

Moxa Managed DSL Ethernet Extender Switch User's Manual

Edition 1.0, April 2016

www.moxa.com/product

Models covered by this manual:

IEX-408E-2VDSL2 series



© 2016 Moxa Inc. All rights reserved.

Moxa Managed DSL Ethernet Extender Switch User's 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

© 2016 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

Moxa Americas

Toll-free: 1-888-669-2872

Tel: +1-714-528-6777

Fax: +1-714-528-6778

Moxa Europe

Tel: +49-89-3 70 03 99-0

Fax: +49-89-3 70 03 99-99

Moxa India

Tel: +91-80-4172-9088

Fax: +91-80-4132-1045

Moxa China (Shanghai office)

Toll-free: 800-820-5036

Tel: +86-21-5258-9955

Fax: +86-21-5258-5505

Moxa Asia-Pacific

Tel: +886-2-8919-1230

Fax: +886-2-8919-1231

Table of Contents

1. About this Manual	1-1
2. Getting Started	2-1
USB Console Configuration (115200, None, 8, 1, VT100).....	2-2
Configuration by Command Line Interface (CLI)	2-5
Configuration by Web Browser	2-6
Disabling Telnet and Browser Access.....	2-8
3. Featured Functions	3-1
Home.....	3-2
System Settings	3-2
System Information.....	3-2
User Account	3-3
Network.....	3-5
Date and Time	3-7
Warning Notification	3-8
MAC Address Table.....	3-13
System Files.....	3-14
Turbo Ring DIP Switch	3-18
Restart.....	3-19
Factory Default	3-19
VLAN.....	3-19
The Virtual LAN (VLAN) Concept.....	3-19
Sample Applications of VLANs Using Moxa Ethernet extender switches.....	3-22
Configuring a Virtual LAN	3-23
VLAN Table.....	3-25
Port	3-26
Port Settings.....	3-26
Port Status	3-27
xDSL Port Settings	3-27
xDSL Port Status.....	3-30
Link Aggregation	3-31
Link-Swap Fast Recovery	3-33
Multicast.....	3-33
The Concept of Multicast	3-33
The Concept of Multicast Filtering and Management.....	3-34
IGMP Snooping	3-36
IGMP Snooping Setting	3-36
IGMP Group Status.....	3-37
Static Multicast Address	3-38
GMRP.....	3-38
QoS	3-39
The Traffic Prioritization Concept	3-39
Configuring Traffic Prioritization	3-41
CoS Classification	3-41
CoS Mapping	3-42
DSCP Mapping	3-43
Rate Limiting	3-43
Security.....	3-45
Login Authentication	3-45
Management Interface	3-46
Trusted Access.....	3-47
Authentication Certificate	3-48
IEEE 802.1X	3-48
IEEE 802.1X Setting	3-49
Local Database	3-50
RADIUS Server Settings	3-51
Port Security.....	3-51
Port Access Control Table	3-52
Broadcast Storm Protection	3-52
Loop Protection	3-52
DHCP	3-53
IP-Port Binding.....	3-53
DHCP Relay Agent	3-53
SNMP	3-55
SNMP Read/Write Settings.....	3-56
Trap Settings	3-57
Industrial Protocol	3-58
Diagnostics	3-59
LLDP.....	3-59

Ping	3-60
Port Mirror.....	3-60
Monitoring	3-60
CPU/Memory Utilization.....	3-61
Statistics	3-61
Event Log.....	3-63

A. MIB Groups A-1

About this Manual

Thank you for purchasing a Moxa managed DSL Ethernet extender switch. Read this user's manual to learn how to connect your Moxa Ethernet extender 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 an Moxa Ethernet extender switch. There are three ways to access an Moxa Ethernet extender switch's configuration settings: USB console interface, Telnet command line interface, and web-based interface.

□ **Chapter 3: Featured Functions**

This chapter explains how to access an Moxa Ethernet extender switch's various configuration, monitoring, and administration functions. These functions can be accessed by serial, Telnet command line, or web-based interface. As the web-based interface is the most user-friendly way to configure an Moxa Ethernet extender 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 an Moxa Ethernet extender switch for the first time. There are three ways to access the Moxa Ethernet extender switch's configuration settings: USB console, command line interface, or web-based interface. If you do not know the Moxa Ethernet extender switch's IP address, you can open the USB console by connecting the Moxa Ethernet extender switch to a PC's USB port with a USB cable. You can open the Telnet or web-based console over an Ethernet LAN or over the Internet.

The following topics are covered in this chapter:

- ❑ **USB Console Configuration (115200, None, 8, 1, VT100)**
- ❑ **Configuration by Command Line Interface (CLI)**
- ❑ **Configuration by Web Browser**
- ❑ **Disabling Telnet and Browser Access**

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

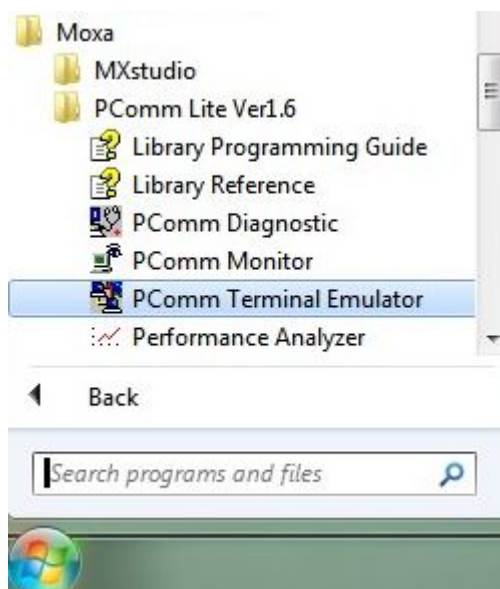
- NOTE**
- You cannot connect to the USB console and command line interface at the same time.
 - You can connect to the web console and another console (serial or Telnet) at the same time. However, we strongly recommend that you do NOT do so. Following this advice will allow you to maintain better control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

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

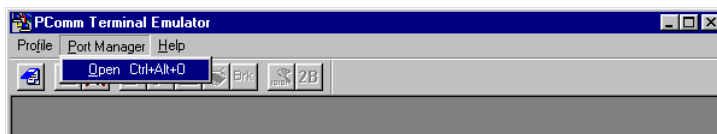
Before running PComm Terminal Emulator, first install the USB console driver on your PC and then connect the Moxa Ethernet extender switch's USB console port to your PC's USB port with a USB cable.

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

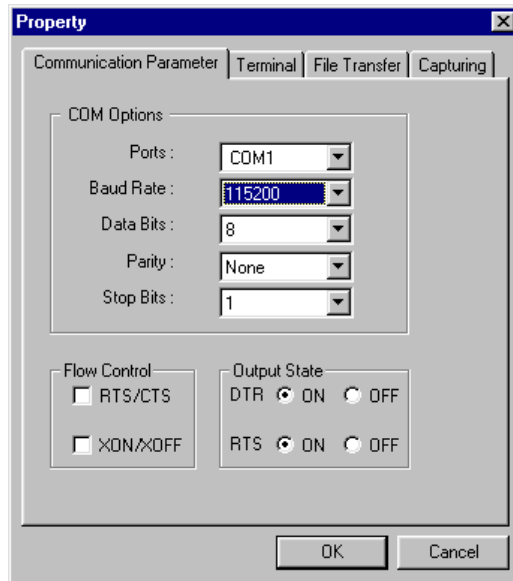
1. From the Windows desktop, click **Start > Moxa > PComm Lite Ver1.6 > Terminal Emulator**.



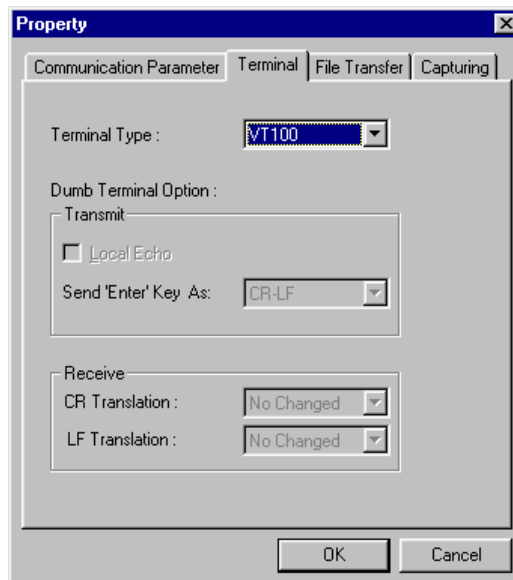
2. Select **Open** under the **Port Manager** menu to open a new connection.



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.



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

```
MOXA EtherDevice Switch  EDS-510E-3GTXSFP
Console terminal type (1: ansi/vt100, 2: vt52) : 1
```


- The USB 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 :          EDS-510E-3GTXSFP
Name :
Location :       Switch Location

Firmware Version : V3.3 build 13061918
Serial No :       03131
IP :              192.168.127.124
MAC Address :     00-90-E8-22-52-25

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

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

- The **Main Menu** of the Moxa Ethernet extender switch’s USB console should appear. (In PComm Terminal Emulator, you can adjust the font by selecting **Font...** from the **Edit** menu.)

```

                                EDS-510E series V3.3 build 13061918
-----
1.Basic Settings      - Basic settings for network and system parameter.
2.Port Trunking       - Allows multiple ports to be aggregated as a link.
3.SNMP                - The settings for SNMP.
4.Redundant Protocol - Establish Ethernet communication redundant path.
5.QoS                 - Prioritize Ethernet traffic to help determinism.
6.VLAN                - Set up a VLAN by IEEE802.1Q VLAN or Port-based VLAN.
7.Multicast           - Enable the multicast filtering capability.
8.Rate Limiting       - Restrict unpredictable network traffic.
9.Security            - Port access control by IEEE802.1X or Static Port Lock.
a.Warning Notification - Warning email and/or relay output by events.
b.Link-Swap Recovery  - Fast recovery after moving devices to different ports.
c.DHCP                - Assign IP addresses to connected devices.
d.Diagnostics         - Ping command and the settings for Mirror port, LLDP.
e.Monitoring          - Monitor a port and network status.
f.MAC Address Table   - The complete table of Ethernet MAC Address List.
g.System log          - The settings for Syslog and Event log.
h.Exit                - Exit
                    - Use the up/down arrow keys to select a category,
                    and then press Enter to select. -
    
```

- Use the following keys on your keyboard to navigate the Moxa Ethernet extender switch’s USB 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 Command Line Interface (CLI)

Opening the Moxa Ethernet extender switch's Telnet or web console over a network requires that the PC host and Moxa Ethernet extender 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 Ethernet extender switch's IP address is 192.168.127.253 and the Moxa Ethernet extender 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.

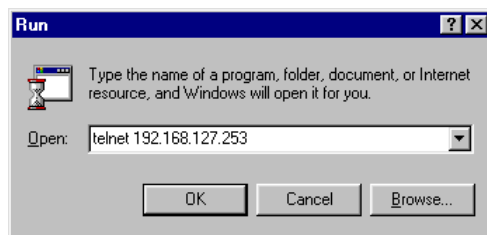
NOTE To connect to the Moxa Ethernet extender switch's Telnet or web console, your PC host and the Moxa Ethernet extender switch must be on the same logical subnet.

NOTE When connecting to the Moxa Ethernet extender switch's Telnet or web console, first connect one of the Moxa Ethernet extender 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 Ethernet extender switch's default IP address is 192.168.127.253.

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

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



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

```
MOXA EtherDevice Switch  EDS-510E-3GTXSFP
Console terminal type (1: ansi/vt100, 2: vt52) : 1
```

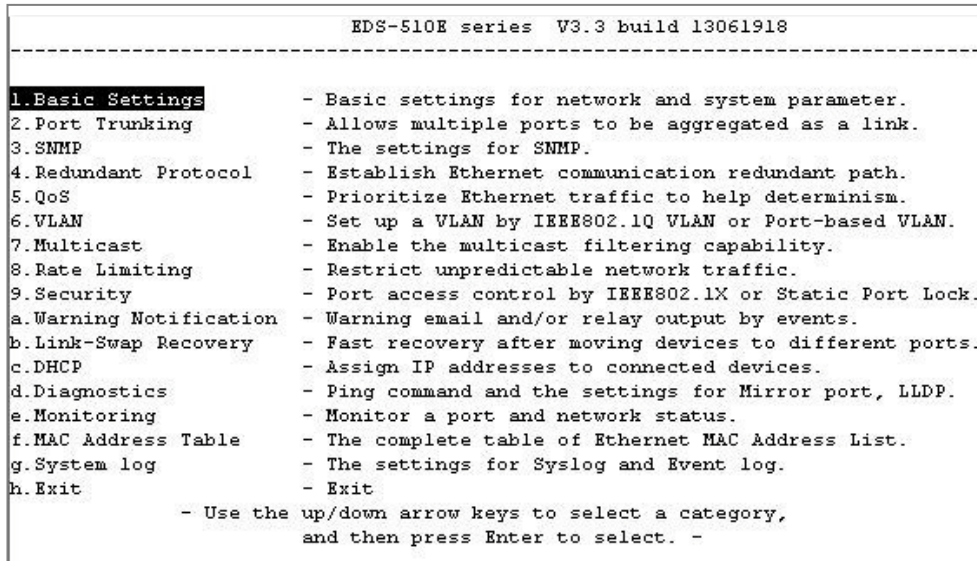
3. The Telnet console will prompt you to log in. Press **Enter** and then select **admin** or **user**. Use the down arrow key on your keyboard to select the **Password** field and enter a password if desired. This password will be required to access any of the consoles (web, serial, Telnet). If you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

```
Model :                EDS-510E-3GTXSFP
Name :
Location :            Switch Location

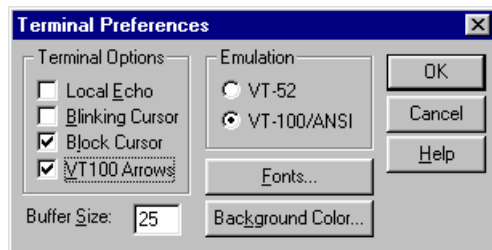
Firmware Version :    V3.3 build 13061918
Serial No :           03131
IP :                  192.168.127.124
MAC Address :         00-90-E8-22-52-25

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

4. The **Main Menu** of the Moxa Ethernet extender 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 the Moxa Ethernet extender 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 USB console.

Configuration by Web Browser

The Moxa Ethernet extender 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 Ethernet extender switch’s web console using a standard web browser, such as Internet Explorer.

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

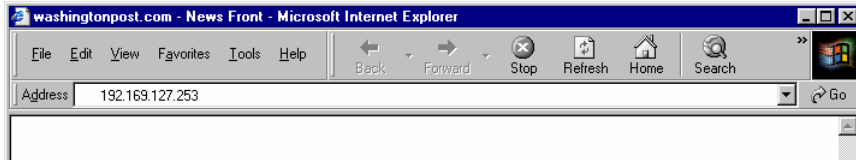
NOTE If the Moxa Ethernet extender switch is configured for other VLAN settings, you must make sure your PC host is on the management VLAN.

NOTE When connecting to the Moxa Ethernet extender switch’s Telnet or web console, first connect one of the Moxa Ethernet extender 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.

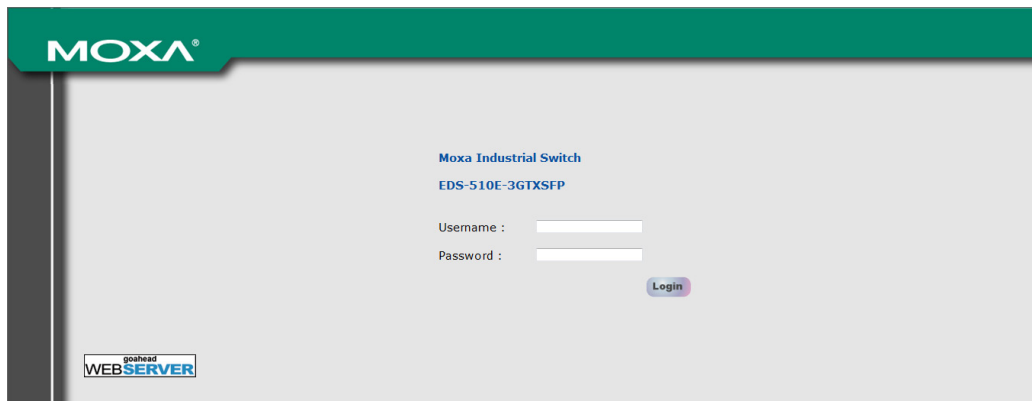
NOTE The Moxa Ethernet extender switch’s default IP address is 192.168.127.253.

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

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

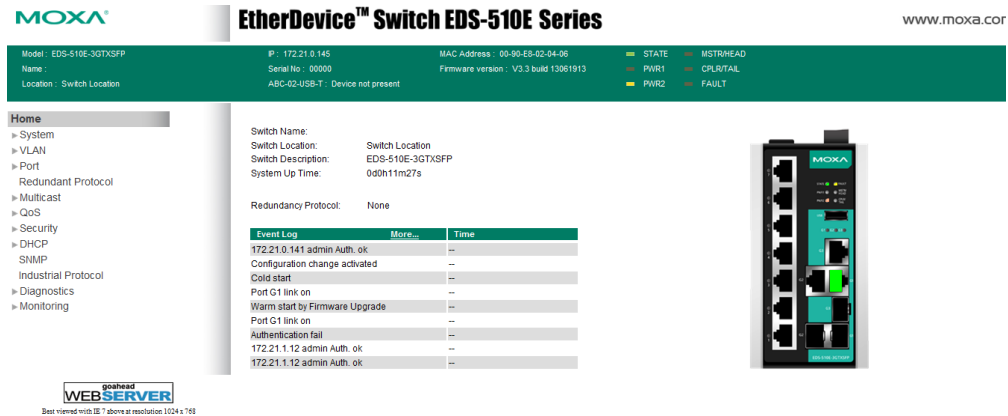


2. The Moxa Ethernet extender switch’s web console will open, and you will be prompted to log in. Select the login account (admin or user) and enter the **Password**. This password will be required to access any of the consoles (web, serial, Telnet). If you do not wish to create a password, leave the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



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

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



Disabling Telnet and Browser Access

If you are connecting the Moxa Ethernet extender 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 USB console by navigating to **System Identification** under **Basic Settings**. Disable or enable the **Telnet Console** and **Web Configuration** as shown below:

```

MOXA EtherDevice Switch EDS-510E-3GTXSFP
Basic Settings
[System Information] [User Account] [Trusted Access] [Port] [Network]
[Date and Time] [DIP] [GARP Timer] [Restart] [Factory default]
[Firmware Upgrade] [Config File] [Login mode] [Activate] [Main menu]
System Identification
ESC: Previous menu  Enter: Select  Space bar: Toggle

Switch Name          [ | ]
Switch Location      [Switch Location ]
Switch Description   [EDS-510E-3GTXSFP ]
Contact Information  [ ]

Serial NO.           03131
Firmware Version     V3.3 build 13061918
MAC Address          00-90-E8-22-52-25

Telnet Console       [Enable ]
Web Configuration    [http or https]
Web Auto-logout (s) [300 ]
Age-time (s)        [300 ]

```

Featured Functions

In this chapter, we explain how to access the Moxa Ethernet extender switch's various configuration, monitoring, and administration functions. These functions can be accessed by serial, Telnet, or web console. The USB console can be used if you do not know the Moxa Ethernet extender switch's IP address. To access the USB console, connect switch's USB port to your PC's 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 an Moxa Ethernet extender switch. In this chapter, we use the web console interface to introduce the console functions. There are only a few differences between the web console, USB console, and Telnet console.

The following topics are covered in this chapter:

- ❑ **Home**
- ❑ **System Settings**
- ❑ **VLAN**
- ❑ **Port**
- ❑ **Multicast**
- ❑ **QoS**
- ❑ **Security**
- ❑ **DHCP**
- ❑ **SNMP**
- ❑ **Industrial Protocol**
- ❑ **Diagnostics**
- ❑ **Monitoring**

Home

The **Home** page shows the summary of the Moxa Ethernet extender switch information including System Information, Redundancy Protocol, Event Log, and Device virtualization panel. With the organized key summary, the operators can easily understand the system and port link status at a glance.

Switch Name:

Switch Location: Switch Location

Switch Description: IEX-408E-2VDSL2

System Up Time: 0d0h13m29s

Redundancy Protocol: Turbo Ring V2

Event Log	More...	Time
192.168.127.99 admin Auth. ok		2016/03/27, 14:29
Port 6 link off		2016/03/27, 14:29
Port 5 link on		2016/03/27, 14:29
192.168.127.99 admin Auth. ok		2016/03/27, 14:29
Topology changed		2016/03/27, 14:30
Configuration change activated		2016/03/27, 14:30
Turbo Ring - Ring Master is changed.		2016/03/27, 14:30
Port 5 link off		2016/03/27, 14:30
Port 6 link on		2016/03/27, 14:30



System Settings

The **System Settings** section includes the most common settings required by administrators to maintain and control an Moxa Ethernet extender switch.

System Information

Define **System Information** items to make it easier to identify different pieces of network equipment that are connected to your network.

System Information

Switch Name

Switch Location

Switch Description

Contact Information

[Apply](#)

Switch Name

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

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

Switch Location

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

Switch Description

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

Contact Information

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

User Account

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

- NOTE**
1. In order to maintain a higher level of security, we strongly suggest that you change the password after you first log in.
 2. By default, the **admin** user account cannot be deleted or disabled.

User Account

Active

Authority

User Name

Password

Confirm Password

Account List

Active	User Name	Authority
<input checked="" type="checkbox"/>	admin	admin
<input checked="" type="checkbox"/>	user	user

Active

Setting	Description	Factory Default
Checked	This account can access the switch’s configuration settings.	Checked
Unchecked	This account cannot access the switch’s configuration settings.	

Authority

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

Creating a New Account

When creating a new user account, please type in the user name and password, and assign an authority to the new account. Click **Create** to add the account to the **Account List** table.

Setting	Description	Factory Default
Authority	Privilege of the user account	admin
User Name (Max. of 30 characters)	User name set for the user account	None
Password	Password for the user account. (between 4 and 16 characters)	None
Confirm Password	Confirm the Password setting (between 4 and 16 characters)	None

Modifying an Existing Account

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

User Account

Active

Authority admin

User Name admin

Old Password

Password

Confirm Password

Create
Apply

Account List

Active	User Name	Authority	
<input checked="" type="checkbox"/>	admin	admin	
<input checked="" type="checkbox"/>	user	user	Delete

Deleting an Existing Account

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

User Account

Active

Authority admin

User Name testuser1

Old Password

Password

Confirm Password

Create
Apply

Account List

Active	User Name	Authority	
<input checked="" type="checkbox"/>	admin	admin	
<input checked="" type="checkbox"/>	user	user	Delete
<input checked="" type="checkbox"/>	testuser1	admin	Delete

Would you like to delete account "testuser1"?

OK
CANCEL

Network

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

IP Settings

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

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

IP Settings

Get IP From	DHCP ▾
IP Address	172.21.0.145
Subnet Mask	25(255.255.255.128) ▾
Default Gateway	172.21.0.254
1st DNS Server	192.168.50.41
2nd DNS Server	192.168.50.33
IPv6 Global Unicast Address Prefix	
IPv6 Global Unicast Address	::
IPv6 Link-Local Address	fe80::290:e8ff:fe02:406

Get IP From

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

IP Address

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

Subnet Mask

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

Default Gateway

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

DNS Server IP Addresses

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

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

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

IPv6 Global Unicast Address

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

IPv6 Link-Local Address

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

IPv6 Neighbor Cache

The IPv6 neighbor cache includes the neighboring node's IPv6 address, the corresponding Link-Layer address, and the current state of the entry.

IPv6 Neighbor Cache		
IPv6 Address	Link Layer (MAC) Address	State
fe80::290:e8ff:fe02:406	00-90-e8-02-04-06	Reachable

Date and Time

The Moxa Ethernet extender switch has a time calibration function based on information from an NTP server or user specified time and date, allowing functions such as automatic warning emails to include a time and date stamp.

System Time

System Up Time: 0d0h50m1s Refresh

Current Time: 2016/03/27 15:06:57

Clock Source: Local NTP SNTP

Time Settings

Manual Time Settings

Date (YYYY/MM/DD): / /

Time (HH:MM:SS): : :

Sync. from Local Device Time 2016/3/27 15:7:1

Enable NTP/SNTP Server

Time Zone: ▼

Daylight Saving

	Month	Week	Day	Hour
Start Date	<input type="text" value="--"/> ▼	<input type="text" value="--"/> ▼	<input type="text" value="--"/> ▼	<input type="text" value="--"/> ▼
End Date	<input type="text" value="--"/> ▼	<input type="text" value="--"/> ▼	<input type="text" value="--"/> ▼	<input type="text" value="--"/> ▼
Offset(hr)	<input type="text" value="0"/> ▼			

Apply

System Up Time

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

Current Time

Setting	Description	Factory Default
User-specified time	Indicates time in the yyyy/mm/dd hh:mm:ss format.	None

Clock Source

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

Time Zone

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

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

Daylight Saving Time

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

Start Date

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

End Date

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

Offset

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

If the NTP or SNTP options are enabled, you will also need to configure the following settings.

Time Server IP / Name

Setting	Description	Factory Default
IP address or name of primary 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 Ethernet extender switch will try to locate the secondary NTP server if the first NTP server fails to connect.	

Enable NTP/SNTP Server

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

Warning Notification

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 Ethernet extender switch supports different approaches to warn engineers automatically, such as email, trap, syslog and relay output. It also supports one set of digital input to integrate sensors into your system to automate alarms by email and relay output.

System Event Settings

System Events are related to the overall function of the extender switch. Each event can be activated independently with different warning approaches. The Administrator also can decide the severity of each system event.

System Event Settings

Active	Event	Action				Severity
		Trap	E-Mail	Syslog	Relay1	
<input checked="" type="checkbox"/>	Cold Start	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>		Critical
<input checked="" type="checkbox"/>	Warm Start	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>		Warning
<input checked="" type="checkbox"/>	Config. Changed	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>		Warning
<input checked="" type="checkbox"/>	PWR 1 Off->On	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>		Warning
<input checked="" type="checkbox"/>	PWR 2 Off->On	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>		Warning
<input checked="" type="checkbox"/>	PWR 1 On->Off	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Warning
<input checked="" type="checkbox"/>	PWR 2 On->Off	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Warning
<input checked="" type="checkbox"/>	Auth. Fail	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>		Warning
<input checked="" type="checkbox"/>	Password Changed			<input checked="" type="checkbox"/>		Warning
<input checked="" type="checkbox"/>	TACACS+ Auth. Fail			<input checked="" type="checkbox"/>		Warning
<input checked="" type="checkbox"/>	TACACS+ Auth. Timeout			<input checked="" type="checkbox"/>		Warning

Apply

System Events	Description
Cold Start	Power is cut off and then reconnected.
Warm Start	The Moxa Ethernet extender switch is rebooted, such as when network parameters are changed (IP address, subnet mask, etc.).
Configuration Changed	Any configuration item has been changed.
Power Transition (Off→On)	The Moxa Ethernet extender switch is powered up.
Power Transition (On→Off)	The Moxa Ethernet extender switch is powered down.
Authentication Fail	An incorrect password was entered.
Password Changed	User changes the account password.
TACACS+ Authentication Fail	Incorrect authentication details were entered.
TACACS+ Authentication Timeout	Timed out when attempting to get authenticated from TACACS+ sever.
RADIUS Authentication Fail	Incorrect authentication details were entered.
RADIUS Authentication Timeout	Timed out when attempting to get authenticated from RADIUS sever.
Topology Changed	<ul style="list-style-type: none"> If the Master of the Turbo Ring has changed or the backup path is activated. If the Turbo Ring path is disconnected. If the MSTP topology has changed.
Coupling Changed	Backup path of the Coupling is activated.
Master Changed	Master of the Turbo Ring has changed.
RSTP Root Changed	If the RSTP root has changed.
RSTP Topology Changed	If any Rapid Spanning Tree Protocol switches have changed their position (applies only to the root of the tree).
Turbo Ring Break	Turbo Ring path is disconnected.
DI1 (On→Off)	Digital Input 1 is triggered by an on to off transition.
DI1 (Off→On)	Digital Input 1 is triggered by an off to on transition.
ABC-02 Status	Detects if the ABC-02-USB-T is connected or disconnected to the switch when the ABC-02-USB-T automatically imports/exports/back-up the configuration.
Web Login	Any account has logged in to the web-based configuration console.
Rate Limit On/Off	When the port is disabled due to the ingress throughput exceeds the configured rate limit.
Port Looping	Port looping event is triggered.
LLDP Table Changed	Nearly connected devices are changed and shown in the LLDP table.
VDSL Train Fail	Attempt to establish DSL connection has failed.

Four response actions are available on the Moxa Ethernet extender switch when events are triggered.

Action	Description
Trap	The Moxa Ethernet extender switch will send a notification to the trap server when event is triggered.
E-Mail	The Moxa Ethernet extender switch will send a notification to the email server defined in the Email Setting.
Syslog	The Moxa Ethernet extender switch will record a syslog to syslog server defined in Syslog Server Setting.
Relay	When an event is triggered, the Moxa Ethernet extender switch will automate alarms through the relay output.

Severity

Severity	Description
Emergency	System is unusable
Alert	Action must be taken immediately
Critical	Critical conditions
Error	Error conditions
Warning	Warning conditions
Notice	Normal but significant condition
Information	Informational messages
Debug	Debug-level messages

Port Event Settings

Port Events are related to the activity of a specific port.

Port Event Settings

Active	Port	Link			Traffic		Action				Severity
		On	Off	Overload	RX-Threshold (%)	Traffic-Duration (s)	Trap	E-Mail	Syslog	Relay1	
<input checked="" type="checkbox"/>	1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0	1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Warning
<input checked="" type="checkbox"/>	2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0	1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Warning
<input checked="" type="checkbox"/>	3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0	1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Warning
<input checked="" type="checkbox"/>	4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0	1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Warning
<input checked="" type="checkbox"/>	5	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0	1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Warning
<input checked="" type="checkbox"/>	6	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0	1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Warning
<input checked="" type="checkbox"/>	7	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0	1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Warning
<input checked="" type="checkbox"/>	G1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0	1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Warning
<input checked="" type="checkbox"/>	G2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0	1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Warning

Apply

Port Events	Warning e-mail is sent when...
Link-ON	The port is connected to another device.
Link-OFF	The port is disconnected (e.g., the cable is pulled out, or the opposing device shuts down).
Traffic-Overload	The port's traffic surpasses the Traffic-Threshold for that port (provided this item is Enabled).
RX-Threshold (%)	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.

Four response actions are available on the Moxa Ethernet extender switch when events are triggered.

Action	Description
Trap	The Moxa Ethernet extender switch will send a notification to the trap server when event is triggered.
E-Mail	The Moxa Ethernet extender switch will send a notification to the email server defined in the Email Setting.
Syslog	The Moxa Ethernet extender switch will record a syslog to syslog server defined in Syslog Server Setting.
Relay	When an event is triggered, the Moxa Ethernet extender switch will automate alarms through the relay output.

Severity

Severity	Description
Emergency	System is unusable
Alert	Action must be taken immediately
Critical	Critical conditions
Error	Error conditions
Warning	Warning conditions
Notice	Normal but significant condition
Information	Informational messages
Debug	Debug-level messages

NOTE The Traffic-Overload, RX-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.

Email Settings

Email Setup

Mail Server

TCP Port

User Name

Password

1st Recipient Email Address

2nd Recipient Email Address

3rd Recipient Email Address

4th Recipient Email Address

Mail Server

Setting	Description	Factory Default
IP address or url	The IP Address or url of the email server.	None

TCP Port

Setting	Description	Factory Default
TCP Port number	The TCP port number of your email server.	25

User Name

Setting	Description	Factory Default
---------	-------------	-----------------

Max. of 45 characters	Your email account name	None
-----------------------	-------------------------	------

Password Setting

Setting	Description	Factory Default
Password	The email account 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 Ethernet extender switch.	None

Sending a Test Email

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

Syslog Server Settings

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. Each Syslog server can be activated separately by checking the appropriate checkbox to enable it.

Syslog Settings

Syslog 1

Server

UDP Port (1~65535)

Syslog 2

Server

UDP Port (1~65535)

Syslog 3

Server

UDP Port (1~65535)

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 Ethernet extender switch's Event Log table, and will then be sent to the specified Syslog Server:

- Cold start
- Warm start
- Configuration change activated
- Power 1 or 2 transition: Off to On or On to Off
- Authentication fail
- Password change
- Redundancy protocol/topology change
- Master setting mismatch
- ABC-02 status
- Web Login
- Rate Limit on/off(Disable port)
- Port looping
- VDSL Train Fail
- Port traffic overload
- dot1x Auth Fail
- Port link off/on

Relay Warning Status

When a relay warning is triggered by either the system or port events, the administrator can turn off the hardware warning buzzer by clicking the **Apply** button. The event will still be recorded in the event list.

Relay Warning Status

Relay 1 Alarm Cut-Off (ACO)

Apply

Index	Event	Relay
-------	-------	-------

MAC Address Table

The MAC address table shows the MAC address list passed through the Moxa Ethernet extender switch. The Ageing time (15 to 3825 seconds) defines the length of time that a MAC address entry can remain in the Moxa Ethernet extender 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.

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

MAC Address Table

Ageing Time (sec)

All Page 1/2

Index	MAC	Type	Port
1	00-14-2a-da-16-da	Unicast(I)	G1
2	00-19-21-b0-26-98	Unicast(I)	G1
3	00-19-cb-d6-d9-06	Unicast(I)	G1
4	00-1e-4f-51-8a-b3	Unicast(I)	G1
5	00-1e-90-88-e8-1c	Unicast(I)	G1
6	00-21-9b-6f-a8-24	Unicast(I)	G1
7	00-23-54-e1-20-69	Unicast(I)	G1
8	00-90-e8-00-90-e8	Unicast(I)	G1
9	00-90-e8-20-0f-6d	Unicast(I)	G1
10	00-90-e8-2e-8f-1c	Unicast(I)	G1

Drop Down List

ALL	Select this item to show all of the Moxa Ethernet extender switch’s MAC addresses.
ALL Learned	Select this item to show all of the Moxa Ethernet extender switch’s Learned MAC addresses.
ALL Static	Select this item to show all of the Moxa Ethernet extender switch’s Static, Static Lock, and Static Multicast MAC addresses.
ALL Multicast	Select this item to show all of the Moxa Ethernet extender switch’s Static Multicast MAC addresses.
Port x	Select this item to show all of the MAC addresses on the dedicated port.

The MAC Address 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.

System Files

Firmware Upgrade

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

Local

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

Firmware Upgrade

Local
 TFTP Server
 Auto Backup Configurator (ABC-02)

Upgrade Firmware From

TFTP Server

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

The screenshot shows the 'Firmware Upgrade' section. At the top, there are three radio buttons: 'Local', 'TFTP Server' (which is selected), and 'Auto Backup Configurator (ABC-02)'. Below these are two input fields: 'Server IP' and 'Filename'. A green 'Upgrade' button is located at the bottom right of the form.

Auto Backup Configurator (ABC-02)

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

The screenshot shows the 'Firmware Upgrade' section with 'Auto Backup Configurator (ABC-02)' selected. It features a text input field labeled 'Upgrade Firmware From' with a 'Browse' button to its right. Below this is a large green file selection area containing the text '/MOXA' and '/HIS_INI', with a 'Select' button at the bottom right. A green 'Upgrade' button is positioned above the file selection area.

Configuration Backup and Restore

There are three ways to back up and restore your Moxa Ethernet extender switch's configuration: from a local configuration file, by remote TFTP server, and with Auto Backup Configurator (ABC-02).

The screenshot shows the 'Configuration Backup and Restore' section. It has three radio buttons: 'Local' (selected), 'TFTP Server', and 'Auto Backup Configurator (ABC-02)'. There are three main actions: 'Backup Configuration File to Local Device' with a 'Backup' button, 'Restore Configuration From' with a text input field, a 'Browse' button, and a 'Restore' button. At the bottom, there are two checkboxes: 'Auto load configuration from ABC to system when boot up' (checked) and 'Auto backup to ABC-02 when configuration change' (unchecked). An 'Apply' button is located at the bottom right.

Local

1. Click the **Backup** button to back up the configuration file (file will be assigned with "**Sys.ini**" as the file name and extension) to a local drive.
2. Browse for a configuration on a local disk, and then click the **Restore** button.

TFTP Server

1. Enter the TFTP Server's IP address.
2. Input the backup/restore file name (supports up to 54 characters, including the .ini file extension) and then click the **Backup/Restore** button.

Auto Backup Configurator (ABC-02)

Manually Backup and Restore

1. Click **Backup** to save the configuration file to the ABC-02. The file will be saved in the ABC-02's **Moxa** folder as a *.ini file (e.g., **Sys.ini**).

NOTE Note that two files will be saved to the ABC-02-USB's **Moxa** folder: **Sys.ini** and **MAC.ini**. The purpose of saving the two files is to identify which file will be used when **Auto load configuration from ABC to system when boot up** is activated.

MAC.ini is named using the last 6 digits of the switch's MAC address, without spaces.

2. Click **Browse** to select the configuration file, and then click **Restore** to start loading the configuration into your switch.

Automatically Backup and Restore

1. **Auto load configuration from ABC to system when boot up**
Enable this function by checking the **Auto load configuration from ABC to system when boot up** checkbox and then click **Apply**.

NOTE Note that this function is enabled by default.

Power off your switch first, and then plug in the ABC-02. When you power on your switch, the system will detect the configuration file on the ABC-02 automatically. The switch will recognize the file name, with the following sequence priority:

First priority: **MAC.ini**

Second priority: **Sys.ini**

If no matching configuration file is found, the fault LED light will turn on, and the switch will boot up normally.

NOTE MAC.ini is named using the last 6 digits of the switch's MAC address, without spaces.

2. **Auto backup to ABC-02 when configuration change**

Enable this function by checking the **Auto backup to ABC-02 when configuration change** checkbox and then click **Apply**. This function is disabled by default.

Then use Moxa ABC-02 which is capable of backing up switch configuration files automatically. While the ABC-02 is plugged into the switch, enable the **Auto backup to ABC-02 when configuration change** option, and then click **Apply**. Once this configuration is modified, the switch will back up the current configuration to the **/His_in** folder on the ABC-02. The file name will be the system date/time (MMDDHHmm.ini).

NOTE MM=month, DD=day, HH=hour, mm=minutes, from the system time.

Log File Backup

There are three ways to back up Moxa Ethernet extender switch's log files: from a the local drive, by remote TFTP server, and with Auto Backup Configurator (ABC-02).

Local

Click the **Backup** button to back up the log file (file will be assigned with "**Sys.log**" as file name and extension) to a local drive.

TFTP Server

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

Auto Backup Configurator (ABC-02)

Manually Backup

Click **Backup** to save the configuration file to the ABC-02. The file will be saved in the ABC-02's **Moxa** folder with filename and extension as **Sys.log**.

Automatically Backup

Auto backup of event log to prevent overwrite

This function is designed to maintain a long-term record of the switch's log files. Moxa Ethernet switches are capable of saving 1000 event log entries. When the 1000-entry storage limit is reached, the switch will delete the oldest saved event log. The ABC-02 can be used to back up these event logs. When the number of switch log entries reaches 1000, the ABC-02 will save the oldest 100 entries from the switch.

Enable the **Auto backup of event log to prevent overwrite**, and then click **Apply**. After that, when the ABC-02 is plugged into the switch, the event logs will always be saved to the ABC-02 automatically when the number of switch log entries reaches 1000. Each backup action saves the oldest 100 logs to the ABC-02 in one file, with the filename generated by the current system time as **MMDDHHmm.log**. The file is saved to the **His_log** folder.

NOTE MM=month, DD=day, HH=hour, mm=minutes, from the system time.

The log file includes following information:

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

Switch Reset Button

The Moxa Ethernet extender switch reset button can be used to quickly reset the switch’s configuration, and save the current configuration and log files to the ABC-02. Press the Reset button on top of the EDS switch to back up the current system configuration files and event logs to the ABC-02.

NOTE DO NOT remove the ABC-02 when performing an upgrade, backup, or restore.

Please refer to Moxa’s Ethernet Extender Switch Quick Installation Guide for the detailed instructions of the reset button.

Turbo Ring DIP Switch

The **Turbo Ring DIP Switch** page allows users to disable the 4th DIP switch located on the Moxa Ethernet extender switch’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:

Turbo Ring DIP Switch

Disable the Turbo Ring DIP Switch

1. To enable the entire set of Hardware DIP switches, uncheck the "Disable the Turbo Ring DIP Switch" option.
2. To disable the entire set of Hardware DIP switches, check the "Disable the Turbo Ring DIP Switch" option.

Set DIP switch as Turbo Ring
 Set DIP switch as Turbo Ring v2

[Apply](#)

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 the DSL D1/D2 ports or port 5 and port 6, do not use the fourth DIP switch to activate Turbo Ring’s settings. In this case, you should use the Web, Telnet, or Serial console to activate Turbo Ring’s settings.

NOTE Once you have activated the redundant features through the hardware DIP switches, the default ring ports are set to the DSL D1/D2 ports with the Ring Coupling or the Primary ports set to port 5. The Coupling Control or Backup port is set to port 6

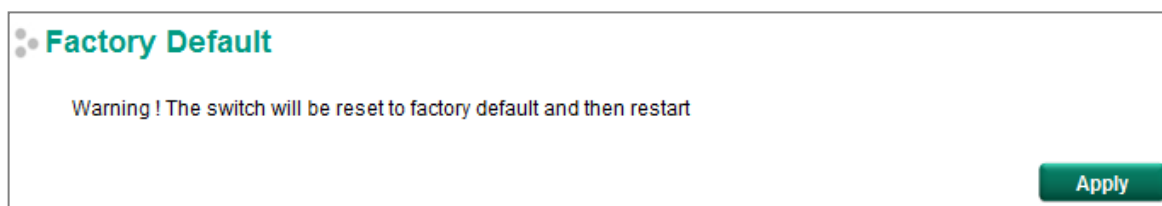
Restart

The **Restart** function provides users with a quick way to restart the Moxa Ethernet extender switch's operating system.



Factory Default

The **Factory Default** function provides users with a quick way of restoring the Moxa Ethernet extender switch's configuration to factory defaults. The function can be activated from the USB serial interface, via Telnet, through the web-based console, and with the hardware reset button.



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 Ethernet extender switch.

VLAN

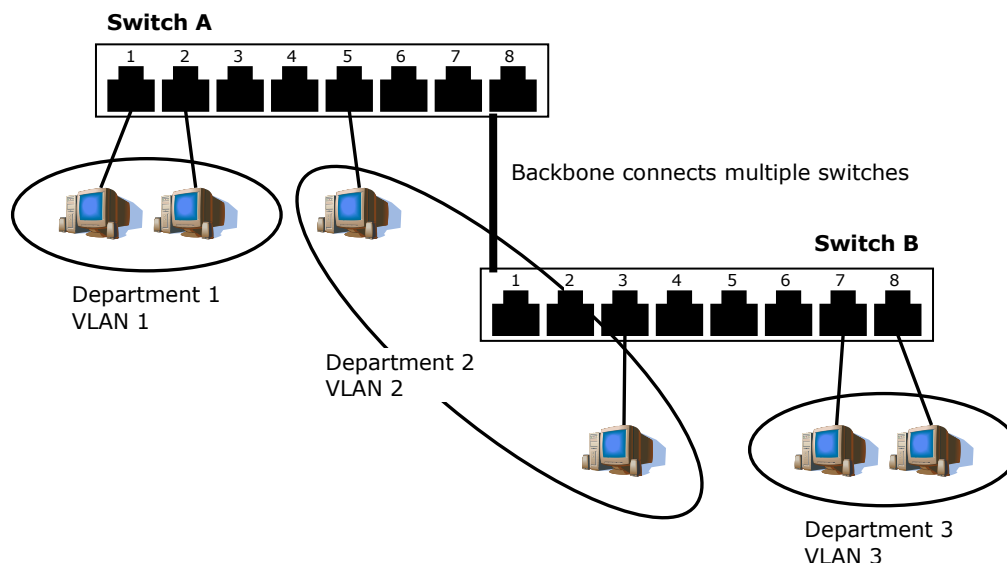
Setting up Virtual LANs (VLANs) on your Moxa Ethernet extender switch increases the efficiency of your network by dividing the LAN into logical segments, as opposed to physical segments. In general, VLANs are easier to manage.

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

VLANs and the Rackmount switch

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

- On a single VLAN defined in the Moxa Ethernet extender 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 Ethernet extender switch before the extender switch can use it to forward traffic:

Managing a VLAN

A new or initialized Moxa Ethernet extender 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 Ethernet extender switch over the network.

Communication Between VLANs

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

VLANs: Tagged and Untagged Membership

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

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

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

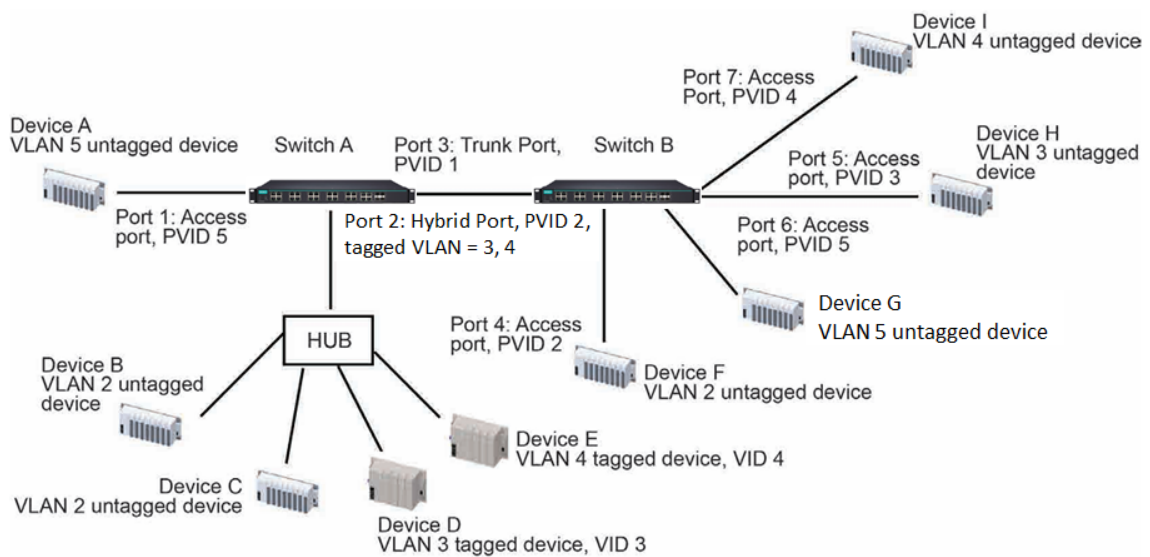
To carry multiple VLANs across a single physical link (backbone, trunk), each packet must be tagged with a VLAN identifier so that the switches can identify which packets belong in which VLAN. To communicate between VLANs, a router must be used.

The Moxa Ethernet extender 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 Ethernet extender switch will insert this PVID into this packet so the next 802.1Q VLAN switch can recognize it.
- **Trunk Port:** The port connects to a LAN that consists of untagged devices, tagged devices, and/or switches and hubs. In general, the traffic of the Trunk Port must have a Tag. Users can also assign a PVID to a Trunk Port. The untagged packet on the Trunk Port will be assigned the default port PVID as its VID.
- **Hybrid Port:** The port is similar to a Trunk port, except users can explicitly assign tags to be removed from egress packets.

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

Sample Applications of VLANs Using Moxa Ethernet extender switches



In this application:

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

After the application is properly configured:

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

Configuring a Virtual LAN

To configure 802.1Q VLAN and port-based VLANs on the Moxa Ethernet extender switch, use the **VLAN Settings** page to configure the ports for either an **802.1Q VLAN** or **Port-based VLAN** mode.

VLAN Mode

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

VLAN Settings: 802.1Q VLAN

VLAN Settings

VLAN Mode 802.1Q VLAN ▼

Quick Setting Panel ▼

Port	Type	PVID	Tagged VLAN	Untagged VLAN	Forbidden VLAN
D1,D2	Trunk ▼	2	3		

Add

Note: Use port description such as "6", "G6", "1-6"

Note: 5,6,G1:G3 means the configuration will be copied to port 5,6,G1,G2,G3

VLAN ID Configuration Table

Enable GVRP

Management VLAN ID

Port	Type	PVID	Tagged VLAN	Untagged VLAN	Forbidden VLAN
1	Access ▼	1			
2	Access ▼	1			
3	Access ▼	1			
4	Access ▼	1			
5	Access ▼	1			
6	Access ▼	1			
D1	Access ▼	1			
D2	Access ▼	1			

Apply

When VLAN Mode is set to 802.1Q VLAN, the configuration options will be divided into the **Quick Setting Panel** and **VLAN ID Configuration Table**. The Quick Setting Panel is generally used to configure VLAN settings for groups of ports, with the settings pushed down to the VLAN ID Configuration Panel when the user clicks the Add button. The VLAN ID Configuration Table can be used to configure the settings for individual ports.

Quick Setting Panel

The Moxa Ethernet extender switch provides a **Quick Setting Panel** that administrators can use to quickly configure VLAN settings for single ports or groups of ports. To configure a group of ports, type the port names in the **Port** column, separated commas (,) for individual port names, or colons (:) to indicate a range of ports. For example, typing "G1,G3" applies the settings to ports G1 and G3, whereas typing "G1:G3" applies the settings to ports G1, G2, and G3. Next, if necessary configure **Type**, **PVID**, **Tagged VLAN**, **Untagged VLAN**, and **Forbidden VLAN**, and then click the **Add** button to move the settings down to the table at the bottom of the window.

VLAN ID Configuration Table

Enable GVRP

Setting	Description	Factory Default
Checked/Unchecked	Check the checkbox to enable the GVRP function. Remove the checkmark to disable the GVRP function.	Checked

Management VLAN ID

Setting	Description	Factory Default
1 to 4094	Assigns the VLAN ID to this Moxa Ethernet extender switch.	1

Note: Some of the following settings can be modified in the Quick Setting Panel.

Port

Setting	Description	Factory Default
Port name	Read only	N/A

Type

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



ATTENTION

For communication redundancy in the VLAN environment, set **Redundant Port, Coupling Ports** and **Coupling Control Ports** to **Trunk Port**, since these ports act as the **backbone** for transmitting packets from different VLANs to different Moxa Ethernet extender switch units.

PVID

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

Tagged VLAN

Setting	Description	Factory Default
1 to 4094	This field will 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 VLANs.	None

Untagged VLAN

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

Forbidden VLAN

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

NOTE The **Quick Setting Panel** provides a quick way of configuring multiple VLAN ports with the same setting.

VLAN Settings: Port-based VLAN

When **VLAN Mode** is set to **Port-based VLAN**, the VLAN Settings window will appear as shown below. Check the appropriate checkbox under a port to assign the port to a VLAN. The maximum VLAN ID equals the number of Moxa Ethernet extender switch ports. In the following example, all of the ports are assigned to VLAN 1.

VLAN Settings

VLAN Mode Port-based VLAN

VLAN	Port								
	1	2	3	4	5	6	D1	D2	
1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
7	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
8	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Apply

NOTE When Port-based VLAN is configured, IGMP will be disabled.

VLAN Table

VLAN Table

VLAN Mode 802.1Q VLAN

Management VLAN 1

Index	VID	Joined Access Port	Joined Trunk Port	Joined Hybrid Port
1	1	1, 4, 5, 6, 7, G1, G2, G3,	2,	3,

VLAN Table

VLAN Mode Port-based VLAN

Index	VLAN	Joined Port
1	1	1, 4, 5, 6, 7, G1, G2, G3,
2	2	2,
3	3	3,


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 groups** and **Joined Ports**.

Port

There are two port setting pages **Port Settings** and **xDSL Port Settings** included in Moxa's Ethernet extender switch's console utility. The web browser interface is for users to control Ethernet ports and xDSL ports respectively. The two port status pages **Port Status** and **xDSL Port Status** display the status/settings of each port on the Moxa Ethernet extender switch.

Port Settings

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

 **Port Settings**

Port	Enable	Media Type	Description	Speed	Flow Ctrl	MDI/MDIX
1	<input checked="" type="checkbox"/>	100TX,RJ45.		Auto ▾	Disable ▾	Auto ▾
2	<input checked="" type="checkbox"/>	100TX,RJ45.		Auto ▾	Disable ▾	Auto ▾
3	<input checked="" type="checkbox"/>	100TX,RJ45.		Auto ▾	Disable ▾	Auto ▾
4	<input checked="" type="checkbox"/>	100TX,RJ45.		Auto ▾	Disable ▾	Auto ▾
5	<input checked="" type="checkbox"/>	100TX,RJ45.		Auto ▾	Disable ▾	Auto ▾
6	<input checked="" type="checkbox"/>	100TX,RJ45.		Auto ▾	Disable ▾	Auto ▾

Enable

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

Media Type

Setting	Description	Factory Default
Media type	Displays the media type for each Ethernet port	N/A

Description

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

Speed

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

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 Ethernet extender switch and connected devices.

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

MDI/MDIX

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

Port Status

The following table shows the status of each Ethernet/DSL port, including the media type, link status, flow control, and port state.

Port Status					
Port	Media Type	Link Status	MDI/MDIX Status	Flow Control	Port State
1	100TX,RJ45.	Link Down	--	--	--
2	100TX,RJ45.	Link Down	--	--	--
3	100TX,RJ45.	Link Down	--	--	--
4	100TX,RJ45.	Link Down	--	--	--
5	100TX,RJ45.	Link Down	--	--	--
6	100TX,RJ45.	100M Full	MDI	Off	Forwarding
D1	VDSL2.	Link Down	--	--	--
D2	VDSL2.	Link Down	--	--	--

NOTE MDI/MDIX is not applied to xDSL (D1/D2) ports

xDSL Port Settings

xDSL port settings are included to give the user control over DSL ports' access, port role, port transmission rate, INP, and initiating the re-training.

xDSL Port Settings

Port Settings

Port	Enable	Media Type (Standard)	Description	CO/CPE Mode		Rate Control	Auto/Force Speed (DS/U/S)	INP	Retrain
				Set	Act				
D1	<input checked="" type="checkbox"/>	VDSL2.		Auto	CPE	Symmetric	Auto	Disable	<input type="checkbox"/>
D2	<input checked="" type="checkbox"/>	VDSL2.		Auto	CPE	Symmetric	Auto	Disable	<input type="checkbox"/>

Apply

Smart Speed Detection Settings

Port	Enable
D1	<input type="checkbox"/>
D2	<input type="checkbox"/>

Apply

Port Settings

Port

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

Enable

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

Media Type

Setting	Description	Factory Default
Media type	Displays the media type (standard) for each DSL port	N/A

Description

Setting	Description	Factory Default
Max. 63 characters	Specifies an alias for the DSL port to help administrators differentiate between different DSL ports. Example: Intersection #123-1	None

CO/CPE Mode (Set)

Setting	Description	Factory Default
Auto	DSL port with this setting will perform CO/CPE automatic negotiation with its link partner DSL port to decide the role of CO or CPE.	Auto
CO	DSL port with this setting will perform CO role.	
CPE	DSL port with this setting will perform CPE role.	

CO/CPE Mode (Act)

Setting	Description	Factory Default
CO	Shows the current activated role on the DSL port is CO.	By factory default, DSL D1 is activated at CO role and the DSL D2 is activated at CPE role with CO/CPE automatic negotiation enabled.
CPE	Shows the current activated role on the DSL port is CPE.	

NOTE CO/CPE automatic negotiation

The VDSL2 connection between 2 units must operate in pairs. One port functions as the CO with the other port on the other device as the CPE.

To make configuration easier, the IEX-408E-2VDSL2 supports auto CO/CPE negotiation as the default setting on both DSL ports (DSL D1 and DSL D2). When 2 DSL ports from Moxa's IEX-408E-2VDSL2 or IEX-402-VDSL2 are connected, auto CO/CPE negotiation will automatically assign one port on one device as the CO and the other port on the other side as the CPE.

Also, by factory default, the 2 DSL ports on one IEX-408E-2VDSL2 are set for one to be CO (DSL D1) and the other to be CPE (DSL D2) with auto CO/CPE negotiation enabled.

NOTE To speed up establishing a DSL connection, we suggest you connect the DSL D1 port on one IEX-408E-2VDSL2 to the DSL D2 port on the other IEX-408E-2VDSL2 when installing.

NOTE The CO/CPE roles on DSL ports can be set/changed through web browser or Telnet/serial console interfaces.

Rate Control

Setting	Description	Factory Default
Symmetric	Set the Downstream rate similar to Upstream rate.	Symmetric
Asymmetric	Set the Downstream rate higher than Upstream rate.	

NOTE In Moxa's Ethernet extender switch, data flows from CO side to CPE side and is designated as the Downstream (DS) while Upstream (US) is defined as data flow from CPE to CO.

Auto/Force Speed (DS/US)

Setting	Description	Factory Default
Transmission rate	<p>Auto: Allows the DSL ports to negotiate the best transmission rate based on line conditions.</p> <p>Fixed Speed: Manually assigning one of the below fixed rate options.</p> <ul style="list-style-type: none"> • Asymmetric speed (DS/US): 100M/100M, 100M/70M, 80M/50M, 60M/30M, 55/15M, 50M/8M, 40M/5M, 30M/2.5M, 20M/1.5M, 10M/1M, 8M/1M, 5M/768K, 3M/512K, 1M/256K • Symmetric speed (DS/US): 100M/100M, 75M/75M, 60M/60M, 40M/40M, 30M/30M, 25M/25M, 20M/20M, 15M/15M, 10M/10M, 5M/5M, 4M/4M, 3M/3M, 2M/2M, 1M/1M 	Auto

NOTE Once a DSL port has been assigned manually or selected after automatic CO/CPE negotiation to act as CPE role, the settings of the Rate Control, Auto/Force Speed (DS/US), INP on this DSL port are no longer valid. The corresponding settings of this DSL port will follow its link partner DSL port that is acting as CO.

INP

According to the ITU-993.2 standard, INP (impulse noise protection) is an error correction algorithm. If noise lasts for consecutive DMT symbols or fractions, the errors can be completely corrected by the error correcting code.

The Moxa Ethernet VDSL2 extender switch supports two modes: STD (standard) and INP (impulse noise protection). By default, the standard mode is enabled. One can activate/deactivate the INP mode through web browser or Telnet/serial console interfaces.

Setting	Description	Factory Default
Enabled	Enable INP mode on the specific DSL port.	Disabled
Disabled		(When disabled, the port acts in standard mode)

NOTE When INP mode is enabled, the latency when the packet is transmitted through the DSL port will be longer than in standard mode. The latency of the DSL port can be observed from the **xDSL Port Status** page through web browser or Telnet/serial console interfaces.

Retrain

Setting	Description	Factory Default
Checked	To initiate the re-training (including role negotiation, transmission rate negotiate etc.) on the DSL port.	Unchecked
Unchecked		

NOTE After checkmark **Retrain** on certain DSL port, please click **Apply** to activate the re-training.

NOTE Due to the characteristics of DSL technology, it takes a few minutes to complete the training process for establishing the DSL link. Therefore, when the re-training is triggered, you need to wait for a few minutes for the establishment of the connection.

Smart Speed Detection Settings

The Moxa Ethernet extender switch supports an automatic condition detection mechanism to decide whether to initiate re-training on the certain DSL link that is in a better condition to reach a higher transmission rate.

Setting	Description	Factory Default
Checked	Activate the automatic detection; re-training (including role negotiation, transmission rate negotiation etc.) will be initiated automatically on the certain DSL link once a better environment condition is detected. *Better condition is a comparison between the condition when DSL link established and the current condition.	Unchecked
Unchecked		

NOTE **Smart Speed Detection** can only be activated when the DSL port is set under **Auto Speed** mode; If the environment condition varies frequently (e.g. at train wayside), we recommend to use **Force Speed** to prevent frequent re-train.

xDSL Port Status

The following summary table shows the status of each DSL port, including DSL link status, established connection duration, signal-to-noise (SNR) ratio, acting role, acting rate control mode, DS/US transmission rate setting and the current bandwidth usage, INP state, delay (latency) on DS/US, and the smart speed status.

xDSL Port Status

Bypass Mode Status Disable

Port Status

Port	Link Status	Connection Time	SNR (dB)		Acting Mode (CO/CPE)	Rate Control Mode	Data Rate (kbps)		INP	Actual Delay (ms)		Smart Speed Status
			DS	US			DS (Usage/Max.)	US (Usage/Max.)		DS	US	
D1	Link Down	0d/0h/0m/0s	--	--	CPE	Symmetric	--	--	Disable	--	--	--
D2	Link Down	0d/0h/0m/0s	--	--	CO	Symmetric	--	--	Disable	--	--	--

[Refresh](#)

Link Aggregation

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 Ethernet extender switch's port trunking feature allows devices to communicate by aggregating up to 4 trunk groups, with a maximum of 6 Ethernet or 2 xDSL ports for each group. If one of the ports fails within a specific trunk group, the rest of the ports will automatically provide backup and share the traffic.

Ethernet port trunking on a Moxa Ethernet extender switch can be used to combine up to 6 ports between two Moxa Ethernet extender switches. If all Ethernet ports on both switches are configured as 100BaseTX and they are operating in full duplex, the potential bandwidth of the connection will be 1200 Mbps.

xDSL port trunking on a Moxa Ethernet extender switch can be used to combine up to 2 xDSL ports between two Moxa Ethernet extender switches. If all xDSL ports on both extender switches are configured as symmetric mode and with speed forced at 5Mbps/5Mbps, the potential bandwidth of the connection will be 20 Mbps.

NOTE The xDSL port can only be established in a trunk group with a xDSL port. And the xDSL ports set in same trunk group should have the exact same xDSL port settings (i.e. same CO/CPE mode, Rate Control mode and Forced Speed)

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.

NOTE 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.

NOTE Each Moxa Ethernet extender 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

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

The screenshot shows the 'Port Trunking' configuration interface. At the top, there are two dropdown menus: 'Group' set to 'Trk1' and 'Type' set to 'Static'. Below these is a table with columns: 'Select', 'Port', 'Media Type', 'Description', and 'Link Status'. The table lists ports 1 through 6 (all 100TX, RJ45) and ports D1 and D2 (both VDSL2). Port 6 is the only one with a 'Link Status' of '100M Full', while all others are 'Link down'. Each row has a checkbox in the 'Select' column. To the right of the table is a vertical scrollbar. Below the table is a green 'Apply' button. At the bottom, there is a summary table with columns: 'Group', 'Type', and 'Member Ports'.

- Step 1:** Select the desired **Trunk Group**
- Step 2:** Select the **Trunk Type** (Static or LACP).
- Step 3:** Select the Trunk Group to modify the desired ports if necessary

NOTE xDSL port can only be established in trunk group with xDSL port. And the xDSL ports to be set in the same trunk group should have exact same xDSL port settings (i.e. same CO/CPE mode, Rate Control mode and Forced Speed)

Trunk Group (maximum of 4 trunk groups)

Setting	Description	Factory Default
Trk1, Trk2, Trk3, Trk4	Specifies the current trunk group.	Trk1

NOTE The table below indicates the Max. Trunk Groups numbers supported within other Moxa switches. The EDS 400A series does not support Port Trunking. The number of Trunk Groups for other Moxa 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 static trunking protocol.	Static
LACP	Selects LACP (IEEE 802.3ad, Link Aggregation Control Protocol).	

Trunking Status

The **Trunking Status table** shows the Trunk Group configuration status.

Trunking Status			
Group	Type	Member Ports	Status
Trk1	Static	1	OK
		2	OK
Trk2	Static	3	OK
		5	OK

Link-Swap Fast Recovery

The Link-Swap Fast Recovery function, which is enabled by default, allows the Moxa Ethernet extender 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 Link-Swap Fast Recovery function, or to re-enable the function after it has already been disabled, access either the Console utility's **Link-Swap recovery** page, or the Web Browser interface's **Link-Swap fast recovery** page, as shown below.

Link-Swap Fast Recovery

Enable

Link-Swap-Fast-Recovery

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

Multicast

This section explains multicasts, multicast filtering, and how multicast filtering can be implemented on your Moxa Ethernet extender switch.

The Concept of Multicast

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).

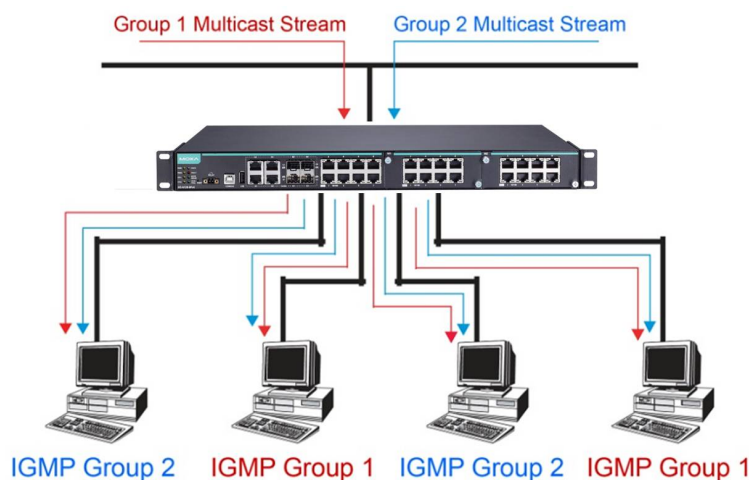
Multicast transmission makes more sense and is more efficient than unicast transmission for some applications. For example, multicasts are often used for video-conferencing, since high volumes of traffic must be sent to several end-stations at the same time, but where broadcasting the traffic to all 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.

The Concept of Multicast Filtering and Management

What is Multicast Filtering?

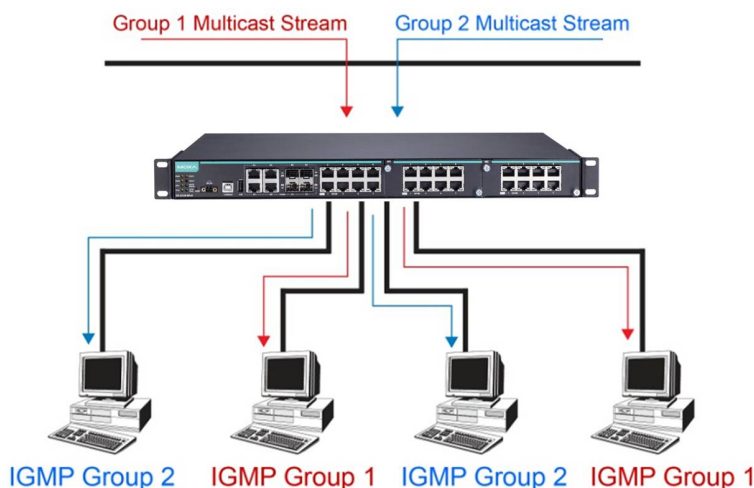
Multicast filtering ensures that only end-stations that have joined certain groups receive multicast traffic and improves the performance of networks that carry multicast traffic. With multicast filtering, network devices only forward multicast traffic to the ports that are connected to registered end-stations. One of the ways to perform multicast filtering in your LAN network in order to higher the network efficiency is by using IGMP snooping to prune multicast traffic so that it travels only to the end destinations that require the traffic, thus reducing the amount of traffic on the Ethernet LAN. The following two figures simply 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 Management Methods on Moxa Ethernet Extender Switches

There are four ways to achieve multicast filtering with an Moxa Ethernet extender switch:

- IGMP (Internet Group Management Protocol) snooping
- GMRP (GARP Multicast Registration Protocol)
- Adding a static multicast MAC address manually to filter multicast traffic automatically
- Multicast filtering for unknown multicast traffic

IGMP and IGMP Snooping

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 such feature. For Moxa Ethernet extender switches, IGMP version 1, 2 and 3 are supported.

IGMP Snooping is a procedure used on Layer 2 switches (e.g. Moxa Ethernet extender switches) in order to translate IP multicast group addresses into MAC multicast addresses and allow the switch to forward multicast packets only to certain appropriate ports so that multicast traffic filtering and management can be achieved. A Moxa Ethernet extender switch with IGMP Snooping enabled 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.

The following indicates how the network works when using IGMP version 1 or 2 and with IGMP snooping enabled on switches:

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

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

IGMP version comparison

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

NOTE IGMP version 2 is compatible with version 1.

NOTE Use the USB/Telnet console or web browser 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.

GMRP (GARP Multicast Registration Protocol)

Moxa Ethernet extender 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 Address

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

Multicast Filtering for Unknown Multicast Traffic

Moxa Ethernet extender switch supports enabling filtering unknown multicast packets manually on certain ports to further manage the network traffic.

IGMP Snooping

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.

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

IGMP Snooping Setting

Enable IGMP Snooping (Global)

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

Query Interval (sec)

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 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
Disable	Disables the Moxa Ethernet extender switch's querier function.	V1/V2
V1/V2 and V3 checkbox	V1/V2: Enables the Moxa Ethernet extender switch to send IGMP snooping version 1 and 2 queries V3: Enables the Moxa Ethernet extender switch to send IGMP snooping version 3 queries	

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 and layer 2 Ethernet extender switches.

If all switches on the network are Moxa layer 2 switches or layer 2 Ethernet extender switches, then only one layer 2 device will act as Querier.

IGMP Group Status

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

IGMP Group Status

VID:

Dynamic Router Port	Static Router Port	Querier Connected Port	Role		
Index	Group	Port	Version	Filter Mode	Sources

[Refresh](#)

The information shown in the table includes:

- Dynamic Router Port: Indicates that a multicast router connects to or sends packets from these port(s).
- Static Router Port: Displays the static multicast querier port(s).
- Querier Connected Port: Displays the port that is connected to the querier.
- Role: Indicates if the switch is a querier. Displays Querier or Non-Querier.
- Group: Displays the multicast group addresses.
- Port: Displays the port that receives the multicast stream or the port the multicast stream is forwarded to
- Version: Displays the IGMP Snooping version.
- Filter Mode: Indicates that the multicast source address is included or excluded. Displays Include or Exclude when IGMP v3 is enabled
- Sources: Displays the multicast source address when IGMP v3 is enabled

Static Multicast Address

NOTE The MAC address (01:00:5E:XX:XX:XX) will appear on the Static Multicast Address page. Activate IGMP Snooping to implement automatic classification.

MAC Address

Setting	Description	Factory Default
Integer	Type the MAC address in the MAC Address field to specify a static multicast address.	None

Member Port

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

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.

Enable GMRP

Setting	Description	Factory Default
Select/Deselect	Checkmark the check boxes to enable GMRP for the port listed in the Port column.	None

GMRP Status

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

MAC Address: The Multicast MAC address

Static Port: This multicast address is defined by static multicast

Learned Port: This multicast address is learned by GMRP

QoS

The Moxa Ethernet extender 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 Ethernet extender 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 Ethernet extender switch's QoS capability improves the performance and determinism of industrial networks for mission critical applications.

The Traffic Prioritization Concept

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

- Improve network performance by controlling a wide variety of traffic and by managing congestion.
- Assign priorities to different categories of traffic. For example, set higher priorities for time-critical or 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 Ethernet extender 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 Ethernet extender 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 for LAN environments, it still has some restrictions:

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

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 Ethernet extender 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 Ethernet extender 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 Ethernet extender 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 Ethernet extender switches has multiple traffic queues that allow packet prioritization to occur. Higher priority traffic can pass through the Moxa Ethernet extender switch without being delayed by lower priority traffic. As each packet arrives in the Moxa Ethernet extender 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 Ethernet extender 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 Ethernet extender 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 Ethernet extender switch’s QoS capability improves your industrial network’s performance and determinism for mission critical applications.

CoS Classification

QoS Classification

Scheduling Mechanism: Weight Fair(8:4:2:1) ▼

Port	ToS Inspection	CoS Overwriting	Priority
1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	3 ▼
2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	3 ▼
3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	3 ▼
4	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	3 ▼
5	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	3 ▼
6	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	3 ▼
D1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	3 ▼
D2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	3 ▼

Apply

Scheduling Mechanism

Setting	Description	Factory Default
Weight Fair	The Moxa Ethernet extender 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 frames egress. This approach can cause the lower priorities to be starved of opportunity for transmitting frames but ensures that all high priority frames will egress the switch as soon as possible.	

TOS Inspection

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

COS Overwriting

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


Priority

Setting	Description	Factory Default
0 to 7	The port priority has 8 priority queues: from 0 (lowest) to 7 (highest)	3

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

1. ToS Inspection
2. CoS Overwriting
3. Priority

CoS Mapping

 **CoS Mapping**

CoS	Priority Queue
0	0 ▼
1	0 ▼
2	1 ▼
3	1 ▼
4	2 ▼
5	2 ▼
6	3 ▼
7	3 ▼

Apply

CoS Value and Priority Queues

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

DSCP Mapping

DSCP Mapping

DSCP	Priority	DSCP	Priority	DSCP	Priority	DSCP	Priority
0	0 ▼	1	0 ▼	2	0 ▼	3	0 ▼
4	0 ▼	5	0 ▼	6	0 ▼	7	0 ▼
8	1 ▼	9	1 ▼	10	1 ▼	11	1 ▼
12	1 ▼	13	1 ▼	14	1 ▼	15	1 ▼
16	2 ▼	17	2 ▼	18	2 ▼	19	2 ▼
20	2 ▼	21	2 ▼	22	2 ▼	23	2 ▼
24	3 ▼	25	3 ▼	26	3 ▼	27	3 ▼
28	3 ▼	29	3 ▼	30	3 ▼	31	3 ▼
32	4 ▼	33	4 ▼	34	4 ▼	35	4 ▼
36	4 ▼	37	4 ▼	38	4 ▼	39	4 ▼

Apply

DSCP Value and Priority Queues

Setting	Description	Factory Default
0 to 7	Maps different TOS values to 7 different egress queues.	0 to 7: 0 8 to 15: 1 16 to 23: 2 24 to 31: 3 32 to 39: 4 40 to 47: 5 48 to 55: 6 56 to 63: 7

Rate Limiting

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 extender 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.

Traffic Rate Limiting Settings

Action setting on the **Rate Limiting** page can be set to **Drop Packet** or **Disable Port**.

Action

Setting	Description	Factory Default
Drop Packet	Set the max. ingress/egress rate limit for ingress/egress packets	Drop Packet
Disable Port	When the ingress 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.	

Rate Limiting: Drop Packet

Rate Limiting

Action Drop Packet ▼

Port	Ingress Rate	Egress Rate
1	Unlimited ▼	Unlimited ▼
2	Unlimited ▼	Unlimited ▼
3	Unlimited ▼	Unlimited ▼
4	Unlimited ▼	Unlimited ▼
5	Unlimited ▼	Unlimited ▼
6	Unlimited ▼	Unlimited ▼
D1	Unlimited ▼	Unlimited ▼
D2	Unlimited ▼	Unlimited ▼

Apply

Setting	Description	Factory Default
Ingress rate (% of max. throughput)	Select the ingress rate limit (% of max. throughput) for all packets from the following options: 3%, 5%, 10%, 15%, 25%, 35%, 50%, 65%, 85%, Unlimited	Unlimited
Egress rate (% of max. throughput)	Select the egress rate limit (% of max. throughput) for all packets from the following options: 3%, 5%, 10%, 15%, 25%, 35%, 50%, 65%, 85%, Unlimited	Unlimited

Rate Limiting: Disable Port

Rate Limiting

Action: Disable Port ▾

Disabled Duration (sec): 30

Port	Ingress Threshold
1	Unlimited ▾
2	Unlimited ▾
3	Unlimited ▾
4	Unlimited ▾
5	Unlimited ▾
6	Unlimited ▾
D1	Unlimited ▾
D2	Unlimited ▾

Apply

Setting	Description	Factory Default
Duration (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: 4464, 7441, 14881, 22322, 37203, 52084, 74405, Unlimited	Unlimited

Security

Security can be categorized into two levels: the user name/password level, and the port access level. Moxa Ethernet extender switches provide many kinds of security functions, including Login Authentication, Management Interface, Trusted Access, Authentication Certificate, IEEE 802.1X, Port Security, Broadcast Storm Protection, and Loop Protection.

Login Authentication

Moxa Ethernet extender switches provide five different user login options: Local, TACACS+ (Terminal Access Controller Access-Control System Plus), RADIUS (Remote Authentication Dial In User Service), TACACS+ with Local, and RADIUS with Local. The TACACS+ and RADIUS mechanisms are centralized authentication systems for connecting to network services. The fundamental purpose of both TACACS+ and RADIUS is to provide an efficient and secure mechanism for user account management.

NOTE TACACS+ with Local and RADIUS with Local are mechanisms that enable automatic failover from TACACS+ server or RADIUS server to local login credentials when the TACACS+ server or RADIUS server are unreachable.

Login Authentication

Authentication Protocol: TACACS+, Local

Server IP/Name:

TCP Port: 49

Shared Key:

Authentication Type: ASCII

Timeout (sec): 30

Apply

Login Authentication

Authentication Protocol: RADIUS, Local

Server IP/Name:

UDP Port: 1812

Shared Key:

Authentication Type: Radius CHAP

Timeout (sec): 5

Apply

Setting	Description	Factory Default
Authentication Protocol	Authentication mechanism selection (Local; TACACS+; RADIUS; TACACS+, Local; and RADIUS, Local)	Local
Server IP/Name	Sets the IP address of an external TACACS+/RADIUS server as the authentication database.	None
TCP/UDP Port	Sets the communication port of an external TACACS+/RADIUS server as the authentication database.	TACACS+: 49 RADIUS: 1812
Shared Key	Sets specific characters for server authentication verification.	None
Authentication Type	Authentication mechanism selection. ASCII, PAP, CHAP, MSCHAP are for TACACS+, and CHAP is for RADIUS.	ASCII for TACACS+ CHAP for RADIUS
Timeout (sec)	The timeout period for waiting for a server response.	TACACS+: 30 RADIUS: 5

Management Interface

Management Interface

Enable HTTP Port: 80

Enable SSL Port: 443

Enable Telnet Port: 23

Enable SSH Port: 22

Enable SNMP Port: 161

Enable Moxa Service Port: 4000

Auto Logout Setting (min): 5
(0~1440; 0 for Disable)

Apply

Enable HTTP

Setting	Description	Factory Default
Select/Deselect	Checkmark the appropriate check boxes to enable HTTP and set the corresponding port number.	Port: 80

Enable SSL

Setting	Description	Factory Default
Select/Deselect	Checkmark the appropriate check boxes to enable SSL and set the corresponding port number.	Port: 443

Enable Telnet

Setting	Description	Factory Default
Select/Deselect	Checkmark the appropriate check boxes to enable Telnet and set the corresponding port number.	Port: 23

Enable SSH

Setting	Description	Factory Default
Select/Deselect	Checkmark the appropriate check boxes to enable SSH and set the corresponding port number.	Port: 5

Enable SNMP

Setting	Description	Factory Default
Select/Deselect	Checkmark the appropriate check boxes to enable SNMP.	Select

Enable Moxa Service

Setting	Description	Factory Default
Select/Deselect	Checkmark the appropriate check boxes to enable Moxa Service.	Select

Web Auto Logout (min)

Setting	Description	Factory Default
Integer	Sets the web auto logout period	5

Trusted Access

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

NOTE Please add your local IP address first, otherwise, your PC will not be able to connect the device.

Trusted Access

Enable trusted access Apply

Please add your local IP address first, otherwise, your PC will not be able to connect the device again

<input type="checkbox"/> All	IP Address	Subnet Mask
<input type="checkbox"/>	<input type="text"/>	32(255.255.255.255) ▾
<input type="checkbox"/>	<input type="text"/>	32(255.255.255.255) ▾
<input type="checkbox"/>	<input type="text"/>	32(255.255.255.255) ▾
<input type="checkbox"/>	<input type="text"/>	32(255.255.255.255) ▾
<input type="checkbox"/>	<input type="text"/>	32(255.255.255.255) ▾
<input type="checkbox"/>	<input type="text"/>	32(255.255.255.255) ▾
<input type="checkbox"/>	<input type="text"/>	32(255.255.255.255) ▾
<input type="checkbox"/>	<input type="text"/>	32(255.255.255.255) ▾
<input type="checkbox"/>	<input type="text"/>	32(255.255.255.255) ▾
<input type="checkbox"/>	<input type="text"/>	32(255.255.255.255) ▾
<input type="checkbox"/>	<input type="text"/>	32(255.255.255.255) ▾

Delete

You may add or remove IP addresses to limit access to the Moxa Ethernet extender switch. When the accessible IP list is enabled, only addresses on the list will be allowed access to the Moxa Ethernet extender 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, by removing the checkmark from **Enable trusted access (default setting is disabled.)**

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

Authentication Certificate

Authentication Certificate

SSL Certificate

Re-generate

SSH Key

Re-generate

Note: Few minutes may be required. Web will be unavailable temporarily until it finish.

Apply

SSL Certificate Re-generate

Setting	Description	Factory Default
Select/Deselect	Enable the SSL Certificate Re-generate	Deselect

SSH Key Re-generate

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

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 Ethernet extender 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 Ethernet extender switch by using a Local User Database as the authentication look-up table. When we use an external RADIUS server as the authentication server, the authenticator and the authentication server exchange EAP frames.

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

IEEE 802.1X Setting

802.1X Settings

Authentication Option RADIUS ▼

Re-Auth Enable ▼

Re-Auth Period (sec) 3600

Port	Enable 802.1X	Re-Auth
1	<input type="checkbox"/>	<input type="checkbox"/>
2	<input type="checkbox"/>	<input type="checkbox"/>
3	<input type="checkbox"/>	<input type="checkbox"/>
4	<input type="checkbox"/>	<input type="checkbox"/>
5	<input type="checkbox"/>	<input type="checkbox"/>
6	<input type="checkbox"/>	<input type="checkbox"/>
D1	<input type="checkbox"/>	<input type="checkbox"/>

Apply

Authentication Option

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

Re-Auth (Global)

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.	Enable

Re-Auth Period (sec)

Setting	Description	Factory Default
60 to 65535	Sets the Re-Auth period	3600

Enable 802.1X

Setting	Description	Factory Default
Select/Deselect	Check 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.	Deselect

Re-Auth

Setting	Description	Factory Default
Select/Deselect	Select enable to require re-authentication of the client by port	Deselect

Local Database

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

Local Database

User Name

Password

Confirm Password

Description

[Add](#)

All	User Name	Password	Description
[icon]			

[Delete](#)

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
Confirm Password (Max. of 16 characters)	Confirm 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.

RADIUS Server Settings

RADIUS Server Settings

Apply Login Authentication Settings

1st Server IP/Name

UDP Port

Shared Key

2nd Server IP/Name

UDP Port

Shared Key

Apply Login Authentication Setting

Setting	Description	Factory Default
Select/Deselect	Enables using the same setting as Auth Server.	Deselect

Server Setting

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

Port Security

The Moxa Ethernet extender switch supports adding unicast groups manually if required. By adding the static unicast MAC address into a dedicated port, only that MAC address is allowed to access the LAN network through that port.

Port Security

Port

MAC Address - - - - -

■	All	Port	MAC Address

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

Port Access Control Table

Port Access Control Table

Port ▼

Total Entries:0

All	MAC Address	Status

[Delete](#)

NOTE The port status will show authorized or unauthorized.

Broadcast Storm Protection

Broadcast Storm Protection

Broadcast Storm Protection

Include Multicast Packet

Include Unknown Unicast Packet

[Apply](#)

Setting	Description	Factory Default
Enable/Disable Broadcast Storm Protection	Enables or disables Broadcast Storm Protection for unknown broadcast packets globally.	Enable

Loop Protection

Loop Protection

Enable

[Apply](#)

Enable Loop Protection

Setting	Description	Factory Default
Enable	Enable the loop protection function	Disable
Disable	Disable the loop protection function	

DHCP

IP-Port Binding

IP-Port Binding

Port	Current IP Address	Designated IP Address
1	NA	<input style="width: 90%;" type="text"/>
2	NA	<input style="width: 90%;" type="text"/>
3	NA	<input style="width: 90%;" type="text"/>
4	NA	<input style="width: 90%;" type="text"/>
5	NA	<input style="width: 90%;" type="text"/>
6	NA	<input style="width: 90%;" type="text"/>
D1	NA	<input style="width: 90%;" type="text"/>
D2	NA	<input style="width: 90%;" type="text"/>

Designated IP Address

Setting	Description	Factory Default
IP Address	Set the desired IP for the connected device.	None

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.

DHCP Relay Agent

1st Server

2nd Server

3rd Server

4th Server

Enable Option 82

Assign Remote-ID by IP 192.168.127.253

Remote-ID C0A87FFD

Port	Circuit-ID	Option 82
1	01000101	<input type="checkbox"/> Enable
2	01000102	<input type="checkbox"/> Enable
3	01000103	<input type="checkbox"/> Enable
4	01000104	<input type="checkbox"/> Enable
5	01000105	<input type="checkbox"/> Enable
6	01000106	<input type="checkbox"/> Enable

Apply

Server IP Address

1st Server

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

2nd Server

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

3rd Server

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

4th Server

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

DHCP Option 82

Enable Option 82

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

Assign Remote-ID by

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

Remote-ID

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

SNMP

The Moxa Ethernet extender 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.

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

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

SNMP

SNMP Versions V1, V2c, V3 ▾

Admin Auth. Type No-Auth ▾

Enable Admin Data Encryption Data Encryption Key

User Auth. Type No-Auth ▾

Enable User Data Encryption Data Encryption Key

Community

V1,V2c Read Community

V1,V2c Write/Read Community

Trap/inform Recipient

Trap Mode Trap V1 ▾

Host IP Address 1

1st Trap Community

Host IP Address 2

2nd Trap Community

Apply

SNMP Read/Write Settings

SNMP Versions

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

V1, V2c Read Community

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

V1, V2c Write/Read Community

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

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

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

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

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

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

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

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

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

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

Trap Settings

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

Trap/inform Recipient

Trap Mode

Host IP Address 1

1st Trap Community

Host IP Address 2

2nd Trap Community

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. In a Moxa Ethernet extender switch, Trap V1, V2c and V3 modes are supported (default is Trap V1).

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. In a Moxa Ethernet extender switch, Inform V2c and V3 modes are supported. The maximum timeout time is 300 sec (default is 10 seconds), and the maximum number of retries is 99 times (default is 3 times). When the SNMP agent receives acknowledgement from the NMS, it will stop resending the inform messages.

Host IP Address 1

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

1st Trap Community

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

Host IP Address 2

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

2nd Trap Community

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

Industrial Protocol

The Moxa Ethernet extender switch supports 3 industrial protocols, EtherNet/IP, Modbus TCP, and PROFINET I/O. All three protocols can be enabled or disabled by checking the appropriate checkbox. Modbus TCP is enabled by default, with the other two options disabled.

Industrial Protocol

EtherNet/IP

Enable EtherNet/IP

Note: IGMP snooping will be automatically enabled when EtherNet/IP is activated.

Modbus TCP

Enable Modbus TCP

PROFINET I/O

Enable PROFINET I/O

Apply

- NOTE**
1. IGMP Snooping and IGMP Query functions will be enabled automatically to be properly integrated in Rockwell systems for multicast Implicit (I/O) Messaging for efficient EtherNet/IP communication.
 2. EtherNet/IP can't be enabled while IGMP snooping is disabled due to VLAN setting.

Diagnostics

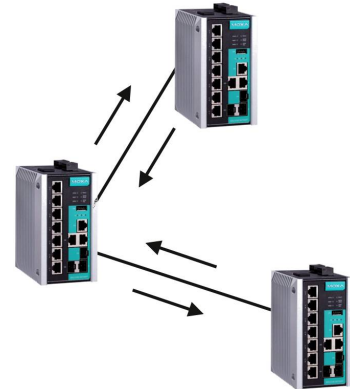
The Moxa Ethernet extender switch provides three important tools for administrators to diagnose network systems: LLDP, Ping, and Port Mirror.

LLDP

Overview

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

LLDP

Enable LLDP

Message Transmit Interval (sec)

[Apply](#)

Port	Neighbor ID	Neighbor Port	Neighbor Port Description	Neighbor System

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.	5 (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.

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 Ethernet extender switch itself. In this way, the user can essentially sit on top of the Moxa Ethernet extender 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.



Port Mirror

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



Port Mirroring Settings

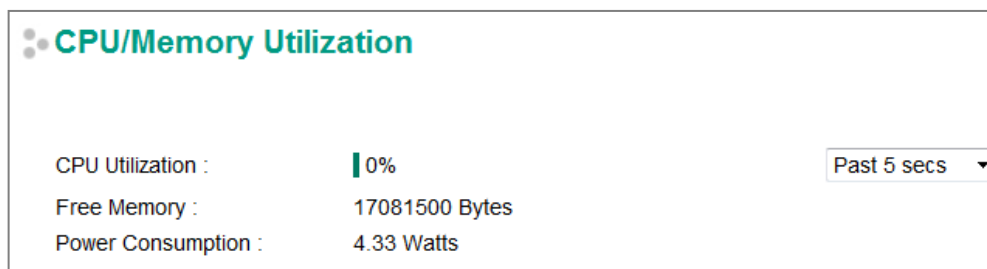
Setting	Description
Monitored Port	Select which ports will be monitored.
Sniffer Mode	Select one of the following three watch direction options: <ul style="list-style-type: none"> RX: Select this option to monitor only those data packets coming into the Moxa Ethernet extender switch's port. TX: Select this option to monitor only those data packets being sent out through the Moxa Ethernet extender switch's port. TX/RX: Select this option to monitor data packets both coming into, and being sent out through, the Moxa Ethernet extender switch's port.
Mirror Port	Select the number of the port that will be used to monitor the activity of the monitored port.

Monitoring

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

CPU/Memory Utilization

The CPU/Memory Utilization page displays the status of system resources. Monitor this information to quickly and easily understand the working status of the extender switch.



CPU Utilization

Setting	Description	Factory Default
Read-only	The CPU usage volume in the past 5 seconds, 30 seconds, and 5 minutes	Past 5 secs

Free Memory

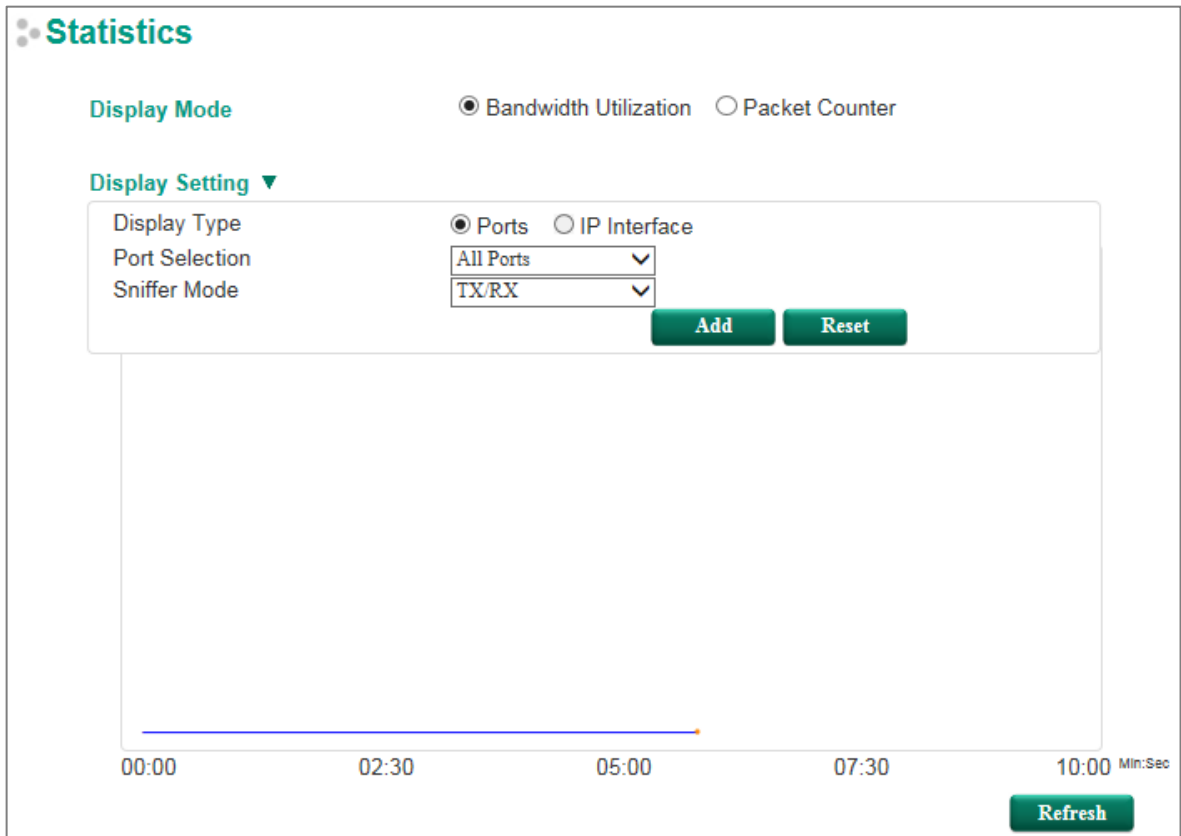
Setting	Description	Factory Default
Read-only	The switch's current free memory	None

Power Consumption

Setting	Description	Factory Default
Read-only	The current system power consumption information. The measurement tolerance is 7% (Unit: watts.)	None

Statistics

Access the Monitor by selecting **Monitoring** 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 Ethernet extender switch's ports. Click one of the two display modes - Bandwidth Utilization or Packet Counter—to view transmission activity of all or specific ports graphically. One can also choose one of four options —Total Packets, TX Packets, RX Packets, or Error Packets—to view transmission activity of specific types of packets on all or specific ports in a summary table. Recall that TX Packets are packets sent out from the Moxa Ethernet extender switch, RX Packets are packets received from connected devices, and Error Packets are packets that did not pass TCP/IP's error checking algorithm.



Port : ▼ Packet: ▼

[Format] Total Packets + Packets in past 5 secs Update Interval: every 5 secs

Tx Total	Tx Unicast	Tx Multicast	Tx Broadcast	Tx Collision			
310828+56	304619+55	6107+1	102+0	0+0			
Rx Total	Rx Unicast	Rx Multicast	Rx Broadcast	Rx Pause			
369324+80	317157+65	5664+0	46503+15	0+0			
Tx		Rx					
Late	Excessive	CRC Error	Discard	Undersize	Fragments	Oversize	Jabber
0+0	0+0	0+0	7306+7	0+0	0+0	0+0	0+0

Event Log

Event Log					
Page 12/12					
Index	Bootup Number	Date	Time	System Startup Time	Event
166	6	2016/03/28	21:37:38	0d10h43m39s	Configuration change activated
167	6	2016/03/28	21:38:02	0d10h44m3s	Port 6 link off
168	6	2016/03/28	21:38:04	0d10h44m5s	Port 6 link on
169	6	2016/03/28	21:38:18	0d10h44m19s	192.168.127.99 admin Auth. ok
170	6	2016/03/28	21:38:21	0d10h44m22s	Port 4 link off
171	6	2016/03/28	21:38:26	0d10h44m27s	Port 4 link on
172	6	2016/03/28	21:38:29	0d10h44m30s	Port 4 link off
173	6	2016/03/28	21:38:44	0d10h44m45s	Topology changed
174	6	2016/03/28	21:38:45	0d10h44m46s	Turbo Ring - Ring Master is changed.
175	6	2016/03/28	21:38:46	0d10h44m47s	Configuration change activated
176	6	2016/03/28	21:38:53	0d10h44m54s	Configuration change activated

The Event Log Table displays the following information:

Index	Event index assigned to identify the event sequence.
Bootup Number	This field shows how many times the Moxa Ethernet extender 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.
Event	Events that have occurred.

NOTE The following events will be recorded into the Moxa Ethernet extender 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

MIB Groups

The Moxa Ethernet extender 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 Ethernet extender switch supports are as follows:

MIB II.1—System Group

sysORTable

MIB II.2—Interfaces Group

ifTable

MIB II.4 – IP Group

ipAddrTable

ipNetToMediaTable

IpGroup

IpBasicStatsGroup

IpStatsGroup

MIB II.5—ICMP Group

IcmpGroup

IcmpInputStatus

IcmpOutputStats

MIB II.6—TCP Group

tcpConnTable

TcpGroup

TcpStats

MIB II.7—UDP Group

udpTable

UdpStats

MIB II.10—Transmission Group

dot3

dot3StatsTable

MIB II.11—SNMP Group

SnmpBasicGroup

SnmpInputStats

SnmpOutputStats

MIB II.17—dot1dBridge Group

dot1dBase

dot1dBasePortTable

dot1dStp

dot1dStpPortTable

dot1dTp

dot1dTpFdbTable

dot1dTpPortTable

```
dot1dTpHCPortTable
dot1dTpPortOverflowTable
pBridgeMIB
dot1dExtBase
dot1dPriority
dot1dGarp
qBridgeMIB
dot1qBase
dot1qTp
dot1qFdbTable
dot1qTpPortTable
dot1qTpGroupTable
dot1qForwardUnregisteredTable
dot1qStatic
dot1qStaticUnicastTable
dot1qStaticMulticastTable
dot1qVlan
dot1qVlanCurrentTable
dot1qVlanStaticTable
dot1qPortVlanTable
```

The Moxa Ethernet extender switch also provides a private MIB file, located in the file **Moxa-[switch's model name]-MIB.my** on the Moxa Ethernet extender switch utility CD-ROM.

Public Traps

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

Private Traps

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