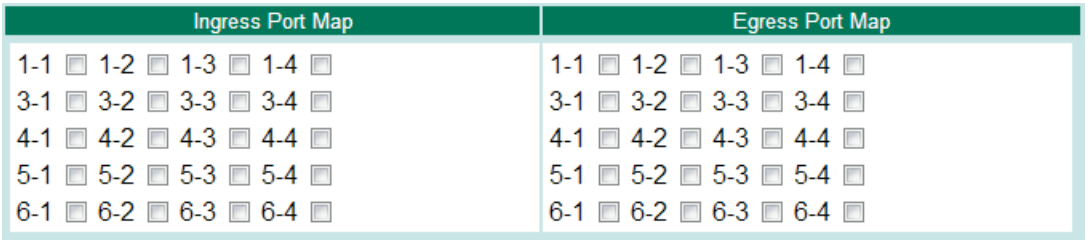
Port Configuration Display

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



NOTE

For EDS-828 and PT-7828 series, there are two limitations on ACL settings. Based on the ingress port type of ACL rules, there are two types for the limitation of numbers.



Limitation Type 1:

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

Limitation Type 2:

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

Example 1 for Limitation 1

Rule A contains 3 ***ingress FE*** ports and 4 ***egress FE*** ports, and it results in the number of 3 x 4 = 12.
Rule B contains 5 ***ingress FE*** ports and 6 ***egress GE*** ports, and it results in the number of 5 x 6 = 30.
Rule C contains 7 ***ingress FE*** ports and ***no egress*** port, and it results in the number of 7.
Make sure the amount of those numbers "12+30+7" is not greater than 160.

Example 2 for Limitation 2

Rule D contains 1 ***ingress GE*** port and 2 ***egress FE*** ports, and it results in the number of 1 x 2 = 2.
Rule E contains 3 ***ingress GE*** ports and 4 ***egress GE*** ports, and it results in the number of 3 x 4 = 12.
Rule F contains 5 ***ingress GE*** ports and ***no egress*** ports, and it results in the number of 5.
Rule G contains ***no ingress*** ports and 6 ***FE egress*** ports, and it results in the number of 6.
Rule H contains ***no ingress*** ports and 7 ***GE egress*** ports, and it results in the number of 7.
Make sure the amount of those numbers "2+12+5+6+7" is not greater than 40.

Example 3 for Limitation 1 and 2

Rule Z contains 3 ***ingress FE*** ports, 2 ***ingress GE*** ports, and 5 ***egress GE*** ports.
It results in the number of 3 x 5 = 15 in Limitation 1, and 2 x 5 = 10 in Limitation 2.
Make sure the amount in limitation 1, "15", is not greater than 160.
Make sure the amount in limitation 2, "10", is not greater than 40.

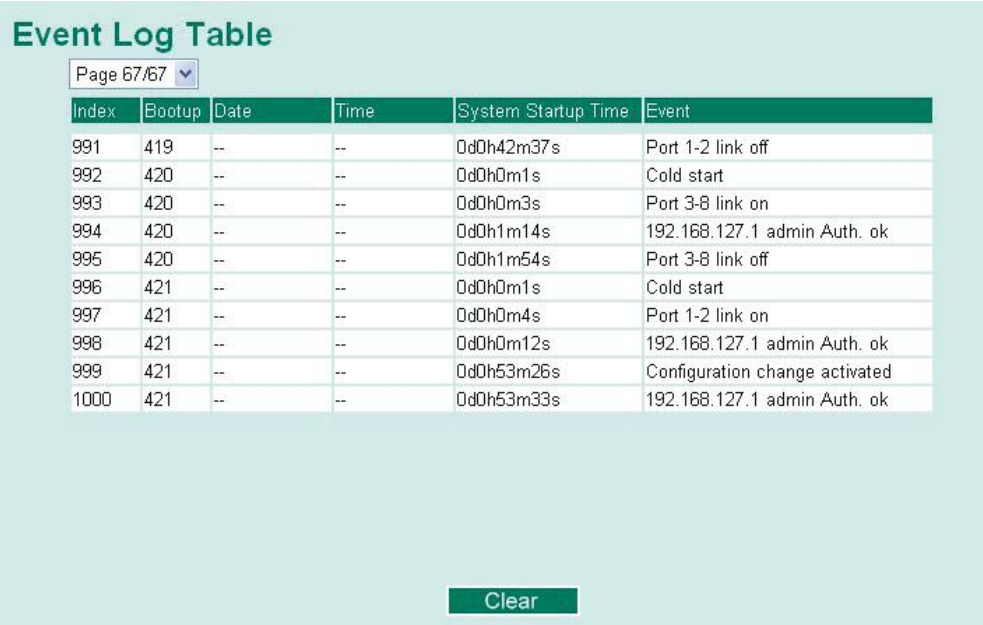
NOTE

EDS-828 and PT-7828 series switches only provide **6 Types** of ACL rules.

NOTE

For EDS-828 and PT-7828 series, Broadcast and Multicast traffic filters are **NOT** supported on egress ports of ACL settings. On the other hand, Broadcast's and Multicast's Addresses are not allowed to be set in Source/Destination Addresses.

Using Event Log



The Event Log Table displays the following information:

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

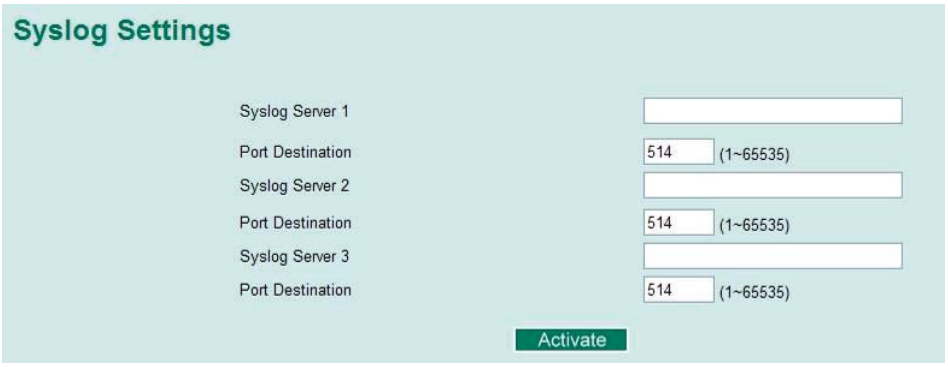
NOTE

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

- Cold start
- Warm start
- Configuration change activated
- Power 1/2 transition (Off (On), Power 1/2 transition (On (Off))
- Authentication fail
- Topology changed
- Master setting is mismatched
- Port traffic overload
- dot1x Auth Fail
- Port link off/on

Using Syslog

The Syslog function provides the event logs for the syslog server. The function supports 3 configurable syslog servers and syslog server UDP port numbers. When an event occurs, the event will be sent as a syslog UDP packet to the specified syslog servers.



Syslog Server 1/2/3

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

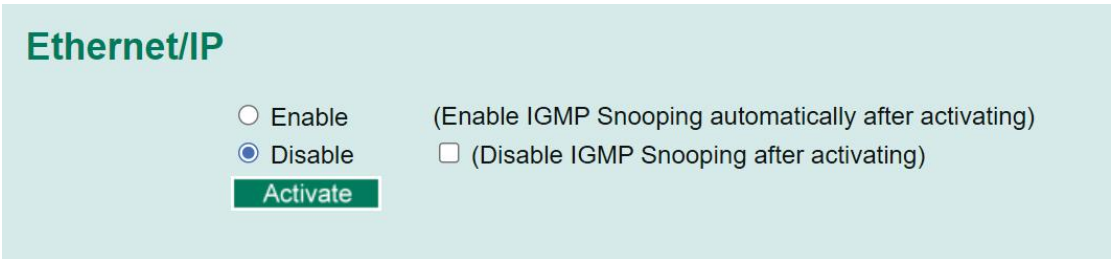
NOTE

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

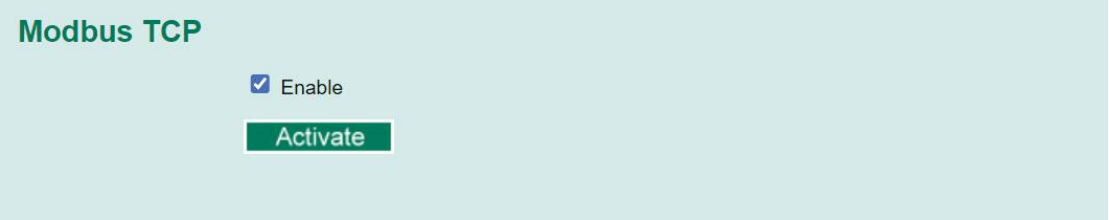
- Cold start
- Warm start
- Configuration change activated
- Power 1/2 transition (Off (On), Power 1/2 transition (On (Off))
- Authentication fail
- Topology changed
- Master setting is mismatched
- Port traffic overload
- dot1x Auth Fail
- Port link off/on

Using Industrial Protocols

The Moxa switch supports two industrial protocols, EtherNet/IP and Modbus TCP. Ethernet/IP is disabled by default. Modbus TCP is enabled by default.



Use the corresponding radio buttons to enable or disable EtherNet/IP. When EtherNet/IP is enabled, IGMP Snooping will also be enabled automatically. When EtherNet/IP is disabled, IGMP Snooping will continue to be active. If IGMP should be disabled if EtherNet/IP is disabled, check the corresponding box on the right-hand side.

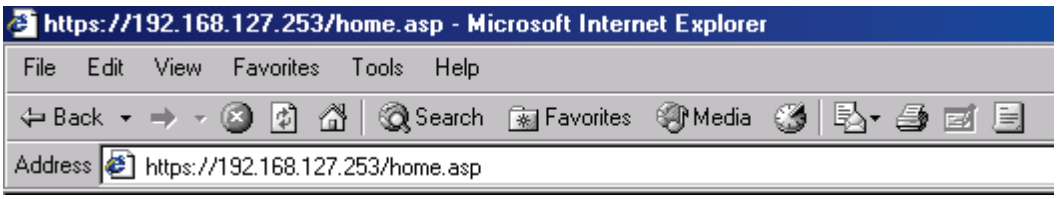


Check the corresponding checkbox to enable or disable Modbus TCP.

Using HTTPS/SSL

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

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



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

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

NOTE

Moxa provides a Root CA certificate. After installing this certificate on your PC or notebook, you can access the web browser interface directly and you will no longer see any warning messages.

4. EDS Configurator GUI

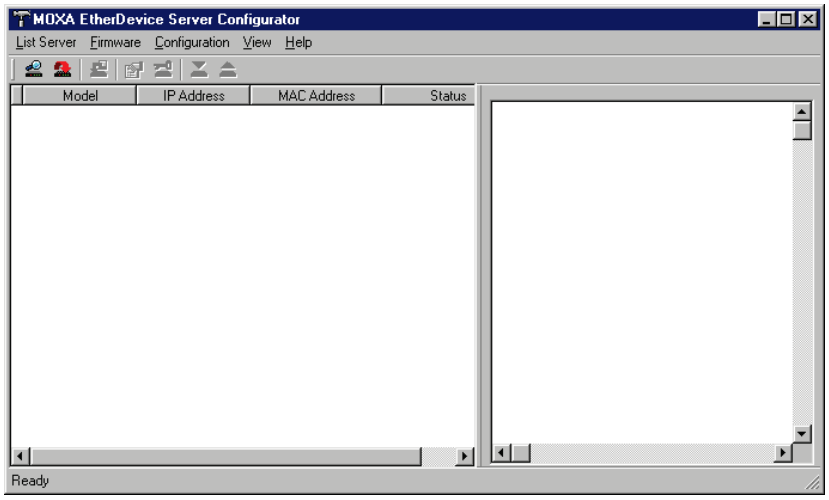
EDS Configurator is a comprehensive Windows-based GUI that is used to configure and maintain multiple Moxa switches. A suite of useful utilities is available to help you locate Moxa switches attached to the same LAN as the PC host (regardless of whether or not you know the IP addresses of the switches), connect to a Moxa switch whose IP address is known, modify the network configurations of one or multiple Moxa switches, and update the firmware of one or more Moxa switch. EDS Configurator is designed to provide you with instantaneous control of all of your Moxa switches, regardless of location. You may download the EDS Configurator software from Moxa's website free of charge.

Starting EDS Configurator

To start EDS Configurator, locate and run the executable file **edscfgui.exe**. There are two ways to do this:

- If the file was placed on the Windows desktop, it should appear as shown below. Simply double click the icon to run the program.

- The Moxa EtherDevice Server Configurator window will open, as shown below.



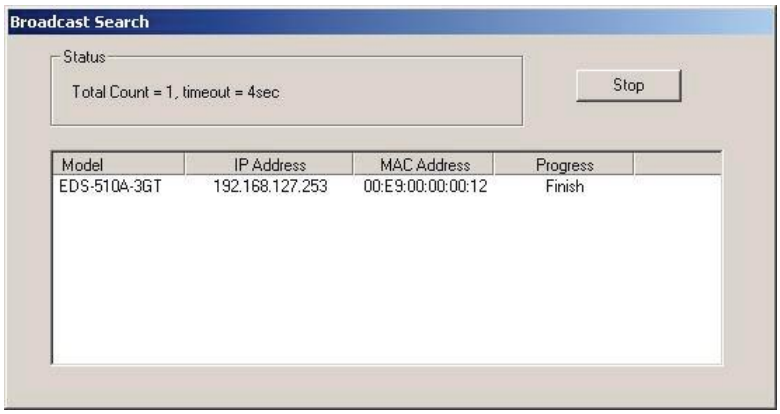
NOTE

You may download the EDS Configurator software free of charge from Moxa's website at www.moxa.com.

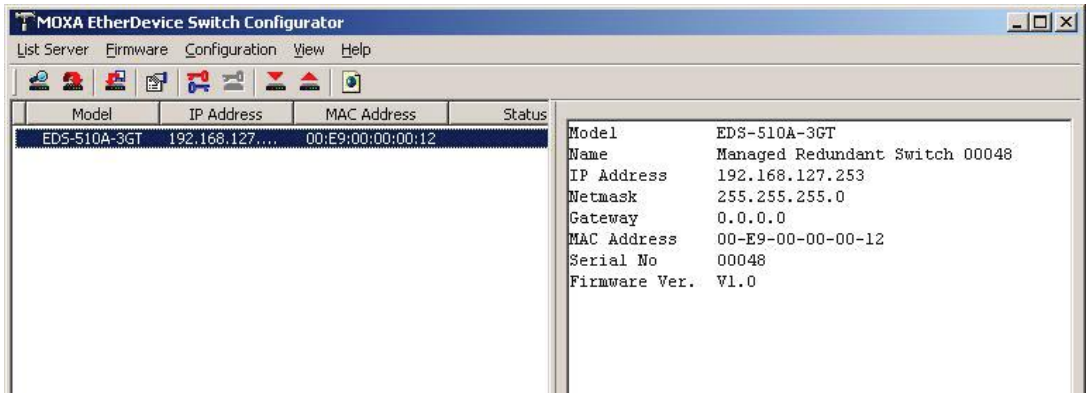
Broadcast Search

Use the **Broadcast Search** utility to search the LAN for all Moxa switches that are connected to the LAN. Note that since the search is done by MAC address. **Broadcast Search** will not be able to locate Moxa EtherDevice switches connected outside the PC host's LAN.

1. Start by clicking the Broadcast Search icon , or select **Broadcast Search** under the **List Server** menu. The Broadcast Search window will open and display a list of all switches located on the network. Look in the **Progress** column to see the progress of the search.



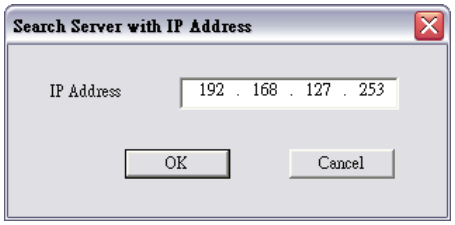
2. Once the search is complete, the Configurator window will display a list of all switches that were located.



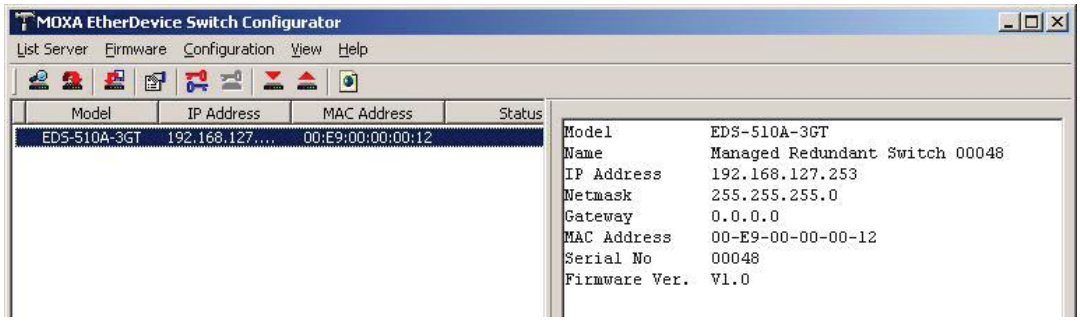
Search by IP Address

Use the **Search by IP Address** utility to search for Moxa switches one at a time. Note that the search is conducted by IP address, so you should be able to locate any Moxa switch that is properly connected to your LAN, WAN, or the Internet.

1. Start by clicking the **Specify by IP address** icon , or by selecting **Specify IP address** under the **List Server** menu. The **Search Server with IP Address** window will open. Enter the IP address of the switch you wish to search for, and then click **OK**.



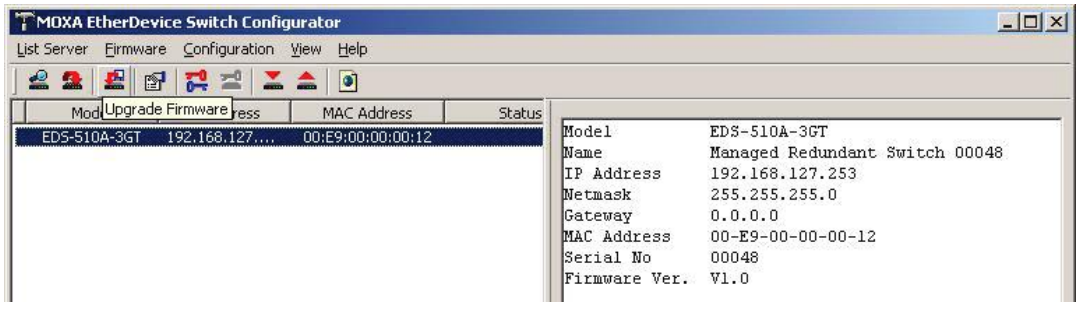
2. Once the search is complete, the Configurator window will add the switch to the list of switches.



Upgrade Firmware

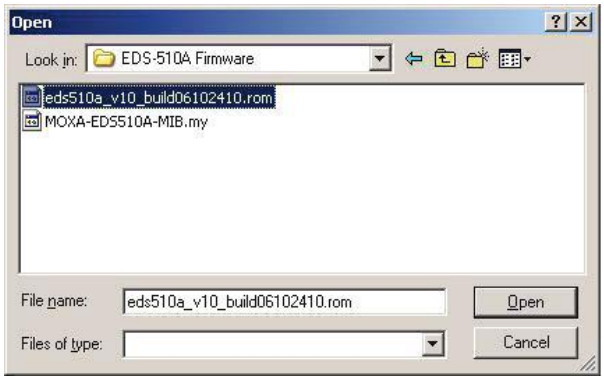
Keep your Moxa switch up to date with the latest firmware from Moxa. Perform the following steps to upgrade the firmware:

1. Download the updated firmware (*.rom) file from Moxa's website (www.moxa.com).
2. Click the switch (from the **Moxa EtherDevice Server Configurator** window) whose firmware you wish to upgrade to highlight it.



3. Click the **Upgrade Firmware** toolbar icon , or select **Upgrade** under the **Firmware** menu. If the switch is Locked, you will be prompted to input the switch's Username and Password.

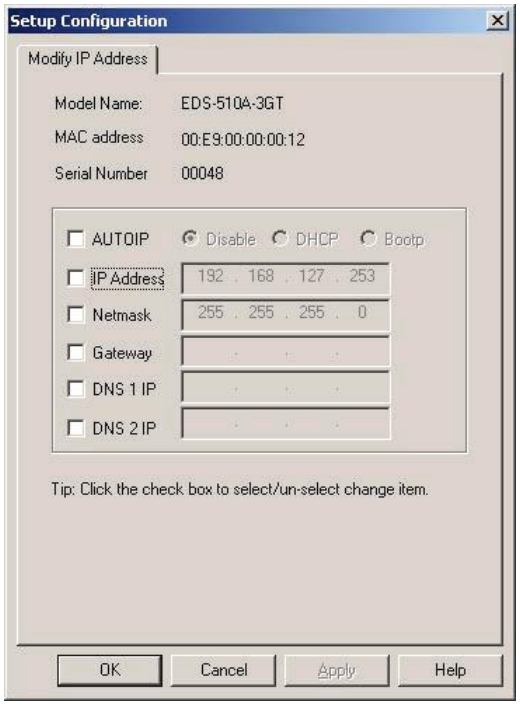
4. Use the **Open** window to navigate to the folder that contains the firmware upgrade file, and then click the correct "*.rom" file (**eds.rom** in the example shown below) to select the file. Click **Open** to activate the upgrade process.



Modify IP Address

You may use the **Modify IP Address** function to reconfigure the Moxa switch's network settings.

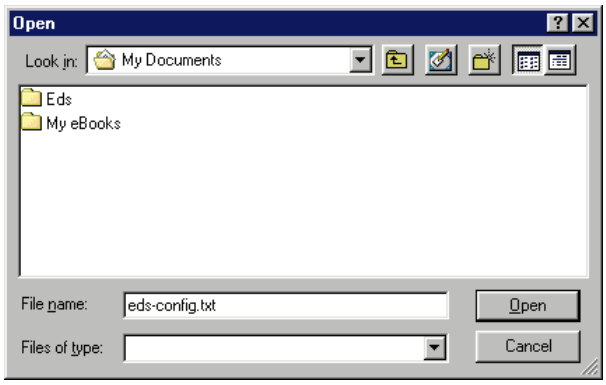
1. Start by clicking the Modify IP address icon , or by selecting **Modify IP address** under the **Configuration** menu.
2. The **Setup Configuration** window will open. Checkmark the box to the left of those items that you wish to modify, and then Disable or Enable DHCP, and enter the IP Address, Subnet mask, Gateway, and DNS IP. Click **OK** to accept the changes to the configuration.



Export Configuration

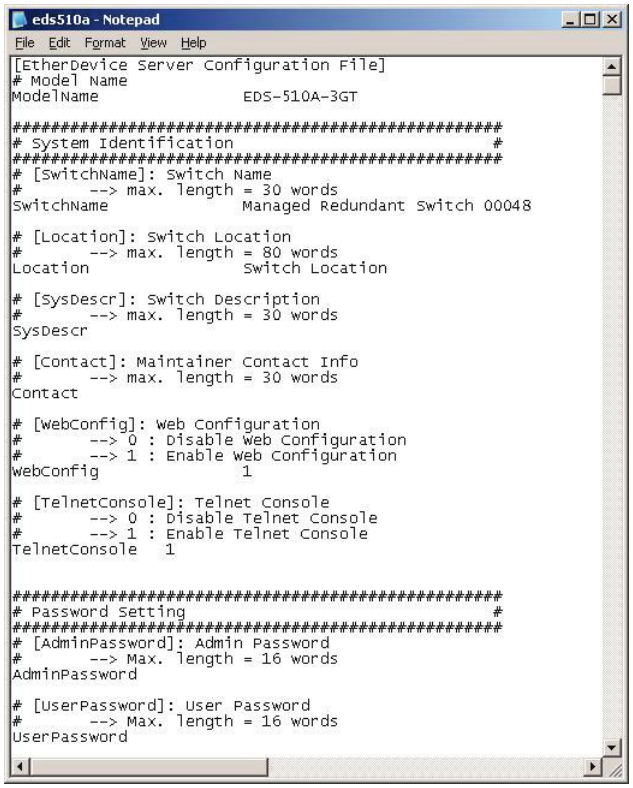
The **Export Configuration** utility is used to save the entire configuration of a particular Moxa switch to a text file. Take the following steps to export a configuration:

1. Highlight the switch (from the Server list in the Configurator window's left pane), and then click the **Export** toolbar icon or select **Export Configuration** from the **Configuration** menu. Use the **Open** window to navigate to the folder in which you would like to store the configuration, and then type the name of the file in the **File name** input box. Click **Open** to continue.



2. Click **OK** when the **Export configuration to file OK** message appears.

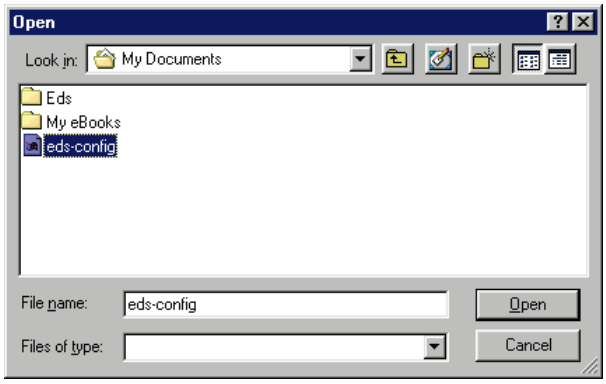
3. You may use a standard text editor, such as Notepad under Windows, to view and modify the newly created configuration file.



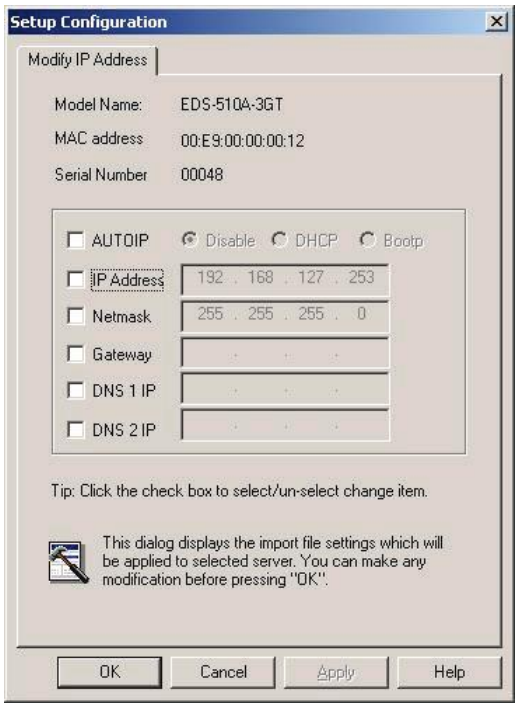
Import Configuration

The **Import Configuration** function is used to import an entire configuration from a text file to the Moxa switch. The utility can be used to transfer the configuration from one Moxa switch to another, by first using the Export Configuration function (described in the previous section) to save a switch configuration to a file, and then using the Import Configuration function. Perform the following steps to import a configuration:

1. Highlight the server (from the Moxa EtherDevice Switch list in the Configurator window's left pane), and then click the **Import** toolbar icon , or select **Import Configuration** from the **Configuration** menu.
2. Use the **Open** window to navigate to the text file that contains the desired configuration. Once the file is selected, click **Open** to initiate the import procedure.



3. The **Setup Configuration** window will be displayed, with a special note attached at the bottom. Parameters that have been changed will be indicated with a checkmark. You may make more changes if necessary, and then click **OK** to accept the changes.



4. Click **Yes** in response to the following warning message to accept the new settings.

Unlock Server

The **Unlock Server** function is used to open a password protected switch so that the user can modify its configuration, import/export a configuration, and perform other procedures. There are six possible responses under the **Status** column. The **Status** of a Moxa switch indicates how Moxa EtherDevice Switch Configurator located the switch, and what type of password protection it has.

The six options are as follows (note that the term **Fixed** is borrowed from the standard fixed IP address networking terminology):

- **Locked**

  The switch is password protected, **Broadcast Search** was used to locate it, and the password has not yet been entered from within the current Configurator session.

- **Unlocked**

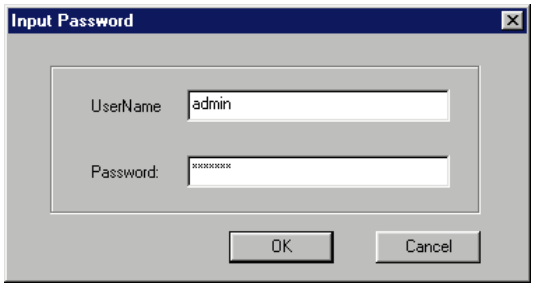
  The switch is password protected, **Broadcast Search** was used to locate it, and the password was entered from within the current Configurator session. Henceforth during this Configurator session, activating various utilities for this switch will not require re-entering the server password.

- **Blank**

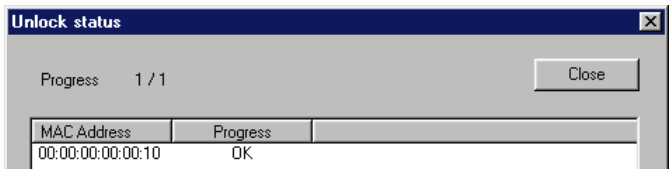
  The Moxa switch is not password protected, and **Broadcast Search** was used to locate it.

Follow the steps given below to unlock a locked Moxa switch (i.e., Moxa switch with Status "Locked" or "Locked Fixed"). Highlight the server (from the Moxa EtherDevice Switch list in the Configurator window's left pane), and then click the **Unlock** toolbar icon , or select **Unlock** from the **Configuration** menu.

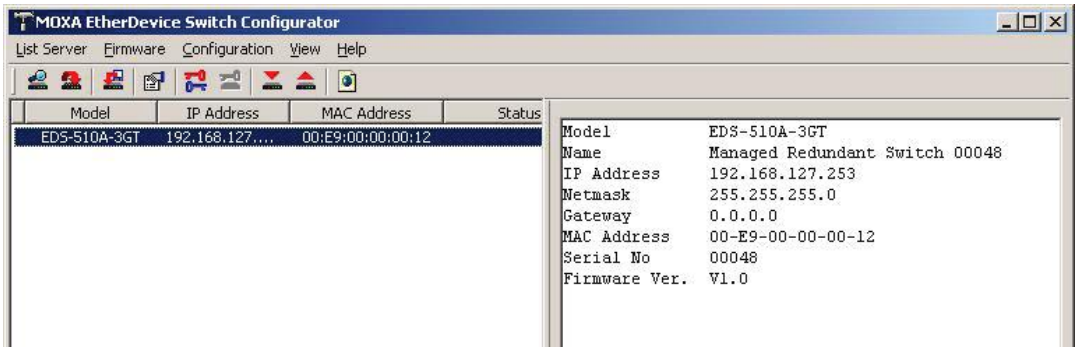
1. Enter the switch's **Username** and **Password** when prompted, and then click **OK**.



2. When the **Unlock status** window indicates the Progress as **OK**, click the **Close** button in the upper right corner of the window.



3. The status of the switch will now be shown as **Unlocked**.



A. MIB Groups

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

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

MIB II.1—System Group

sysORTable

MIB II.2—Interfaces Group

ifTable

MIB II.4 – IP Group

ipAddrTable

ipNetToMediaTable

IpGroup

IpBasicStatsGroup

IpStatsGroup

MIB II.5—ICMP Group

IcmpGroup

IcmpInputStatus

IcmpOutputStats

MIB II.6—TCP Group

tcpConnTable

TcpGroup

TcpStats

MIB II.7—UDP Group

udpTable

UdpStats

MIB II.10—Transmission Group

dot3

dot3StatsTable

MIB II.11—SNMP Group

SnmpBasicGroup

SnmpInputStats

SnmpOutputStats

MIB II.17—dot1dBridge Group

dot1dBase

dot1dBasePortTable

dot1dStp

dot1dStpPortTable

dot1dTp

dot1dTpFdbTable

dot1dTpPortTable

dot1dTpHCPortTable

dot1dTpPortOverflowTable

pBridgeMIB

dot1dExtBase

dot1dPriority

dot1dGarp

qBridgeMIB

dot1qBase

dot1qTp

dot1qFdbTable

dot1qTpPortTable

dot1qTpGroupTable

dot1qForwardUnregisteredTable

dot1qStatic

dot1qStaticUnicastTable

dot1qStaticMulticastTable

dot1qVlan

dot1qVlanCurrentTable

dot1qVlanStaticTable

dot1qPortVlanTable

The private MIB file can be downloaded from Moxa's website: www.moxa.com.

Public Traps

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

Private Traps

- Configuration Changed
- Power On
- Power Off
- Traffic Overloaded
- Turbo Ring Topology Changed
- Turbo Ring Coupling Port Changed
- Turbo Ring Master Mismatch