Moxa Embedded Switch Module

EOM-104 Series User's Manual

www.moxa.com/product

Third Edition, October 2009

EOM-104 Series User's Manual

Copyright Notice

Trademarks

Disclaimer

Information in this document is subject to change without notice and does not represent a commitment on the part of Moxa.

Moxa provides this document "as is," without warranty of any kind, either expressed or implied, including, but not limited to, its particular purpose. Moxa reserves the right to make improvements and/or changes to this manual, or to the products and/or the programs described in this manual, at any time.

Information provided in this manual is intended to be accurate and reliable. However, Moxa assumes no responsibility for its use, or for any infringements on the rights of third parties that may result from its use.

This product might include unintentional technical or typographical errors. Changes are periodically made to the information herein to correct such errors, and these changes are incorporated into new editions of the publication.

Technical Support Contact Information
www.moxa.com/support

Moxa Americas:
Toll-free: 1-888-669-2872
Tel: +1-714-528-6777
Fax: +1-714-528-6778

Moxa China (Shanghai office):
Toll-free: 800-820-5036
Tel: +86-21-5258-9955
Fax: +86-10-6872-3958

Moxa Europe:
Tel: +49-89-3 70 03 99-0
Fax: +49-89-3 70 03 99-99

Moxa Asia-Pacific:
Tel: +886-2-8919-1230
Fax: +886-2-8919-1231

Table of Contents

Chapter 1 Introduction 1-1
Moxa's Ethernet-On-Module Switches 1-2
Features 1-2

Chapter 2 Getting Started 2-1
RS-232 Console Configuration (115200, None, 8, 1, VT100) 2-2
Configuration Using a Telnet Console 2-5
Configuration Using a Web Browser 2-8
Disabling Telnet and Browser Access 2-9

Chapter 3 Featured Functions 3-1
Configuring Basic Settings 3-2
System Identification 3-2
Password 3-3
Accessible IP 3-4
Port 3-5
Network 3-7
Time 3-8
Turbo Ring DIP Switch 3-10
System File Update—By Remote TFTP 3-12
System File Update—By Local Import/Export 3-13
Restart 3-14
Factory Default 3-14
Configuring SNMP 3-14
SNMP Read/Write Settings 3-16
Trap Settings 3-18
Private MIB information 3-18
Using Communication Redundancy 3-18
The Turbo Ring Concept 3-19
Configuring "Turbo Ring" and "Turbo Ring V2" 3-22
The STP/RSTP Concept 3-26
Configuring STP/RSTP 3-30
Using Traffic Prioritization 3-33
The Traffic Prioritization Concept 3-34
Configuring Traffic Prioritization 3-36
Using Auto Warning 3-38
Configuring Email Warning 3-38
Email Warning Events Settings 3-38
Email Settings 3-40
Diagnosis 3-41
Ping 3-41
Using the Monitor 3-42
Monitor by Switch 3-42
Monitor by Port 3-43
Using the MAC Address Table 3-43
Using Event Log 3-44
Using Syslog 3-45

Chapter 4 EDS Configurator GUI 4-1
Starting EDS Configurator 4-2
Broadcast Search 4-2
Search by IP address 4-3
Upgrade Firmware 4-4
Modify IP Address 4-5
Export Configuration 4-5
Import Configuration 4-6
Unlock Server 4-8

Appendix A MIB Groups A-1

Appendix B Specifications B-1

1

Introduction

Welcome to the Moxa EOM-104 Series Ethernet-On-Module, the world's first intelligent Embedded Ethernet switch designed specifically for device manufacturers who would like to add a redundant Ethernet solution to an existing product.

The following topics are covered in this chapter:

- **Moxa's Ethernet-On-Module Switches**
- **Features**

Moxa's Ethernet-On-Module Switches

Moxa's Ethernet-On-Module switches come with a suite of useful maintenance and monitoring functions, and is designed to provide smooth and reliable operation in harsh industrial environments. You will find that Moxa's Ethernet-On-Module switches establish a new industrial Ethernet benchmark. The switches excellent for keeping automation systems running continuously, are ideal for sending status reports to help prevent system damages and losses, are a great tool for mastering your industrial Ethernet networks, and are well-suited for use with industrial device control networks.

ATTENTION

Throughout this User's Manual, we use EOM as an abbreviation for Ethernet-On-Module:

EOM = Ethernet-On-Module

Features

Advanced Industrial Networking Capability

- Moxa Turbo Ring with Redundant Self-Healing Ethernet Ring Capability (recovery time < 20 ms at full load)
- Supports QoS—IEEE 802.1p and TOS/DiffServ to increase determinism

Designed for Industrial Applications

- -40 to 75°C operating temperature range
- 3.3 VDC power input

Useful Utility and Remote Configuration

- Configurable by web browser, Telnet/serial console, and a proprietary Windows utility
- Send ping commands to identify network segment integrity

2

Getting Started

This chapter explains how to access your Moxa Ethernet-On-Module switch for the first time. There are three ways to access the switch: serial console, Telnet console, and web browser. The serial console connection method, which requires using a short serial cable to connect the switch to a PC's COM port, can be used if you do not know the switch's IP address. The Telnet console and web browser connection methods can be used to access a Moxa Ethernet-On-Module switch over an Ethernet LAN, or over the Internet.

The following topics are covered:

- **RS-232 Console Configuration (115200, None, 8, 1, VT100)**
- **Configuration Using a Telnet Console**
- **Configuration Using a Web Browser**
- **Disabling Telnet and Browser Access**

RS-232 Console Configuration (115200, None, 8, 1, VT100)

NOTE **Connection Caution!**

1. You **cannot** connect to the EOM using serial console and Telnet simultaneously.
2. You **can** connect to the EOM using a web browser and serial console simultaneously, or using a web browser and Telnet simultaneously.
3. **Recommendation**—when connecting to the EOM using a web browser, do NOT simultaneously connect using either a serial console or by Telnet.

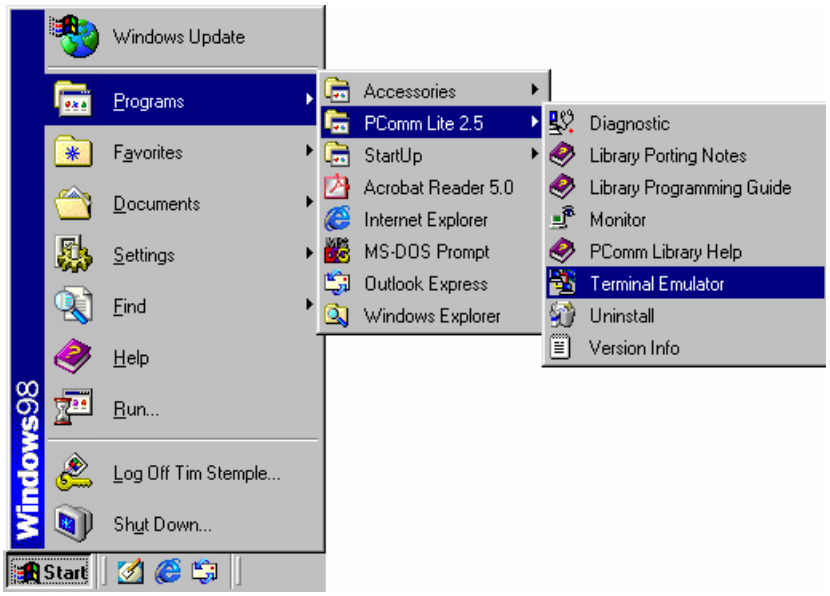
By following this advice, you can maintain better control over how your Moxa Ethernet-On-Module switch is managed.

NOTE We recommend using Moxa PComm Terminal Emulator, which can be downloaded free of charge from Moxa's website.

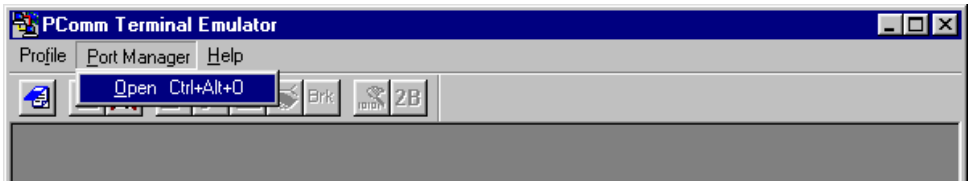
Before running PComm Terminal Emulator, use an RJ45 to DB9-F (or RJ45 to DB25-F) cable to connect the EOM's RS-232 Console port to your PC's COM port (generally COM1 or COM2, depending on how your system is set up).

After installing PComm Terminal Emulator, do the following to access the RS-232 Console utility.

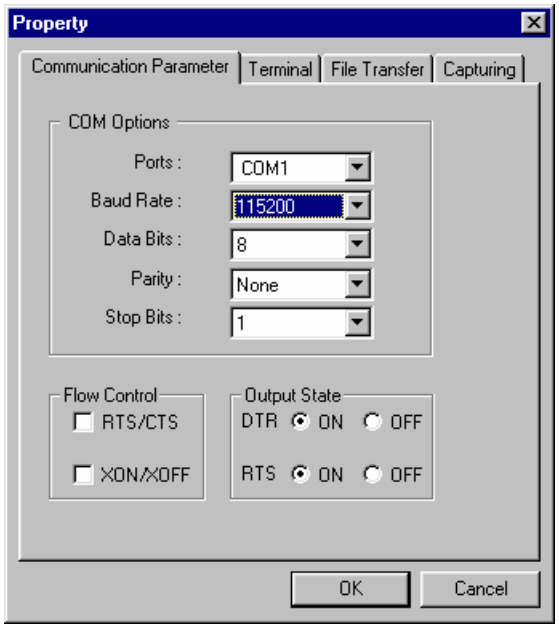
1. From the Windows desktop, click **Start → Programs → PCommLite2.5 → Terminal Emulator.**



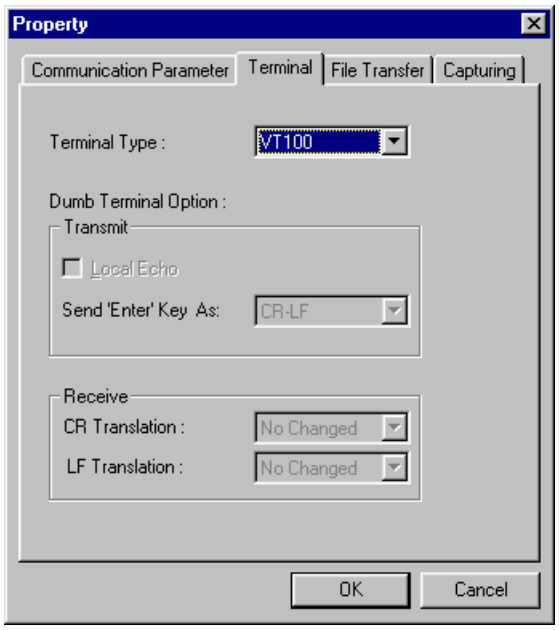
2. Select **Open** under **Port Manager** to open a new connection.



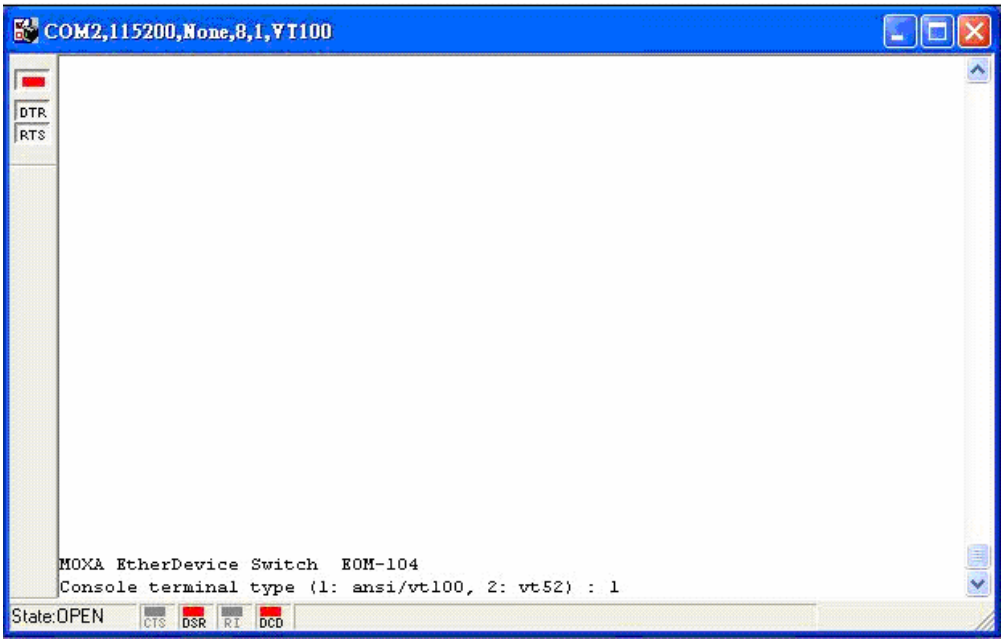
3. The **Communication Parameter** page of the **Property** window opens. Select the appropriate COM port for **Console Connection**, **115200** for **Baud Rate**, **8** for **Data Bits**, **None** for **Parity**, and **1** for **Stop Bits**.



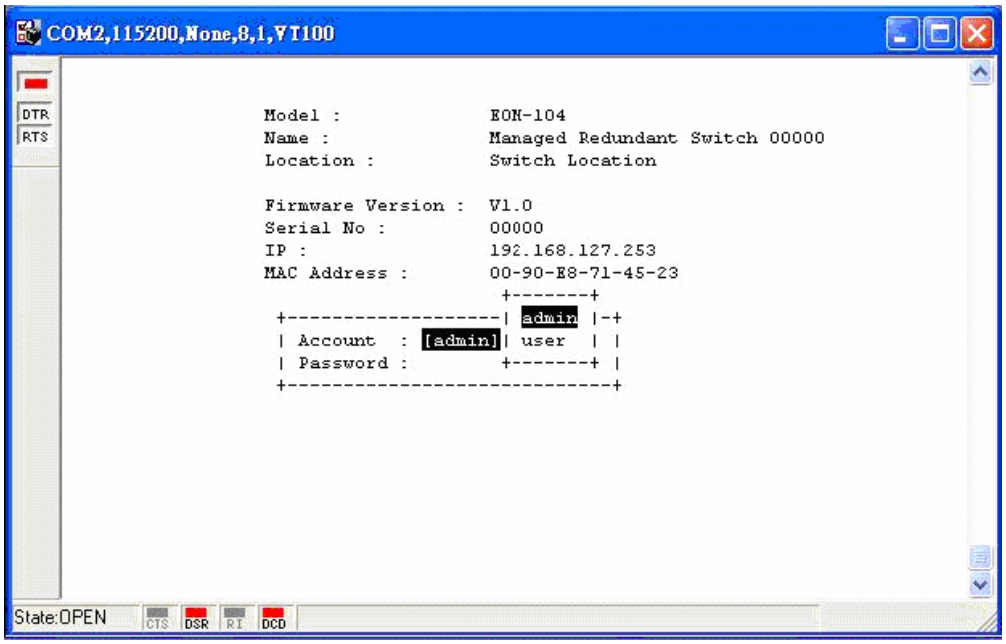
4. Click the **Terminal** tab, and select **VT100** for **Terminal Type**. Click **OK** to confirm.



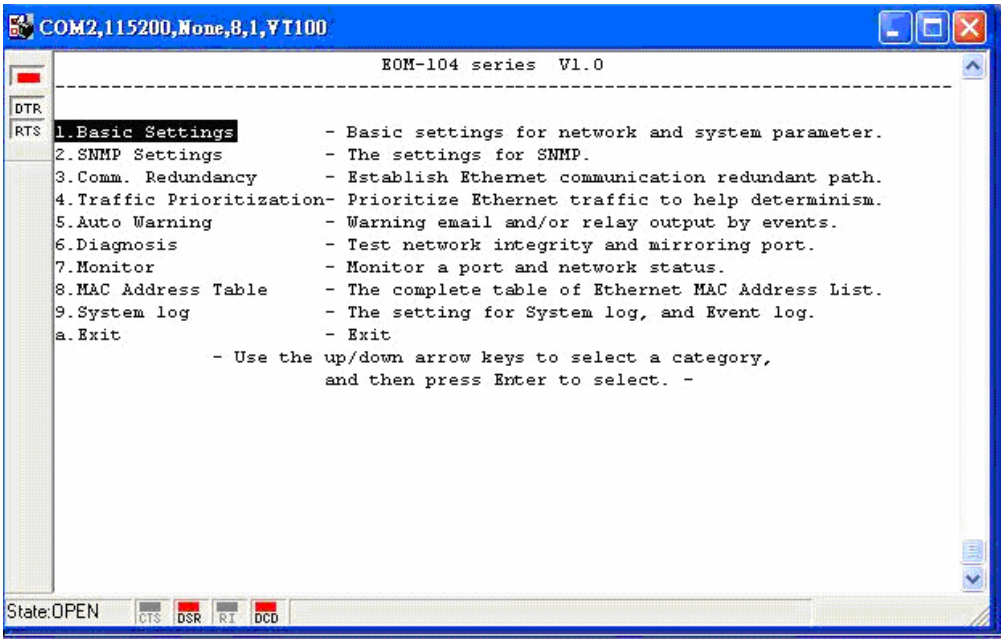
5. Type **1** to select **ansi/VT100** terminal type, and then press **Enter**.



6. The Console login screen will be displayed. Press **Enter** to open the Account pop-up selector and then select either **admin** or **user**. Use the keyboard's down arrow to move the cursor to the Password field, enter the **Console Password** (this is the same as the Web Browser password; leave the **Password** field blank if a console password has not been set), and then press **Enter**.



7. The EOM's **Main Menu** will be displayed. (NOTE: To modify the appearance of the PComm Terminal Emulator window, select **Font…** under the **Edit** menu, and then choose the desired formatting options.)



8. After entering the Main Menu, use the following keys to move the cursor, and to select options.

Key	Function
Up/Down/Left/Right arrows, or Tab	Move the onscreen cursor
Enter	Display & select options
Space	Toggle options
Esc	Previous Menu

Configuration Using a Telnet Console

You may use Telnet to access the EOM's console utility over a network. To be able to access the EOM's functions over the network (using Telnet or a Web Browser) from a PC host that is connected to the same LAN as the EOM, you need to make sure that the PC host and the EOM are on the same logical sub network. To do this, check your PC host's IP address and netmask. By default, the EOM's IP address is 192.168.127.253 and the EOM's netmask is 255.255.0.0 (for a Class B network). If you do not change these values, and your PC host's netmask is 255.255.0.0, then its IP address must have the form 192.168.xxx.xxx. On the other hand, if your PC host's netmask is 255.255.255.0, then its IP address must have the form 192.168.127.xxx.

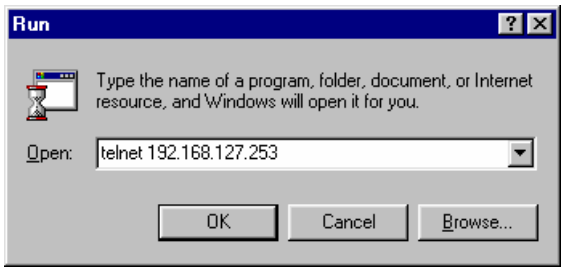
NOTE To use the EOM's management and monitoring functions from a PC host connected to the same LAN as the EOM, you must make sure that the PC host and the EOM are on the same logical sub network.

NOTE Before accessing the console utility via Telnet, first connect one of the EOM's RJ45 Ethernet ports to your Ethernet LAN, or directly to your PC's Ethernet NIC. You can establish a connection with either a straight-through or cross-over Ethernet cable. If you have difficulty connecting, refer to the Auto MDI/MDI-X Connection section from the Hardware installation Guide for more information about the different types of Ethernet cables and ports.

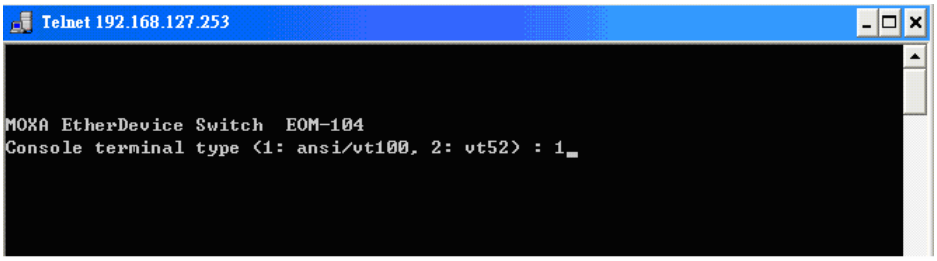
NOTE The EOM's default IP is **192.168.127.253**.

Perform the following steps to access the console utility via Telnet.

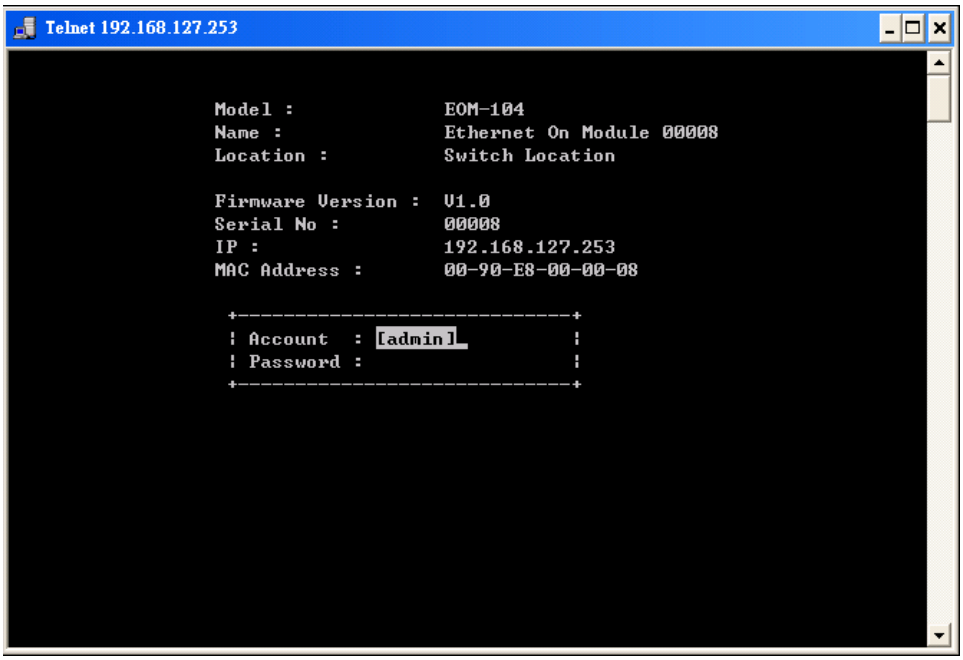
1. Telnet to the EOM's IP address from the Windows **Run** window (or from the command prompt).



2. Type **1** to choose **ansi/vt100**, and then press **Enter**.



3. The Console login screen will be displayed. Press **Enter** to open the Account pop-up selector and then select either **admin** or **user**. Use the keyboard's down arrow to move the cursor to the Password field, enter the **Console Password** (this is the same as the Web Browser password; leave the **Password** field blank if a console password has not been set), and then press **Enter**.



4. The EOM's **Main Menu** will be displayed. (**NOTE:** To modify the appearance of the PComm Terminal Emulator window, select **Font…** under the **Edit** menu, and then choose the desired formatting options.)

NOTE The Telnet Console looks and operates in precisely the same manner as the RS-232 Console.

Configuration Using a Web Browser

The EOM's web browser interface provides a convenient way to modify the switch's configuration and access the built-in monitoring and network administration functions. The recommended web browser is Microsoft Internet Explorer 5.5 or 6.0 with JVM (Java Virtual Machine) installed.

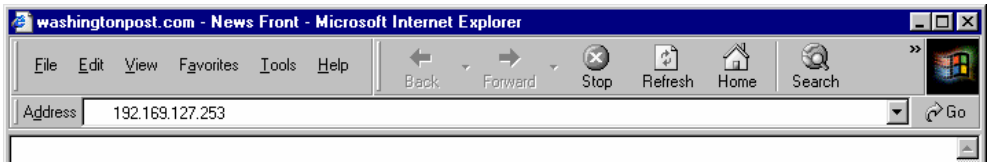
NOTE To use the EOM's management and monitoring functions from a PC host connected to the same LAN as the EOM, you must make sure that the PC host and the EOM are on the same logical sub network.

NOTE Before accessing the EOM's web browser interface, first connect one of the EOM's RJ45 Ethernet ports to your Ethernet LAN, or directly to your PC's Ethernet NIC. You can establish a connection with either a straight-through or cross-over Ethernet cable. If you have difficulty connecting, refer to the Auto MDI/MDI-X Connection section from the Hardware installation Guide for more information about the different types of Ethernet cables and ports.

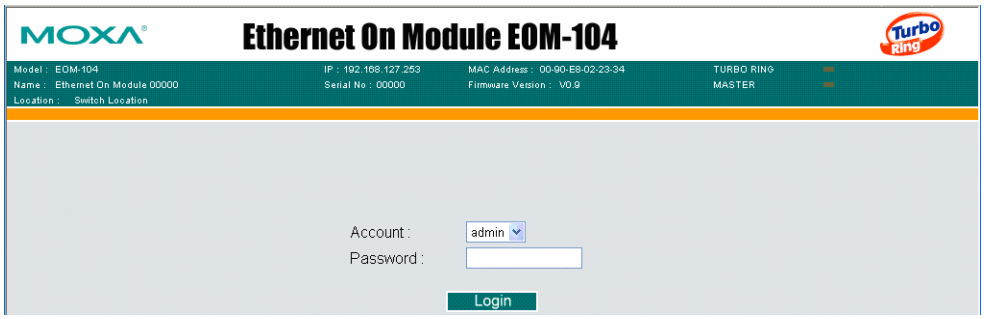
NOTE The EOM's default IP is **192.168.127.253**.

Perform the following steps to access the EOM's web browser interface.

1. Open Internet Explorer and type the EOM's IP address in the **Address** field. Press **Enter** to establish the connection.

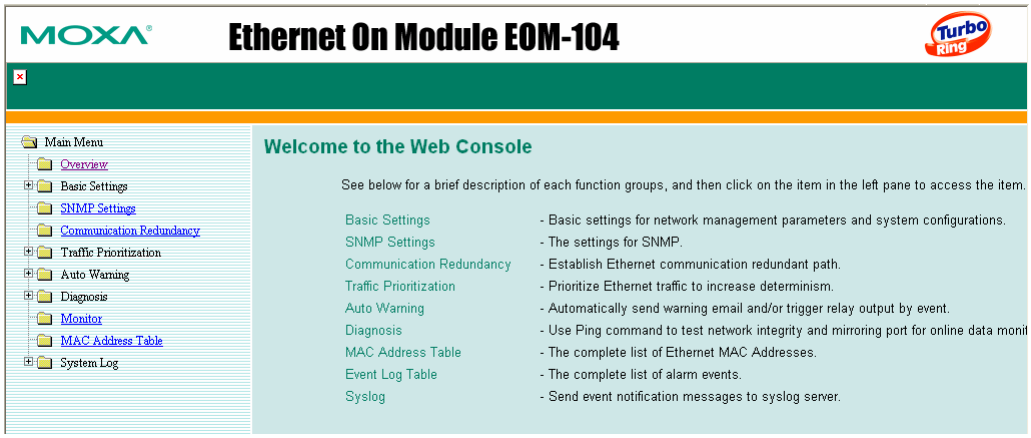


2. The web login page will be displayed. Select the login account (Admin or User) and enter the **Password** (this is the same as the Console password), and then click **Login** to continue. Leave the **Password** field blank if a password has not been set.



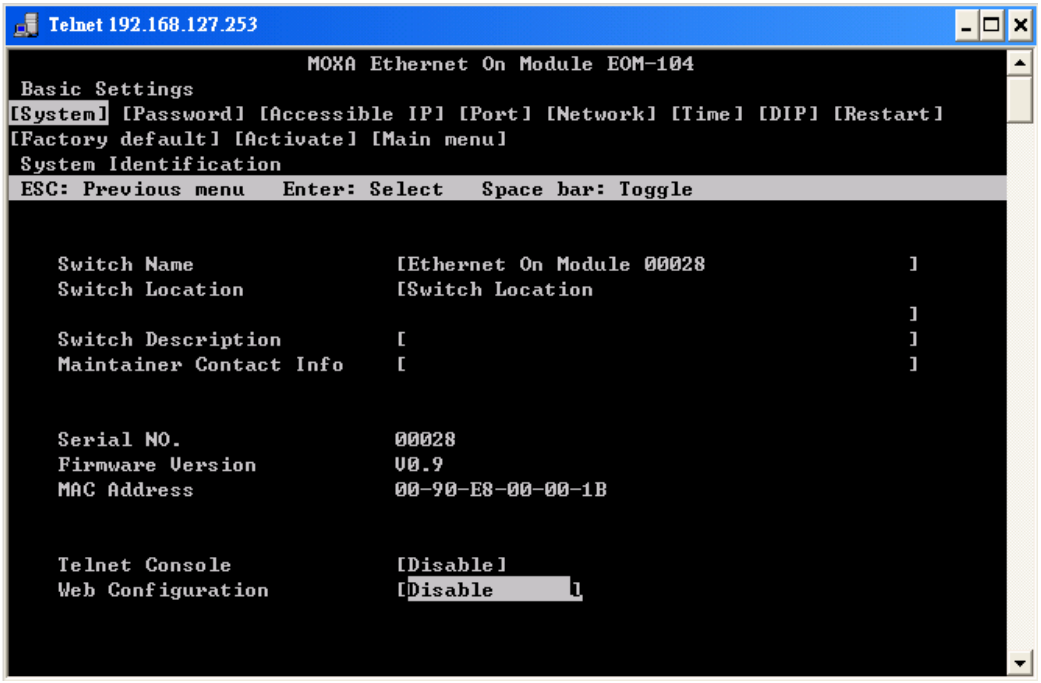
NOTE By default, the EOM's Password is not set (i.e., is blank).

You may need to wait a few moments for the web page to be downloaded to your computer. Use the menu tree on the left side of the window to open the function pages to access each of the EOM's functions.



Disabling Telnet and Browser Access

If you are connecting the EOM to a public network, but do not intend to use its management functions over the network, then we suggest disabling both **Telnet Console** and **Web Configuration** from the RS-232 Console's **Basic Settings → System** page, as shown in the following figure.



NOTE If you are connecting the EOM to a public network, but do not intend to use its management functions over the network, then we suggest disabling both **Telnet Console** and **Web Configuration**.

3

Featured Functions

This chapter explains how to access a Moxa Ethernet-On-Module switch's various configuration, monitoring, and administration functions. There are three ways to access these functions: serial console, Telnet console, and web browser. The serial console connection method, which requires using a short serial cable to connect the EOM to a PC's COM port, can be used if you do not know the EOM's IP address. The Telnet console and web browser connection methods can be used to access the EOM over an Ethernet LAN, or over the Internet.

The Web Console is the most user-friendly way to configure your EOM. In this chapter, we use the Web Console interface to introduce the EOM's functions. There are only a few differences between the Web Console, Serial Console, and Telnet Console access methods.

The following topics are covered in this chapter:

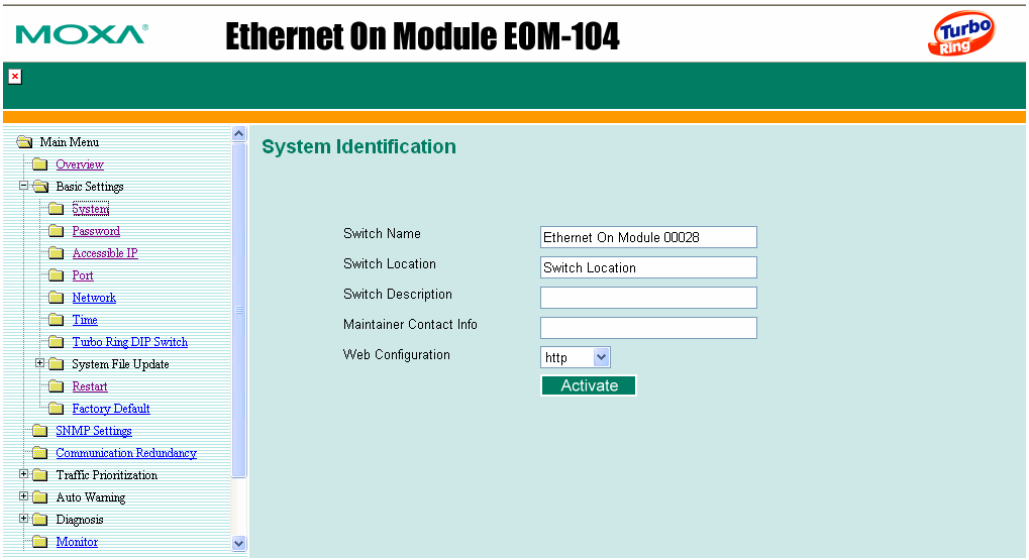
- **Configuring Basic Settings**
- **Configuring SNMP**
- **Using Communication Redundancy**
- **Using Traffic Prioritization**
- **Using Auto Warning**
- **Diagnosis**
- **Using the Monitor**
- **Using the MAC Address Table**
- **Using Event Log**
- **Using Syslog**

Configuring Basic Settings

The Basic Settings group includes the most commonly used settings required by administrators to maintain and control the EOM.

System Identification

The system identification items are displayed at the top of the web page, and will be included in alarm emails. Setting system identification items makes it easier to identify the different switches connected to your network.



Switch Name

Setting	Description	Factory Default
Max. 40 Characters	This option is useful for specifying the role or application of different EOM units. E.g., Factory Switch 1.	Industrial Redundant Switch [*Serial No. of this switch*]

Switch Location

Setting	Description	Factory Default
Max. 80 Characters	To specify the location of different EOM units. E.g., production line 1.	Switch Location

Switch Description

Setting	Description	Factory Default
Max. 40 Characters	Use this to record a more detailed description of the EOM unit.	None

Maintainer Contact Info

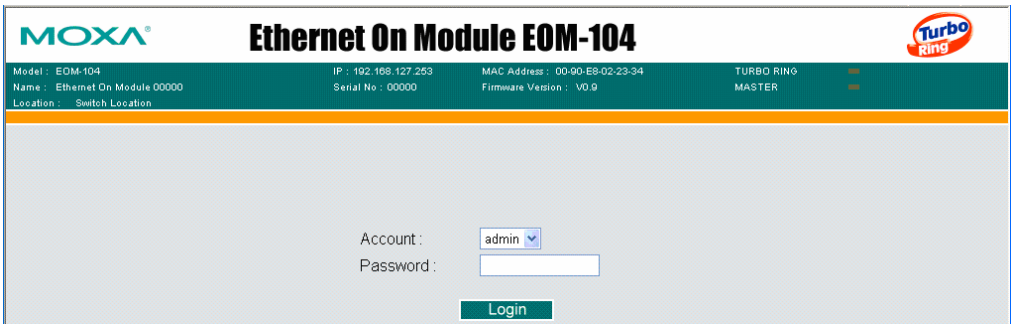
Setting	Description	Factory Default
Max.40 Characters	Use this to record contact information of the person responsible for maintaining this EOM-104 Series.	None

Web Configuration

Setting	Description	Factory Default
http/disable	Use this to enable or disable Web Configuration	http

Password

The EOM-104 Series provides two levels of access privileges: **admin** privilege gives read/write access to all EOM configuration parameters; **user** privilege provides read access only—you will be able to view the configuration, but will not be able to make modifications.



ATTENTION

The EOM's default Password is not set (i.e., is blank). If a Password is already set, then you will be required to type the Password when logging into the RS-232 Console, Telnet Console, or Web Browser interface.

Account

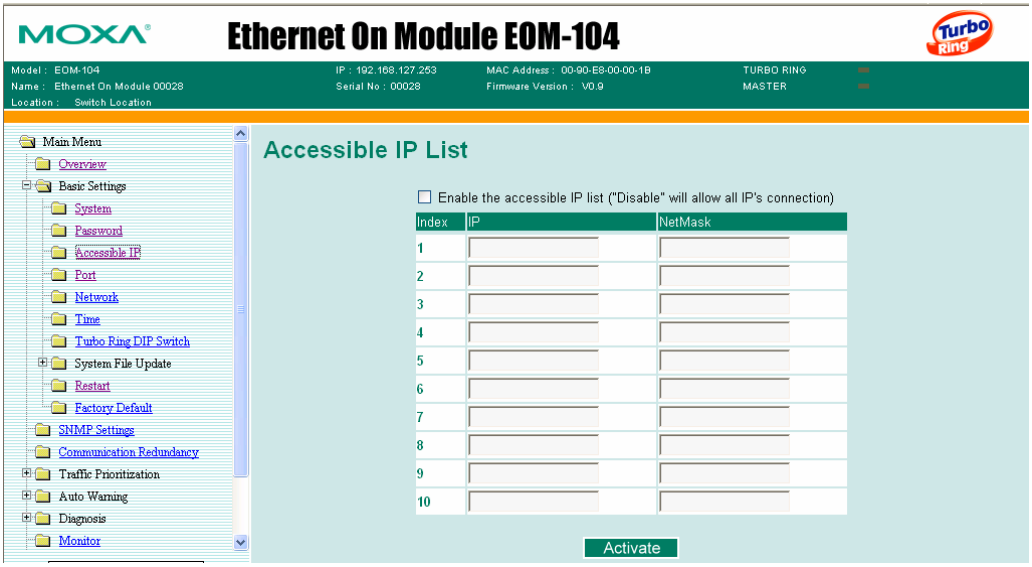
Setting	Description	Factory Default
admin	***admin*** privilege allows the user to modify all EOM configurations.	admin
user	***user*** privilege only allows viewing EOM configurations.	

Password

Setting	Description	Factory Default
Old Password (Max. 16 Characters)	Type current password when changing the password	None
New Password **(**Max. 16 Characters)	Type new password when changing the password	None
Retype Password (Max. 16 Characters)	If you type a new password in the Password field, you will be required to retype the password in the Retype new password field before updating the new password.	None

Accessible IP

An IP address-based filtering method to control access to EOM switches.



Accessible IP Settings allows you to add or remove ***Legal*** remote host IP addresses to prevent unauthorized access. Access to the EOM is controlled by IP addresses. That is, if a host's IP address is in the accessible IP table, then the host will be allowed access to the EOM. You can allow one of the following cases by setting this parameter

- **Only one host with the specified IP address can access the EOM-104 Series**

  E.g., enter "192.168.1.1/255.255.255.255" to allow access to just the IP address 192.168.1.1.

- **Any host on a specific sub network can access the EOM-104 Series**

  E.g., enter "192.168.1.0/255.255.255.0" to allow access to all IPs on the sub network defined by this IP address/netmask combination.

- **Any host can access the EOM-104 Series**

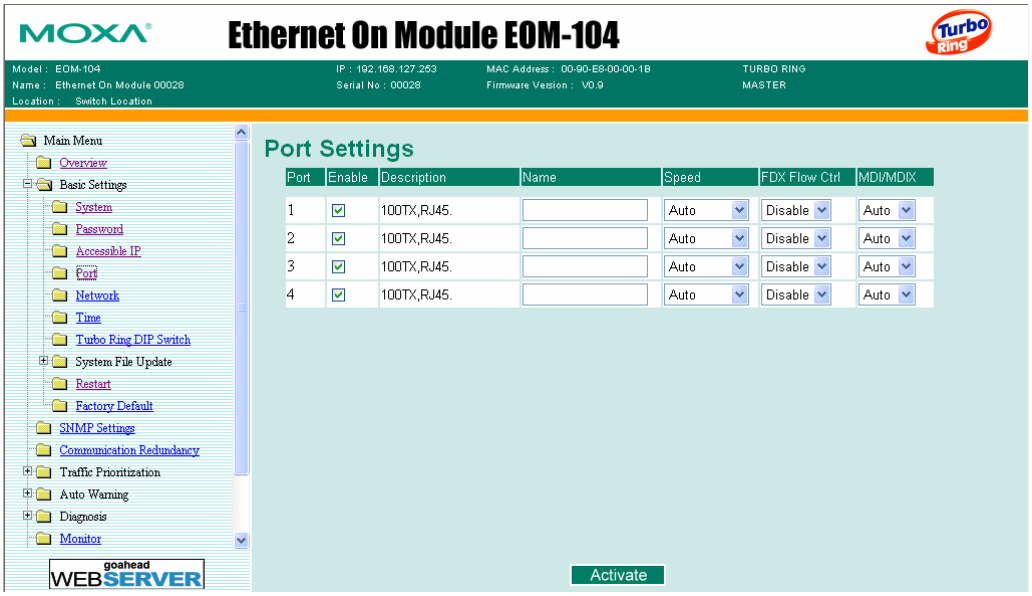
  Disable this function by not selecting the ***Enable the accessible IP list*** checkbox.

The following table shows additional configuration examples:

Allowable Hosts	Input format
Any host	Disable
192.168.1.120	192.168.1.120 / 255.255.255.255
192.168.1.1 to 192.168.1.254	192.168.1.0 / 255.255.255.0
192.168.0.1 to 192.168.255.254	192.168.0.0 / 255.255.0.0
192.168.1.1 to 192.168.1.126	192.168.1.0 / 255.255.255.128
192.168.1.129 to 192.168.1.254	192.168.1.128 / 255.255.255.128

Port

Port settings are included to give the user control over Port Access, Port Transmission Speed, Flow Control, and Port Type (MDI or MDIX). An explanation of each configuration item is given below.



Enable

Setting	Description	Factory Default
checked	Allows data transmission through the port.	disabled
unchecked	Immediately shuts off port access.	

ATTENTION

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

Name

Setting	Description	Factory Default
Max. 63 Characters	Specify an alias for each port, and assist the administrator in remembering important information about the port. E.g., PLC 1	None

Port Transmission 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-nego
100M-Full	Choose one of these fixed speed options if the Ethernet device at the other end has trouble auto-negotiating for line speed.	
100M-Half		
10M-Full		
10M-Half		

FDX Flow Control

This setting enables or disables the flow control capability of this port when the ***port transmission speed*** setting is on ***auto*** mode. The final result will be determined by the ***auto*** process between the EOM and the connected device.

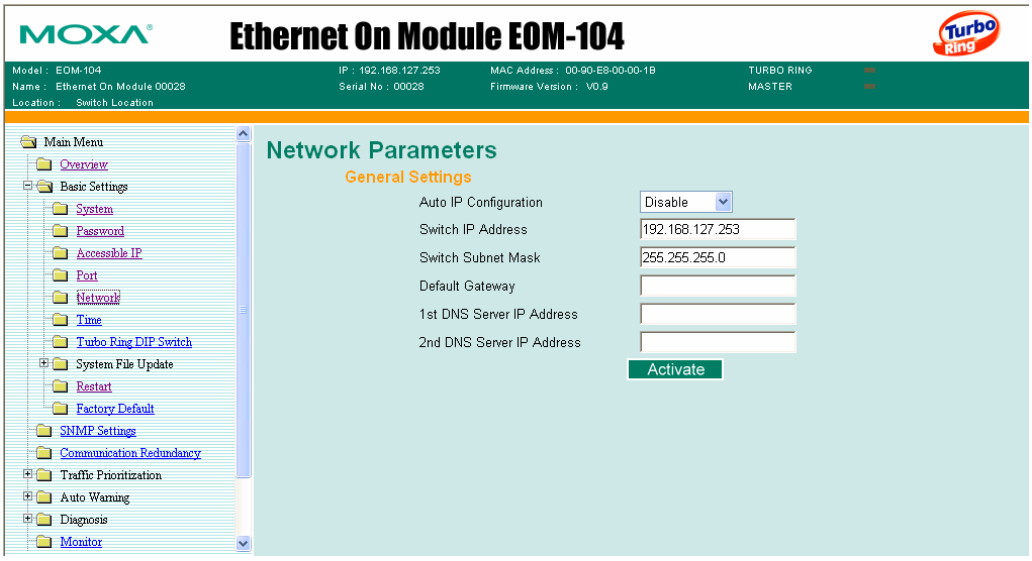
Setting	Description	Factory Default
Enable	Enables the flow control capability of this port when in auto-nego mode.	Disable
Disable	Disables the flow control capability of this port when in auto-nego mode.	

MDI/MDIX

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

Network

The **Network** configuration allows users to modify the usual TCP/IP network parameters. An explanation of each configuration item follows.



Auto IP Configuration

Setting	Descriptions	Factory Default
Disable	Set up the EOM's IP address manually.	Disable
By DHCP	The EOM's IP address will be assigned automatically by the network's DHCP server.	
By BootP	The EOM's IP address will be assigned automatically by the network's BootP server.	

Switch IP Address

Setting	Descriptions	Factory Default
IP Address of the EOM	Identifies the EOM on a TCP/IP network.	192.168.127.253

Switch Subnet Mask

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

Default Gateway

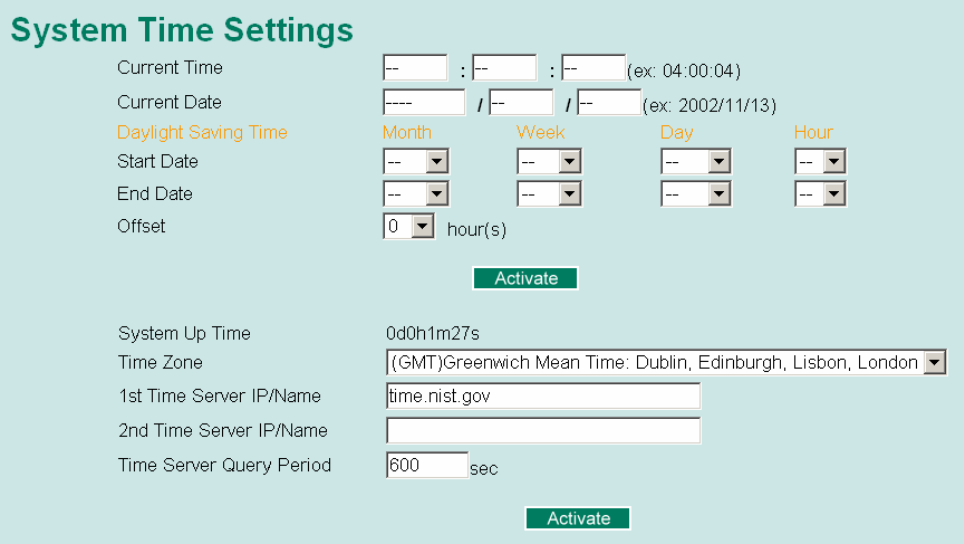
Setting	Descriptions	Factory Default
Default Gateway of the EOM	The IP address of the router that connects the LAN to an outside network.	*None*

DNS IP Address

Setting	Descriptions	Factory Default
1st DNS Server's IP Address	The IP address of the DNS Server used by your network. After entering the DNS Server's IP address, you can input the EOM's URL (e.g., www.eds.company.com) in your browser's address field, instead of entering the IP address.	None
2nd DNS Server's IP Address	The IP address of the DNS Server used by your network. The EOM will try to locate the 2nd DNS Server if the 1st DNS Server fails to connect.	None

Time

The **Time** configuration page lets users set the time, date, and other settings. An explanation of each setting is given below the figure.



The EOM has a time calibration function based on information from an NTP server or user specified Time and Date information. Functions such as **Auto warning Email** can add real-time information to the message.

NOTE The EOM does not have a real time clock. The user must update the **Current Time** and **Current Date** to set the initial time for the EOM after each reboot, especially when the network does not have an Internet connection for NTP server or there is no NTP server on the LAN.

Current Time

Setting	Description	Factory Default
User adjustable time.	The time parameter allows configuration of the local time in local 24-hour format.	None (hh:mm:ss)

Current Date

Setting	Description	Factory Default
User adjustable date.	The date parameter allows configuration of the local date in yyyy/mm/dd format.	None (yyyy/mm/dd)

Daylight Saving Time

Daylight saving time (also know as **DST** or **summer time**) involves advancing clocks (usually 1 hour) during the summer time to provide an extra hour of daylight in the afternoon.

Start Date

Setting	Description	Factory Default
User adjustable date.	The Start Date parameter allows users to enter the date that daylight saving time begins.	None

End Date

Setting	Description	Factory Default
User adjustable date.	The End Date parameter allows users to enter the date that daylight saving time ends.	None

Offset

Setting	Description	Factory Default
User adjustable hour.	The offset parameter indicates how many hours forward the clock should be advanced.	None

System Up Time

Indicates the EOM's up time from the last cold start. The unit is seconds.

Time Zone

Setting	Description	Factory Default
User selectable time zone	The time zone setting allows conversion from GMT (Greenwich Mean Time) to local time.	GMT (Greenwich Mean Time)

NOTE Changing the time zone will automatically correct the current time. You should **configure the time zone before setting the time**.

Time Server IP/Name

Setting	Description	Factory Default
1st Time Server IP/Name	IP or Domain address (e.g., 192.168.1.1 or time.stdtime.gov.tw or time.nist.gov)	None
2nd Time Server IP/Name	The EOM will try to locate the 2nd NTP Server if the connection to the 1st NTP server failed.	

Time Server Query Period

Setting	Description	Factory Default
Query Period	This parameter determines how frequently the time is updated from the NTP server.	600 seconds

Turbo Ring DIP Switch

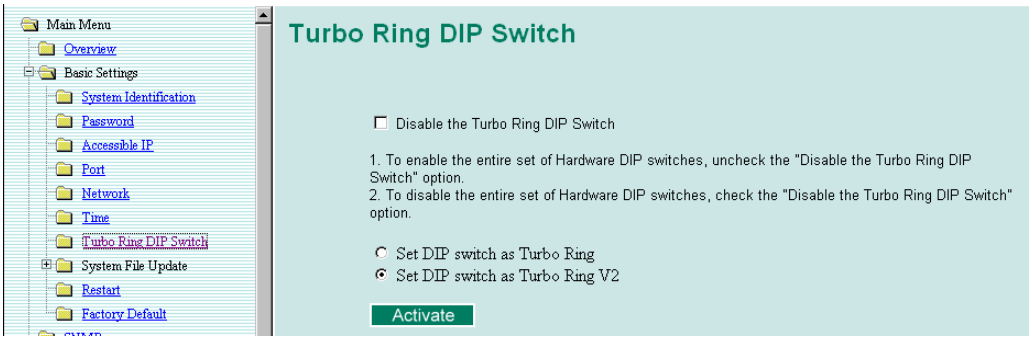
The **Turbo Ring DIP Switch** page allows users to disable the six DIP switches located on the EOM's evaluation board. When enabled, the DIP switches can be used to configure basic settings for either the "Turbo Ring" protocol or "Turbo Ring V2" protocol. A complete description of the settings is given below.

NOTE The proprietary "Turbo Ring" protocol (recovery time < 300 ms) was developed by Moxa in 2003 to provide better network reliability and faster recovery time for redundant ring topologies. The "Turbo Ring V2" protocol (recovery time < 20 ms), which was released in 2007, supports additional redundant ring architectures.

In this manual, we use the terminology ***"Turbo Ring" ring*** and ***"Turbo Ring V2" ring*** to differentiate between rings configured for one or the other of these protocols.

For a detailed description of "Turbo Ring" and "Turbo Ring V2," please refer to the **Using Communication Redundancy** section later in this chapter.

How to Enable or Disable the Turbo Ring DIP Switches



Disable the Turbo Ring DIP Switch

Setting	Description	Factory Default
Enable the Turbo Ring DIP Switches	The six DIP switches are *enabled* when the "Disable the Turbo Ring DIP Switch" box is not checked.	Not checked (i.e., the Turbo Ring DIP Switches are enabled by default)
Disable the Turbo Ring DIP Switches	The six DIP switches are *disabled* when the "Disable the Turbo Ring DIP Switch" box is checked.	

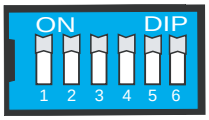
Set DIP switch as Turbo Ring / Set DIP switch as Turbo Ring V2

Setting	Description	Factory Default
Set DIP switch as Turbo Ring	Select this option to enable the Turbo Ring DIP switches to configure the EOM for a "Turbo Ring" ring.	This is the default if you do NOT reset the switch to factory default settings (provided you upgraded the firmware for Turbo Ring V2).
Set DIP switch as Turbo Ring V2	Select this option to enable the Turbo Ring DIP switches to configure the EOM for a "Turbo Ring V2" ring.	This is the default if you DO reset the switch to factory default settings (provided you upgraded the firmware for Turbo Ring V2).

How to Configure the Turbo Ring DIP Switches

The Turbo Ring DIP Switches are set to the OFF position at the factory.

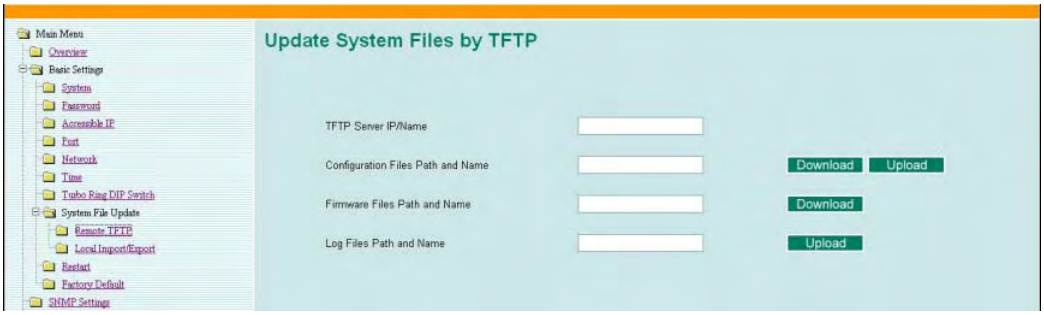
NOTE The six DIP Switches are used to configure both the "Turbo Ring" and "Turbo Ring V2" protocols, depending on which protocol is active. To select which protocol the EOM will use, start the user interface software, and then use the left menu to navigate to the **Communication Redundancy** page. To use one of the Turbo Ring protocols for the EOM, select either "Turbo Ring" or "Turbo Ring V2" in the **Redundancy Protocol** drop-down box. See the **Configuring "Turbo Ring" and "Turbo Ring V2"** section in this chapter for details.



The following tables show how to use the DIP switches to configure the EOM for "Turbo Ring" or "Turbo Ring V2."

	ON	OFF
DIP1	Enable this EOM as the Ring Master	This EOM will not be the Ring Master
DIP2	Activate Turbo Ring or Turbo Ring V2	Do not use Turbo Ring or Turbo Ring V2
DIP3	GPIO Reserve	GPIO Reserve
DIP4	GPIO Reserve	GPIO Reserve
DIP5	GPIO Reserve	GPIO Reserve
DIP6	GPIO Reserve	GPIO Reserve

System File Update—By Remote TFTP



The EOM supports saving your configuration file to a remote TFTP server or local host to allow other EOM switches to use the same configuration at a later time, or saving the Log file for future reference. Loading pre-saved firmware or a configuration file from the TFTP server or local host is also supported for easy upgrading or configuration of the EOM.

TFTP Server IP/Name

Setting	Description	Factory Default
IP Address of the TFTP Server	The IP or name of the remote TFTP server. Must be set up before downloading or uploading files.	None

Configuration Files Path and Name

Setting	Description	Factory Default
Max. 40 Characters	The path and file name of the EOM's configuration file on the TFTP server.	None

Firmware Files Path and Name

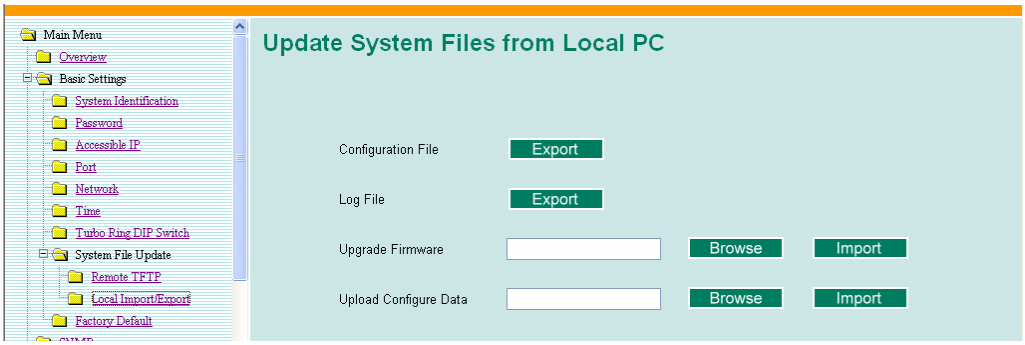
Setting	Description	Factory Default
Max. 40 Characters	The path and file name of the EOM's firmware file.	None

Log Files Path and Name

Setting	Description	Factory Default
Max. 40 Characters	The path and file name of the EOM's log file	None

After setting up the desired path and file name, click **Activate** to save the setting, and then click **Download** to download the prepared file from the remote TFTP server, or click **Upload** to upload the desired file to the remote TFTP server.

System File Update—By Local Import/Export



Configuration File

To export the configuration file of this EOM, click **Export** to save it to the local host.

Log File

To export the Log file of this EOM, click **Export** and save it to the local host.

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

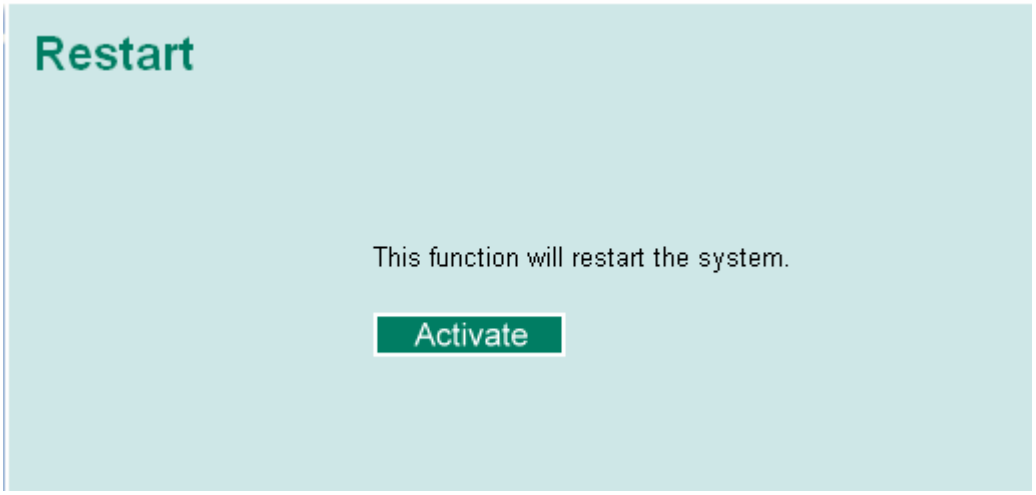
Upgrade Firmware

To import the firmware file of the EOM, click **Browse** to select the firmware file already saved on your computer. The upgrade procedure will proceed automatically after you click **Import**.

Upload Configuration Data

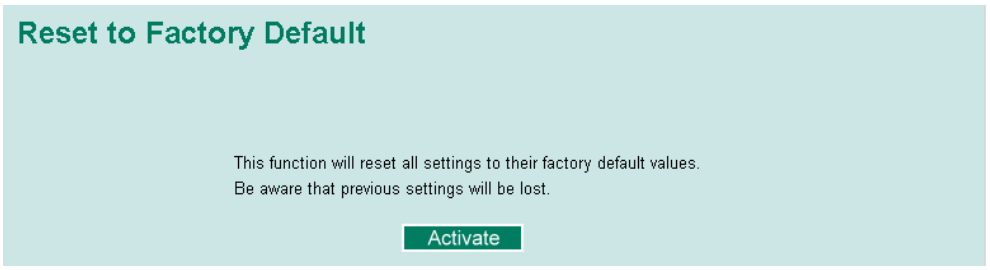
To import the configuration file of the EOM, click **Browse** to select the configuration file already saved on your computer. The upgrade procedure will proceed automatically after you click **Import**.

Restart



This function is used to restart the Moxa Ethernet-On-Module Switch.

Factory Default



The Factory Default function is included to give users a quick way of restoring the EOM's configuration settings to their factory default values. This function can be accessed from either the telnet/RS-232 Console, or Web Browser interface.

NOTE After activating the Factory Default function, you must use the default network settings to re-establish a web-browser or Telnet connection with your Moxa Ethernet-On-Module Switch.

Configuring SNMP

EOM switches support SNMP protocol. The available versions are SNMP V1, SNMP V2c, and SNMP V3. SNMP V1 and SNMP V2c use a community string match for authentication, which means SNMP servers access all objects with read-only or read/write permissions using the community string *public/private* (default value). SNMP V3, which requires you to select an authentication level of MD5 or SHA, is the most secure protocol. You can also enable data encryption to enhance data security.

SNMP security modes and security levels supported by the EOM 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	Security Mode	Authentication Type	Data Encryption	Method
SNMP V1, V2c	V1, V2c Read Community	Community string	No	Use a community string match for authentication
	V1, V2c Write/Read Community	Community string	No	Use a community string match for authentication
SNMP V3	No-Auth	No	No	Use account with admin or user to access objects
	MD5 or SHA	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	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.

The SNMP page can be configured. A more detailed explanation of each parameter follows:

SNMP Read/Write Settings

SNMP Versions

Setting	Description	Factory Default
V1, V2c, V3	Select SNMP protocol versions V1, V2c, V3 to manage the switch	V1, V2c
V1, V2c	Select SNMP protocol versions V1, V2c to manage the switch	
V3 only	Select only SNMP protocol version V3 to manage the switch	

V1, V2c Read Community

Setting	Description	Factory Default
V1, V2c Read Community	Use a community string match for authentication. This means that the SNMP agent accesses all objects with read-only permissions using the community string *public*.	public Maximum 30 characters

V1, V2c Write/Read Community

Setting	Description	Factory Default
V1, V2c Read/Write Community	Uses a community string match for authentication, which means that SNMP servers access all objects with read/write permissions using the community string *private*.	private Maximum 30 characters

For SNMP V3, there are two levels of privilege for different accounts to access the EOM. **Admin** privilege allows access, and authorization to read and write the MIB file. **User** privilege only allows reading the MIB file, but does not authorize writing.

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

Setting	Description	Factory Default
No-Auth	Use admin account to access objects. No authentication	No
MD5-Auth	Provide authentication based on the HMAC-MD5 algorithms. 8-character passwords are the minimum requirement for authentication.	No
SHA-Auth	Provide authentication based on the HMAC-SHA algorithms. 8-character passwords are the minimum requirement for authentication.	No

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

Setting	Description	Factory Default
Enable	8-character data encryption key is the minimum requirement for data encryption. Maximum 30-character encryption key	No
Disable	No data encryption	No

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

Setting	Description	Factory Default
No-Auth	Use the admin or user account to access objects. No authentication.	No
MD5-Auth	Provide authentication based on the HMAC-MD5 algorithms. 8-character passwords are the minimum requirement for authentication.	No
SHA-Auth	Provide authentication based on the HMAC-SHA algorithms. 8-character passwords are the minimum requirement for authentication.	No

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

Setting	Description	Factory Default
Enable	8-character data encryption key is the minimum requirement for data encryption. Maximum 30-character encryption key.	No
Disable	No data encryption	No

Trap Settings

Trap Server IP/Name

Setting	Description	Factory Default
IP or Name	Enter the IP address or name of the Trap Server used by your network.	None

Trap Community

Setting	Description	Factory Default
character string	Use a community string match for authentication; Maximum of 30 characters.	public

Private MIB information

Switch Object ID

Setting	Description	Factory Default
8691.7.31	The EOM-104's enterprise value	Fixed
8691.7.37	The EOM-104-FO's enterprise value	Fixed

This value cannot be changed.

Using Communication Redundancy

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

The Communication Redundancy function allows the user to set up **redundant loops** in the network to provide a backup data transmission route in the event that a cable is inadvertently disconnected or damaged. This feature is particularly important for industrial applications, since it could take several minutes to locate the disconnected or severed cable. For example, if the EOM is used as a key communications component of a production line, several minutes of downtime could result in a big loss in production and revenue. The EOM supports three different protocols to support this communication redundancy function—**Rapid Spanning Tree/ Spanning Tree Protocol (IEEE 802.1W/1D), Turbo Ring**, and **Turbo Ring V2**.

When configuring a redundant ring, all switches on the same ring must be configured to use the same redundancy protocol. You cannot mix the "Turbo Ring," "Turbo Ring V2," and STP/RSTP protocols on the same ring. The following table lists the key differences between each feature. Use this information to evaluate the benefits of each, and then determine which features are most suitable for your network.

	Turbo Ring V2	Turbo Ring	STP	RSTP
Topology	Ring	Ring	Ring, Mesh	Ring, Mesh
Recovery Time	< 20 ms	< 300 ms	Up to 30 sec.	Up to 5 sec

NOTE Most of Moxa's managed switches now support two proprietary Turbo Ring protocols:

(1) **"Turbo Ring"** refers to the original version of Moxa's proprietary redundant ring protocol, which has a recovery time of under 300 ms.

(2) **"Turbo Ring V2"** refers to the new generation Turbo Ring, which has a recovery time of under 20 ms.

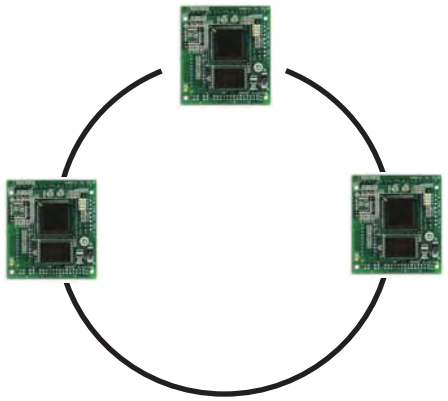
In this manual, we use the terminology ***"Turbo Ring" ring*** and ***"Turbo Ring V2" ring*** to differentiate between rings configured for one or the other of these protocols.

The Turbo Ring Concept

Moxa developed the proprietary Turbo Ring protocol to optimize communication redundancy and achieve a faster recovery time on the network.

The Turbo Ring and Turbo Ring V2 protocols identify one switch as the **master** of the network, and then automatically block packets from traveling through any of the network's redundant loops. In the event that one branch of the ring gets disconnected from the rest of the network, the protocol automatically readjusts the ring so that the part of the network that was disconnected can reestablish contact with the rest of the network.

Initial setup of a "Turbo Ring" or "Turbo Ring V2" ring

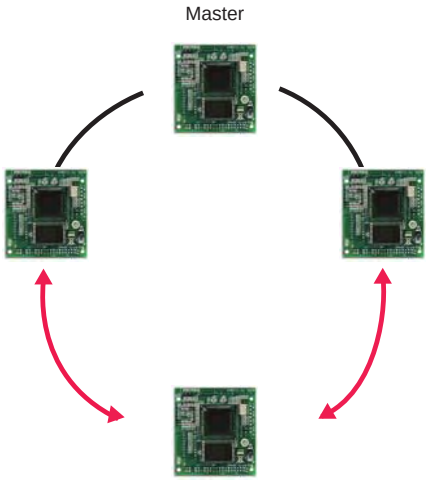


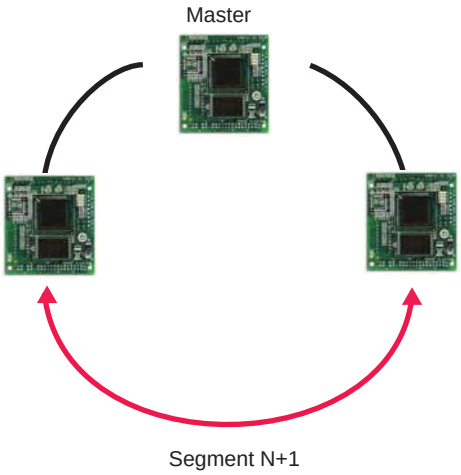
1. For each switch in the ring, select any two ports as the redundant ports.
2. Connect redundant ports on neighboring switches to form the redundant ring.

The user does not need to configure any of the switches as the master to use Turbo Ring or Turbo Ring V2. If none of the switches in the ring is configured as the master, then the protocol will automatically assign master status to one of the switches. In fact, the master is only used to identify which segment in the redundant ring acts as the backup path. In the following subsections, we explain how the redundant path is selected for rings configured for Turbo Ring, and Turbo Ring V2.

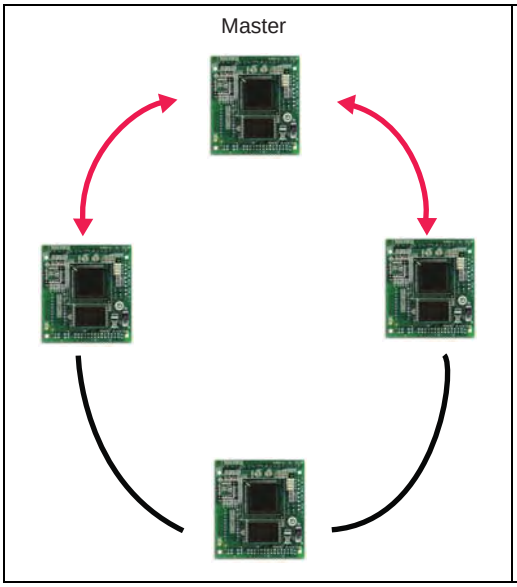
Determining the Redundant Path of a "Turbo Ring" Ring

In this case, the redundant segment (i.e., the segment that will be blocked during normal operation) is determined by the number of EOM units that make up the ring, and where the ring master is located.

"Turbo Ring" rings with an even number of EOM units	
	If there are 2N EOM units (an even number) in the "Turbo Ring" ring, then the backup segment is one of the two segments connected to the (N+1)st EOM (i.e., the EOM unit directly opposite the master).

"Turbo Ring" rings with an odd number of EOM units	
	If there are 2N+1 EOM units (an odd number) in the "Turbo Ring" ring, with EOM units and segments labeled counterclockwise, then segment N+1 will serve as the backup path. For the example shown here, N=1, so that N+1=2.

Determining the Redundant Path of a "Turbo Ring V2" Ring



For a "Turbo Ring V2" ring, the backup segment is the segment connected to the 2nd redundant port on the master.

See **Configuring "Turbo Ring V2"** in the **Configuring "Turbo Ring" and "Turbo Ring V2"** section below.

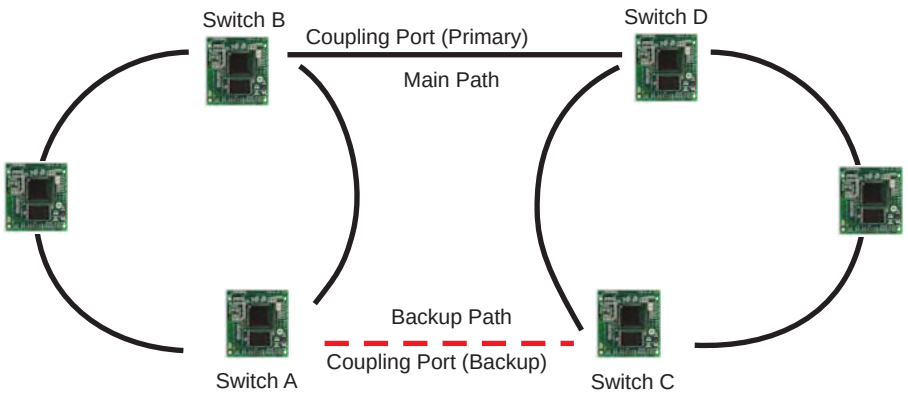
Ring Coupling Configuration

For some systems, it may not be convenient to connect all devices in the system to create one BIG redundant ring, since some devices could be located in a remote area. For these systems, "Ring Coupling" can be used to separate the devices into different smaller redundant rings, but in such a way that they can still communicate with each other.

ATTENTION

In a VLAN environment, the user must set "Redundant Port," and "Coupling Port," to join all VLANs, since these ports act as the "backbone" to transmit all packets of different VLANs to different EOM units.

Ring Coupling for a "Turbo Ring V2" Ring



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

ATTENTION

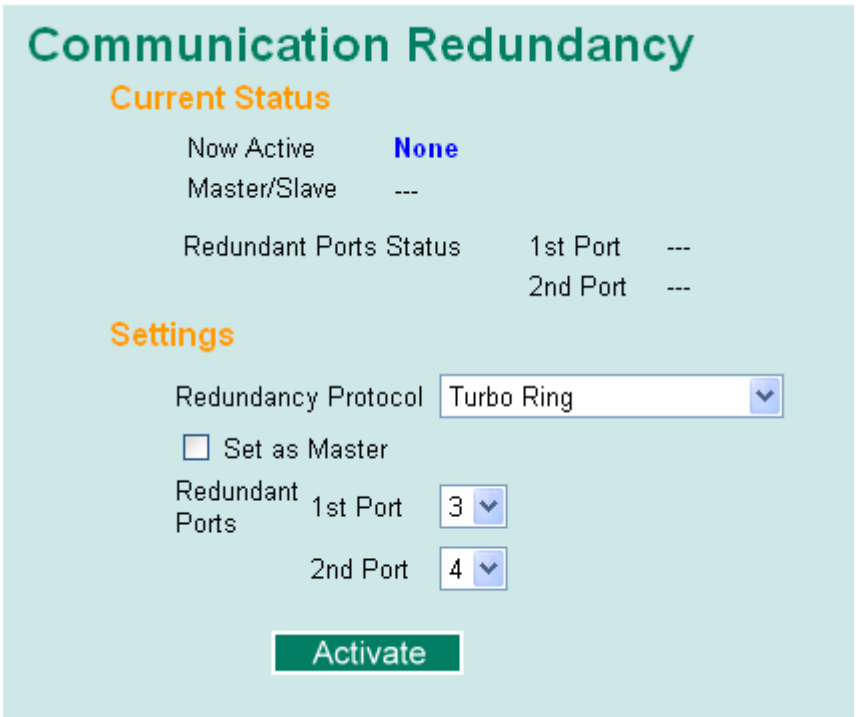
Ring Coupling only needs to be enabled on one of the switches serving as the Ring Coupler. The Coupler must designate different ports as the two Turbo Ring ports and the coupling port.

NOTE You do not need to use the same EOM unit for both Ring Coupling and Ring Master.

Configuring "Turbo Ring" and "Turbo Ring V2"

Use the **Communication Redundancy** page to configure select "Turbo Ring" or "Turbo Ring V2." Note that configuration pages for these two protocols are different.

Configuring "Turbo Ring"



Explanation of "Current Status" Items

Now Active

Shows which communication protocol is in use: **Turbo Ring**, **Turbo Ring V2**, **RSTP**, or **none**.

Master/Slave

Indicates whether or not this EOM is the Master of the Turbo Ring. (This field appears only when selected to operate in Turbo Ring or Turbo Ring V2 mode.)

NOTE The user does not need to set the master to use Turbo Ring. If no master is set, the Turbo Ring protocol will assign master status to one of the EOM units in the ring. The master is only used to determine which segment serves as the backup path.

Redundant Ports Status (1st Port, 2nd Port)

The "Ports Status" indicators show ***Forwarding*** for normal transmission, ***Blocking*** if this port is connected to a backup path and the path is blocked, and ***Link down*** if there is no connection.

Explanation of "Settings" Items

Redundancy Protocol

Setting	Description	Factory Default
Turbo Ring	Select this item to change to the Turbo Ring configuration page.	None
Turbo Ring V2	Select this item to change to the Turbo Ring V2 configuration page.	
RSTP (IEEE 802.1W/1D)	Select this item to change to the RSTP configuration page.	
None	Ring redundancy is not active	

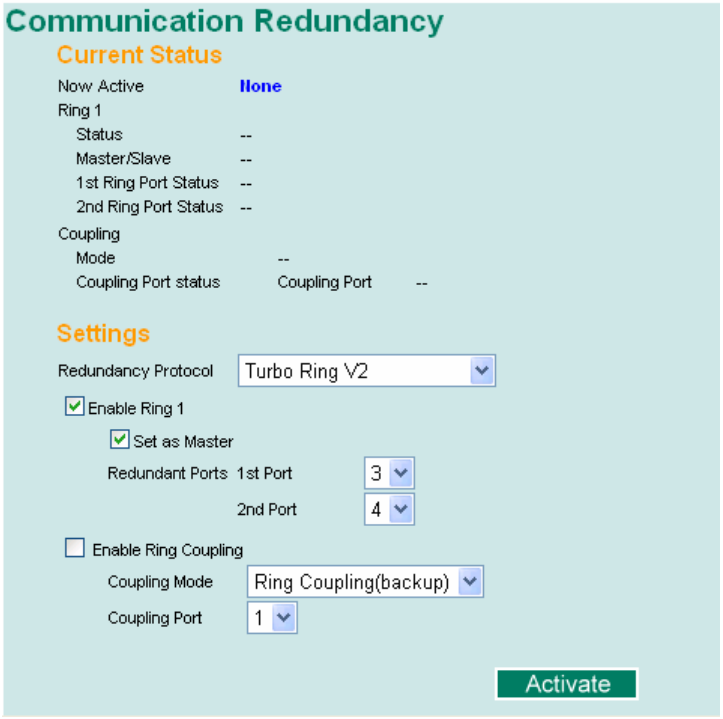
Set as Master

Setting	Description	Factory Default
Enabled	Select this EOM as Master	Not checked
Disabled	Do not select this EOM as Master	

Redundant Ports

Setting	Description	Factory Default
1st Port	Select any port of the EOM to be one of the redundant ports.	EOM-104 Series: port 3
2nd Port	Select any port of the EOM to be one of the redundant ports.	EOM-104 Series: port 4

Configuring "Turbo Ring V2"



Explanation of "Current Status" Items

Now Active

Shows which communication protocol is in use: **Turbo Ring**, **Turbo Ring V2**, **RSTP**, or **none**.

Ring—Status

Shows **Healthy** if the ring is operating normally, and shows **Break** if the ring's backup link is active.

Ring—Master/Slave

Indicates whether or not this EOM is the Master of the Turbo Ring. (This field appears only when selected to operate in Turbo Ring or Turbo Ring V2 mode.)

NOTE The user does not need to set the master to use Turbo Ring. If no master is set, the Turbo Ring protocol will assign master status to one of the EOM units in the ring. The master is only used to determine which segment serves as the backup path.

Ring—1st Ring Port Status

Ring—2nd Ring Port Status

The "Ports Status" indicators show ***Forwarding*** for normal transmission, ***Blocking*** if this port is connected to a backup path and the path is blocked, and ***Link down*** if there is no connection.

Coupling—Mode

Indicates either **None**, or **Ring Coupling**.

Coupling—Coupling Port status

Indicates either **Primary**, or **Backup**.

Explanation of "Settings" Items

Redundancy Protocol

Setting	Description	Factory Default
Turbo Ring	Select this item to change to the Turbo Ring configuration page.	None
Turbo Ring V2	Select this item to change to the Turbo Ring V2 configuration page.	
RSTP (IEEE 802.1W/1D)	Select this item to change to the RSTP configuration page.	
None	Ring redundancy is not active	

Enable Ring 1

Setting	Description	Factory Default
Enabled	Enable the Ring 1 settings	Not checked
Disabled	Disable the Ring 1 settings	

Set as Master

Setting	Description	Factory Default
Enabled	Select this EOM as Master	Not checked
Disabled	Do not select this EOM as Master	

Redundant Ports

Setting	Description	Factory Default
1st Port	Select any port of the EOM to be one of the redundant ports.	EOM-104 Series: port 3
2nd Port	Select any port of the EOM to be one of the redundant ports.	EOM-104 Series: port 4

Enable Ring Coupling

Setting	Description	Factory Default
Enable	Select this EOM as Coupler	Not checked
Disable	Do not select this EOM as Coupler	

The STP/RSTP Concept

Spanning Tree Protocol (STP) was designed to help reduce link failures in a network, and provide protection from loops. Networks that have a complicated architecture are prone to broadcast storms caused by unintended loops in the network. Moxa EthernetOnModule Switch's STP feature is disabled by default. To be completely effective, you must enable RSTP/STP on every EOM connected to your network.

Rapid Spanning Tree Protocol (RSTP) implements the Spanning Tree Algorithm and Protocol defined by IEEE Std 802.1w-2001. RSTP provides the following benefits:

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

RSTP provides essentially the same functionality as STP. To see how the two systems differ, see the **Differences between RSTP and STP** section in this chapter.

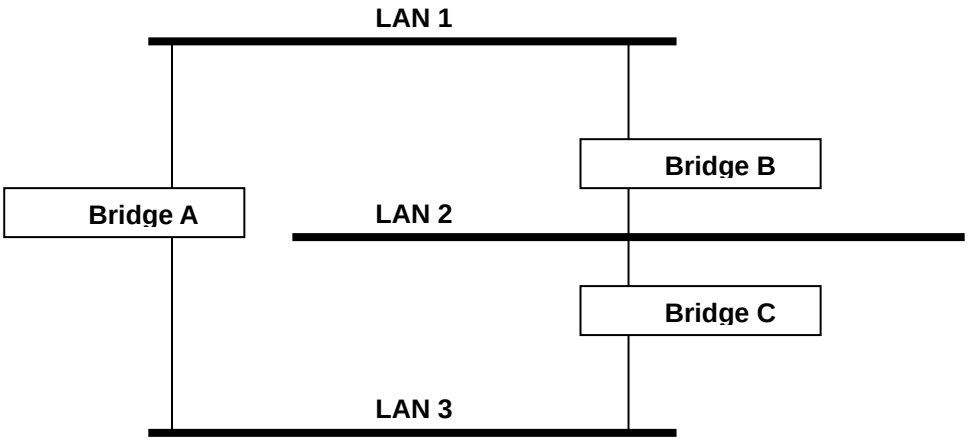
NOTE The STP protocol is part of the IEEE Std 802.1D, 1998 Edition bridge specification. The following explanation uses bridge instead of switch.

What is STP?

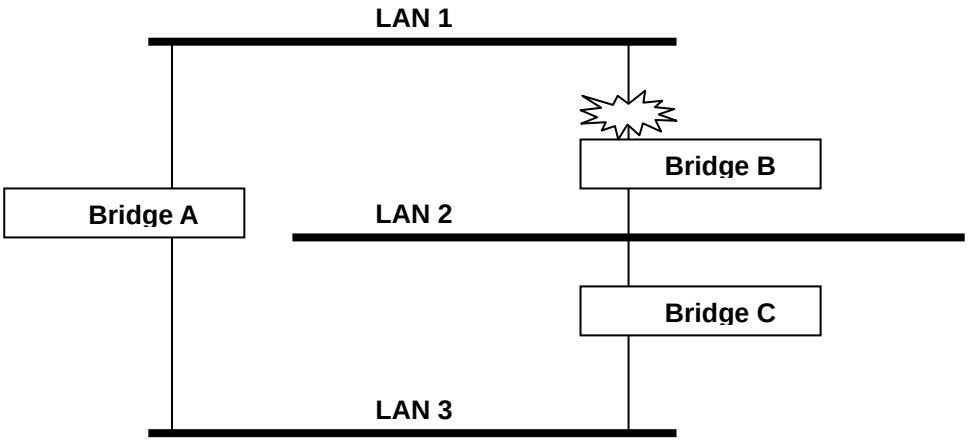
STP (802.1D) is a bridge-based system that is used to implement parallel paths for network traffic. STP uses a loop-detection process to:

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

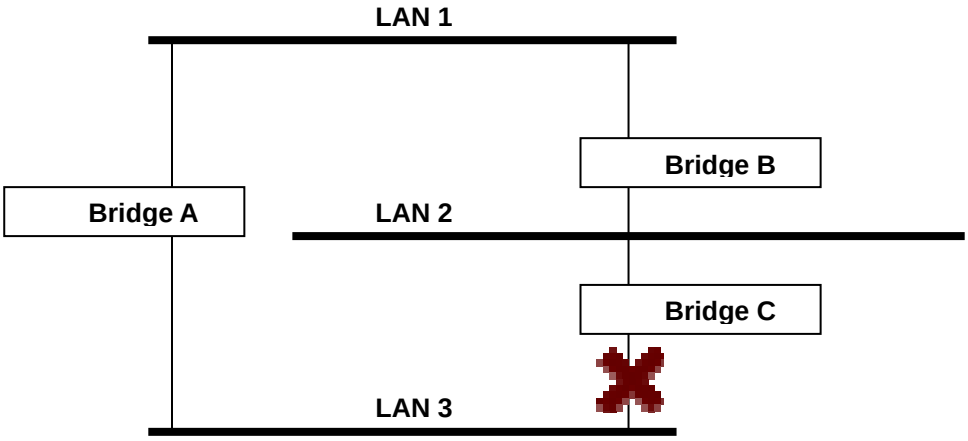
The figure below shows a network made up of three LANs separated by three bridges. Each segment uses at most two paths to communicate with the other segments. Since this configuration can give rise to loops, the network will overload if STP is NOT enabled.



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



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



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

How STP Works

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

STP Requirements

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

- Communication between all the bridges. This communication is carried out using Bridge Protocol Data Units (BPDUs), which are transmitted in packets with a known multicast address.
- Each bridge must have a Bridge Identifier that specifies which bridge acts as the central reference point, or Root Bridge, for the STP system—bridges with a lower Bridge Identifier are more likely to be designated as the Root Bridge. The Bridge Identifier is calculated using the MAC address of the bridge and a priority defined for the bridge. The default priority of EOM is 32768.
- Each port has a cost that specifies the efficiency of each link. The efficieny cost is usually determined by the bandwidth of the link, with less efficient links assigned a higher cost. The following table shows the default port costs for a switch:

Port Speed	**Path Cost 802.1D, 1998 Edition**	**Path Cost 802.1w-2001**
10 Mbps	100	2,000,000
100 Mbps	19	200,000
1000 Mbps	4	20,000

STP Calculation

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

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

STP Configuration

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

STP Reconfiguration

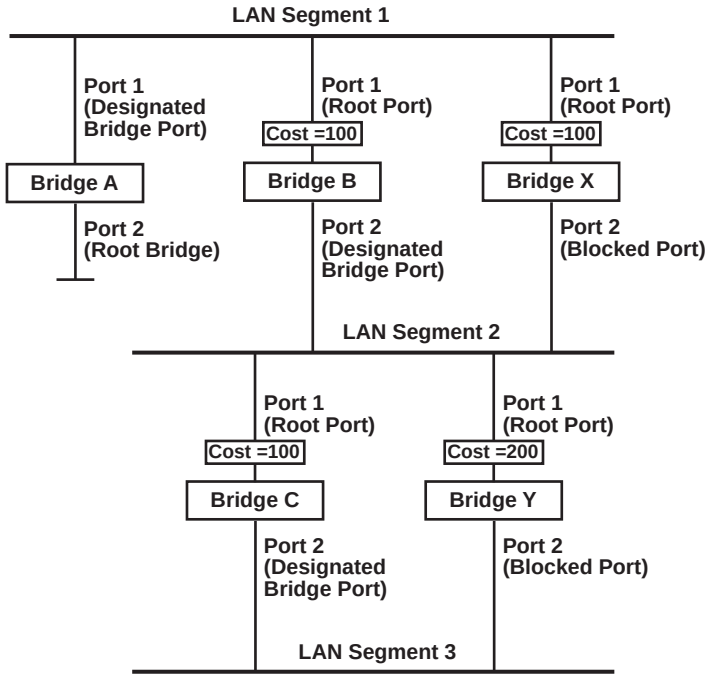
Once the network topology has stabilized, each bridge listens for Hello BPDUs transmitted from the Root Bridge at regular intervals. If a bridge does not receive a Hello BPDU after a certain interval (the Max Age time), the bridge assumes that the Root Bridge, or a link between itself and the Root Bridge,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

Differences between RSTP and STP

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

STP Example

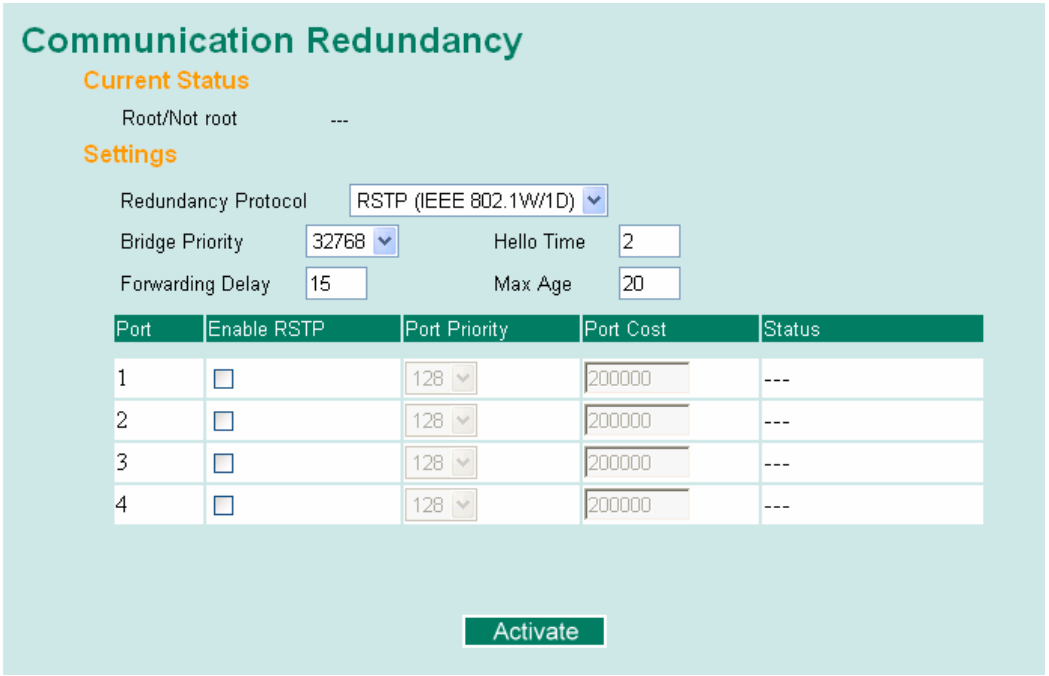
The LAN shown below has three segments, with adjacent segments connected using two possible links. The various STP factors, such as Cost, Root Port, Designated Bridge Port, and Blocked Port are shown in the figure.



- Bridge A has been selected as the Root Bridge, since it was determined to have the lowest Bridge Identifier on the network.
- Since Bridge A is the Root Bridge, it is also the Designated Bridge for LAN segment 1. Port 1 on Bridge A is selected as the Designated Bridge Port for LAN Segment 1.
- Ports 1 of Bridges B, C, X, and Y are all Root Ports since they are nearest to the Root Bridge, and therefore have the most efficient path.
- Bridges B and X offer the same Root Path Cost for LAN segment 2. However, Bridge B was selected as the Designated Bridge for that segment since it has a lower Bridge Identifier. Port 2 on Bridge B is selected as the Designated Bridge Port for LAN Segment 2.
- Bridge C is the Designated Bridge for LAN segment 3, because it has the lowest Root Path Cost for LAN Segment 3:
  - The route through Bridges C and B costs 200 (C to B=100, B to A=100)
  - The route through Bridges Y and B costs 300 (Y to B=200, B to A=100)
- The Designated Bridge Port for LAN Segment 3 is Port 2 on Bridge C.

Configuring STP/RSTP

The following figures indicate the Spanning Tree Protocol parameters that can be configured. A more detailed explanation of each parameter is given below the figure.



At the top of this page, the user can check the ***Current Status*** of this function. For RSTP, you will see:

Now Active:
This shows the communication protocol being used—Turbo Ring, RSTP, or none.

Root/Not Root
This is displayed only when RSTP is selected as the mode of operation. It indicates whether or not this EOM is the Root of the Spanning Tree (the root is determined automatically).

At the lower portion of this page, the user can configure the ***Settings*** of this function. For RSTP, you can configure:

Protocol of Redundancy

Setting	Description	Factory Default
Turbo Ring	Select this item to change to the Turbo Ring configuration page.	None
RSTP (IEEE 802.1W/1D)	Select this item to change to the RSTP configuration page.	None

Bridge priority

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

Forwarding Delay

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

Hello time (sec.)

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

Max. Age (sec.)

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

Enable STP per Port

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

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

Port Priority

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

Port Cost

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

Port Status

This indicates the current Spanning Tree status of this port. The status values are ***Forwarding*** for normal transmission, and ***Blocking*** to block transmission.

Configuration Limits of RSTP/STP

The Spanning Tree Algorithm places limits on three of the configuration items previously described:

[Eq. 1]: 1 sec ≦ Hello Time ≦ 10 sec

[Eq. 2]: 6 sec ≦ Max. Age ≦ 40 sec

[Eq. 3]: 4 sec ≦ Forwarding Delay ≦ 30 sec

These three variables are further restricted by the following two inequalities:

[Eq. 4]: 2 * (Hello Time + 1 sec) ≦ Max. Age ≦ 2 * (Forwarding Delay – 1 sec)

The EOM's firmware will alert you immediately if any of these restrictions are violated. For example, setting

Hello Time = 5 sec, Max. Age = 20 sec, and Forwarding Delay = 4 sec does not violate Eqs. 1 through 3, but does violate Eq. 4, since in this case,

2 * (Hello Time + 1 sec) = 12 sec, and 2 * (Forwarding Delay – 1 sec) = 6 sec.

You can remedy the situation in a multitude of ways. One solution is simply to increase the Forwarding Delay to at least 11 sec.

HINT: Take the following steps to avoid guessing:

Step 1: Assign a value to ***Hello Time*** and then calculate the left most part of Eq. 4 to get the lower limit of ***Max. Age***.

Step 2: Assign a value to ***Forwarding Delay*** and then calculate the right most part of Eq. 4 to get the upper limit for ***Max. Age***.

Step 3: Assign a value to ***Forwarding Delay*** that satisfies the conditions in Eq. 3 and Eq. 4.

Using Traffic Prioritization

The DS'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 EOM can inspect both IEEE 802.1p/1Q layer 2 QoS tags, and even layer 3 TOS information to provide consistent classification of the entire network. The EOM's QoS capability improves the performance and determinism of industrial networks for mission critical applications.

The Traffic Prioritization Concept

What is Traffic Prioritization?

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

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

How Traffic Prioritization Works

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

The EOM 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. This determines the level of service that type of traffic should receive. Refer to the table below for an example of how different traffic types can be mapped to the eight IEEE 802.1p priority levels.

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

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

- It requires an additional 4-byte tag in the frame, which is normally optional in 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 because you can 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.

Advantages of DiffServ over IEEE 802.1D are:

- 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 and therefore priority is preserved across the Internet.
- DSCP is backward compatible with IPV4 TOS, which allows operation with existing devices that use a layer 3 TOS enabled prioritization scheme.

Traffic Prioritization

The EOM classifies 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:

1. A packet received by the EOM 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.
2. 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 EOM will check a packet received at the ingress port for IEEE 802.1D traffic classification, and then prioritize it based upon 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

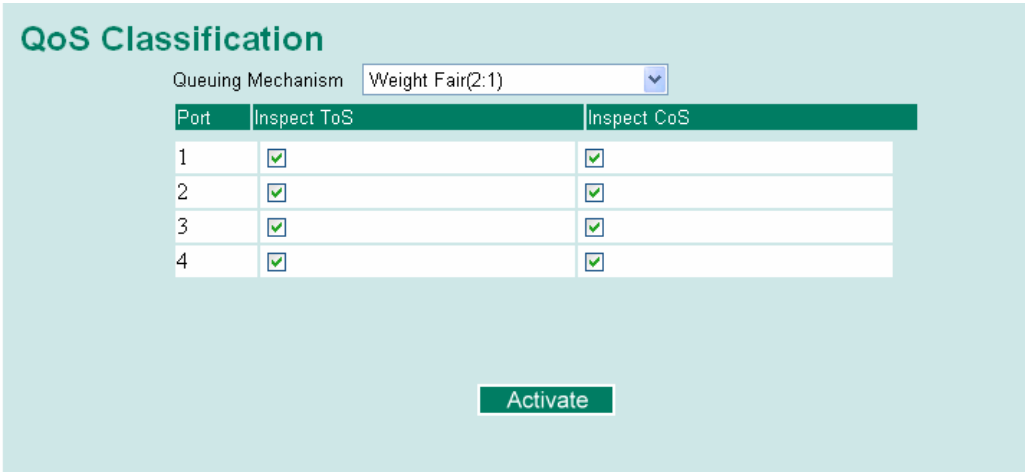
The EOM hardware has multiple traffic queues that allow packet prioritization to occur. Higher priority traffic can pass through the EOM without being delayed by lower priority traffic. As each packet arrives in the EOM, it passes through any ingress processing (which includes classification, marking/re-marking),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

The EOM supports two different queuing mechanisms:

- **Weight Fair:** This method services all the traffic queues, giving priority to the higher priority queues. Under most circumstances, this method gives high priority precedence over low-priority, but in the event that high-priority traffic exceeds 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. This method always gives precedence to high priority over low-priority.

Configuring Traffic Prioritization

QoS Classification



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

Queuing Mechanism

Setting	Description	Factory Default
Weighted Fair	The EOM-104 Series has 2 priority queues. In the weight fair scheme, an 2, 1 weighting is applied to the two priorities. This approach prevents the lower priority frames from being starved of opportunity for transmission with only a slight delay to the higher priority frames.	Weight Fair
Strict	In the Strict-priority scheme, all top-priority frames egress a port until that priority's queue is empty, and then the next lower priority queue's frames egress. This approach can cause the lower priorities to be starved of opportunity for transmitting any frames but ensures all high priority frames to egress the switch as soon as possible.	

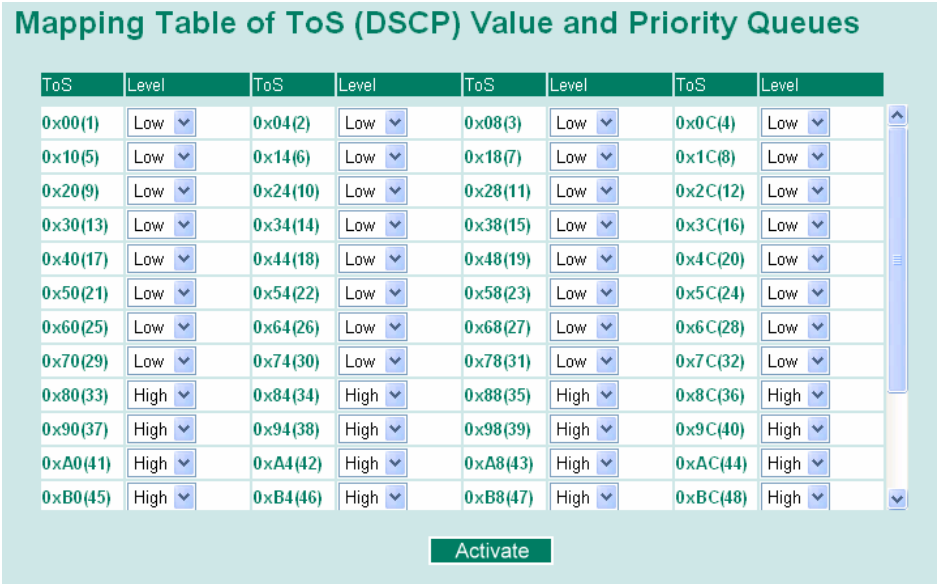
Inspect TOS

Setting	Description	Factory Default
Enable/Disable	Select this setting to enable the EOM-104 Series to inspect the Type of Service (TOS) bits in IPV4 frame to determine the priority of each frame.	Enable

Inspect COS

Setting	Description	Factory Default
Enable/Disable	Select this setting to enable the EOM-104 Series to inspect the 802.1p COS tag in the MAC frame to determine the priority of each frame.	Enable

TOS/DiffServ Mapping



Setting	Description	Factory Default
Low/High	Set the mapping table of different TOS values to 2 different egress queues.	1 to 32: Low 33 to 64: High

Using Auto Warning

Since industrial Ethernet devices are often located at remote areas 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 warning 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 EOM supports different approaches such as email and relay output to warn engineers automatically.

Configuring Email Warning

The Auto Email Warning function uses e-mail to alert the user when certain user-configured events take place.

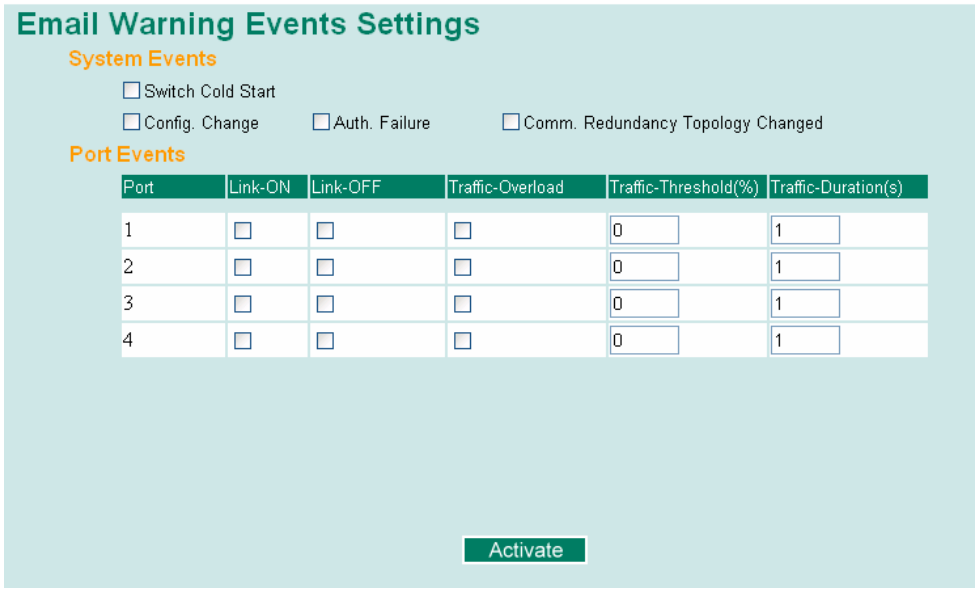
Three basic steps are required to set up the Auto Warning function:

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

2. **Configuring Email Settings**
   To configure the EOM's email setup from the Console interface or browser interface, enter your Mail Server IP/Name (IP address or name), Account Name, Account Password, Retype New Password, and the email address(es) to which warning messages will be sent.

3. **Activate your settings and test email if necessary**
   After configuring and activating your EOM's Event Types and Email Setup, you can use the **Test Email** function to see if your e-mail addresses and mail server address have been properly configured.

Email Warning Events Settings



Event Types

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

System Event	Warning e-mail is sent when…
Switch Cold Start	Power is cut off and then reconnected.
Configuration Change Activated	Any configuration item is changed.
Comm. Redundancy Topology Changed	If any Spanning Tree Protocol switches have changed their position (applies only to the root of the tree). If the Master of Turbo Ring has changed or backup path is activated.
Authentication Failure	An incorrect password is entered.

Port Event	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 setting is Enabled).
Traffic-Threshold (%)	Enter a nonzero number if the port's Traffic-Overload setting is Enabled.
Traffic-Duration (sec.)	A Traffic-Overload warning is sent every *Traffic-Duration* seconds if the average Traffic-Threshold is surpassed during that time period.

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

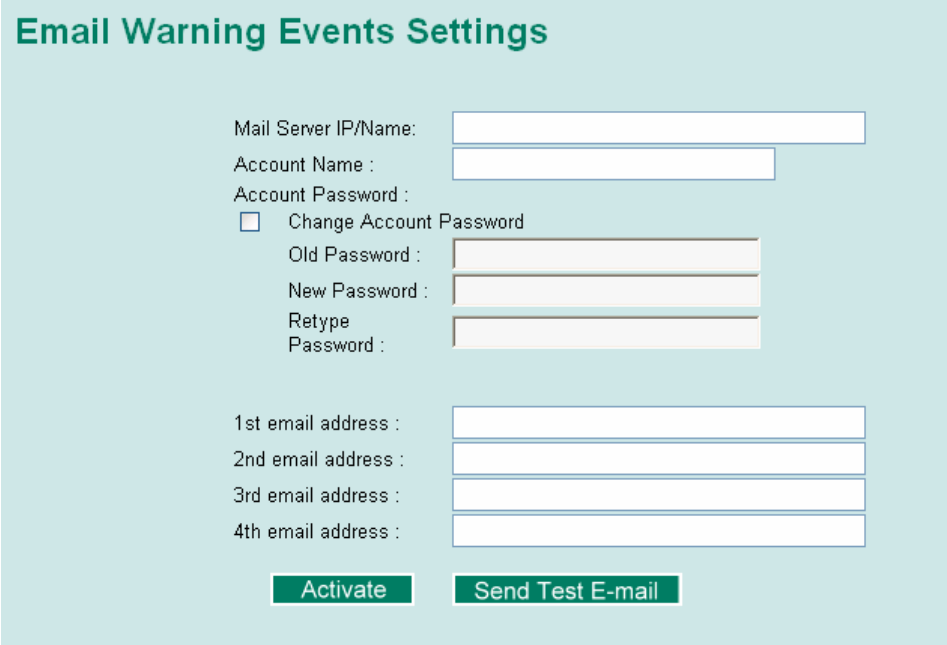
NOTE Warning e-mail messages will have the **sender** field in the form:

Moxa_EthernetOnModule_0001@Switch_Location

where **Moxa_EthernetOnModule** is the default Switch Name, **0001** is EOM's serial number, and **Switch_Location** is the default Server Location.

Refer to the Basic **Settings** section to see how to modify Switch Name and Switch Location.

Email Settings



Mail Server IP/Name

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

Account Name

Setting	Description	Factory Default
Max. 45 Charters	Your email account.	None

Password Setting

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

Email Address

Setting	Description	Factory Default
Max. 30 Characters	You can set up to 4 email addresses to receive warning emails from the EOM.	None

Send Test Email

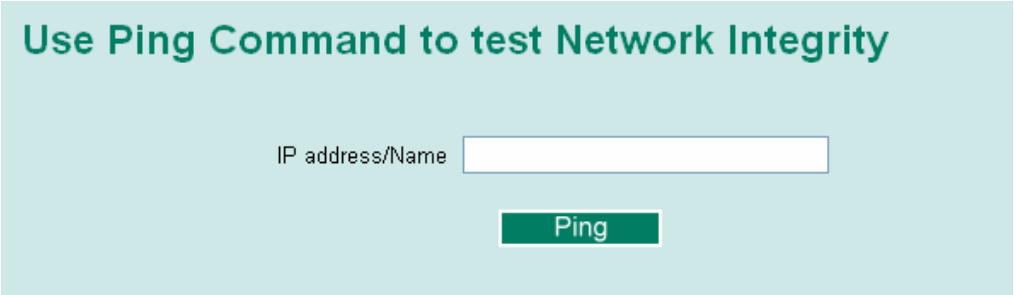
After finishing with the email settings, you should first press the ***Activate*** button to activate those settings, and then press the ***Send Test Email*** button to verify that the settings are correct.

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

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

Diagnosis

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 EOM itself. In this way, the user can essentially control the EOM and send ping commands out through its ports.

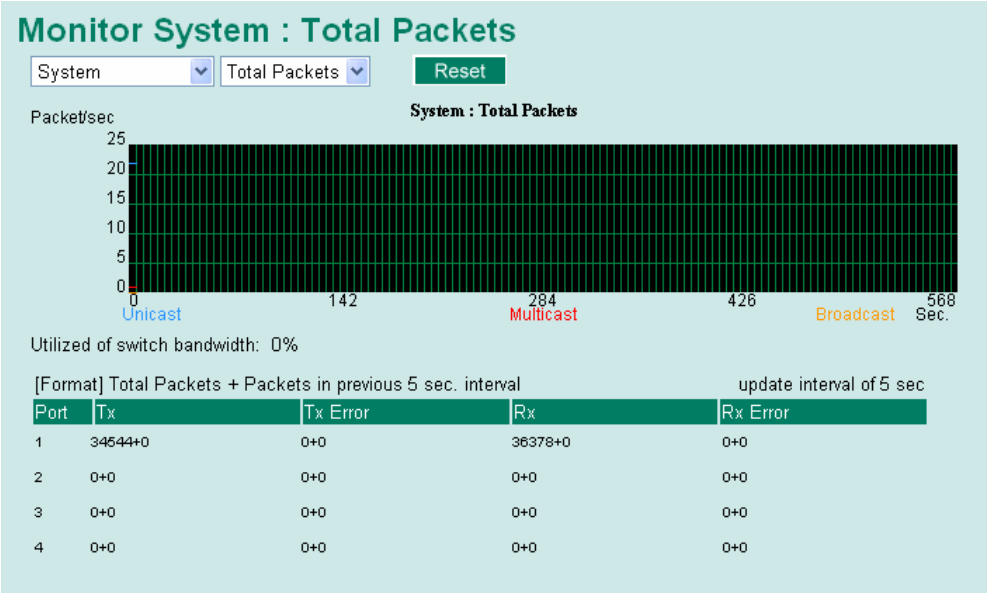
To use the Ping function, type in the desired IP address, and then press **Enter** from the Console utility, or click **Ping** when using the Web Browser interface.

Using the Monitor

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

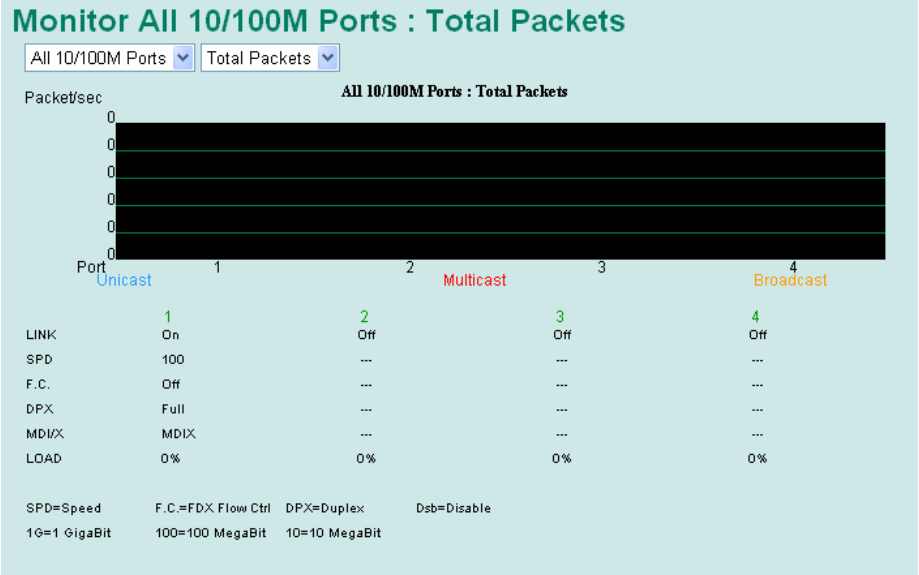
Monitor by Switch

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



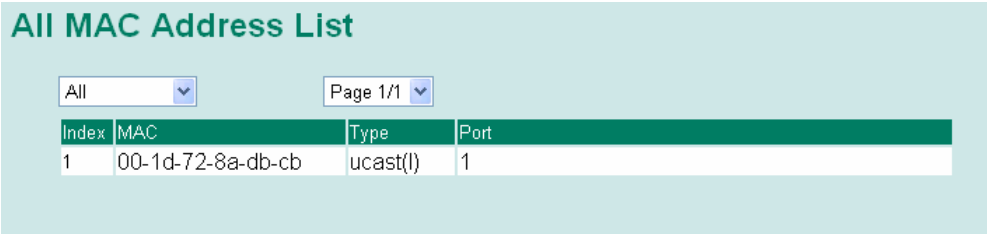
Monitor by Port

Access the Monitor by Port function by selecting **ALL 10/100M Ports** or **Port*i***, in which ***i***= 1, 2, … 8, etc., from the left pull-down list. The **Port*i*** options are identical to the Monitor by System function discussed previously, in that users can view graphs that show Total Packets, TX Packets, RX Packets, or Error Packets activity, but in this case, only for an individual port. The **All 10/100M Ports** option is essentially a graphical display of the individual port activity that can be viewed with the Console Monitor function discussed above. The All 10/100M Ports option shows three vertical bars for each port. The height of the bar represents **Packets/s** for the type of packet, at the instant the bar is being viewed. That is, as time progresses, the height of the bar moves up or down so that the user can view the change in the rate of packet transmission. The red colored bar shows **Uni-cast** packets, the green colored bar shows **Multi-cast** packets, and the blue colored bar shows **Broad-cast** packets. The graph is updated every few seconds, allowing the user to analyze data transmission activity in real-time.



Using the MAC Address Table

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



The MAC Address table can be configured to display the following EOM MAC address groups.

ALL	Select this item to show all EOM MAC addresses
ALL Learned	Select this item to show all EOM Learned MAC addresses
ALL Static	Select this item to show all EOM Static/Static Lock /Static Multicast MAC addresses
ALL Multicast	Select this item to show all EOM Multicast MAC addresses
Port x	Select this item to show all MAC addresses of dedicated ports

The table will display the following information:

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

Using Event Log

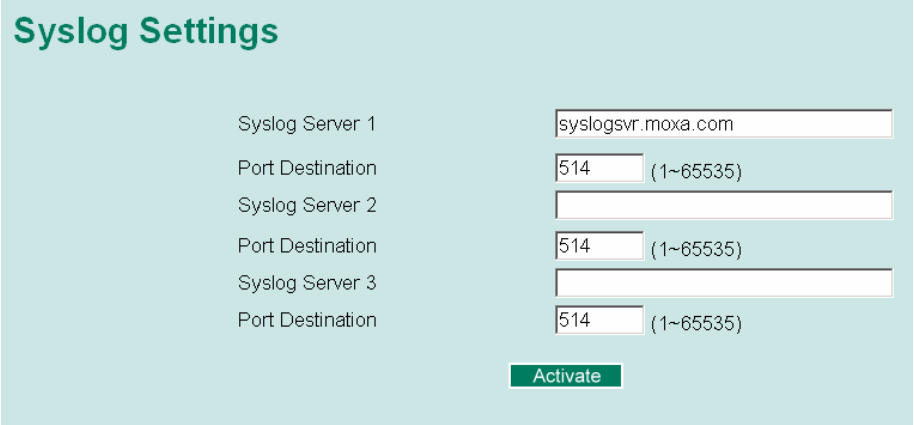
Bootup	This field shows how many times the EOM has been rebooted or cold started.
Date	The date is updated based on how the current date is set in the "Basic Setting" page.
Time	The time is updated based on how the current time is set in the "Basic Setting" page.
System Startup Time	The system startup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

Events are logged in the EOM Event Log when the following events occur:

1. Cold start
2. Configuration Change Activated
3. Authentication Fail
4. Topology Changed
5. Master Setting is Mismatched
6. Port Traffic Overload
7. Port Link from OFF to ON or from ON to OFF

Using Syslog

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



Syslog Server 1

Setting	Description	Factory Default
IP Address	Enter the IP address of 1st Syslog Server used by your network.	None
Port Destination (1 to 65535)	Enter the UDP port of 1st Syslog Server.	514

Syslog Server 2

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

Syslog Server 3

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

NOTE The following events will be recorded into the EOM Event Log table, and will then be sent to the specified Syslog Server:

1. Cold start
2. Configuration change activated
3. Authentication fail
4. Topology changed
5. Master setting is mismatched
6. Port traffic overload
7. Port link off / on

4

EDS Configurator GUI

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

This chapter includes the following sections:

- **Starting EDS Configurator**
- **Broadcast Search**
- **Search by IP address**
- **Upgrade Firmware**
- **Modify IP Address**
- **Export Configuration**
- **Import Configuration**
- **Unlock Server**

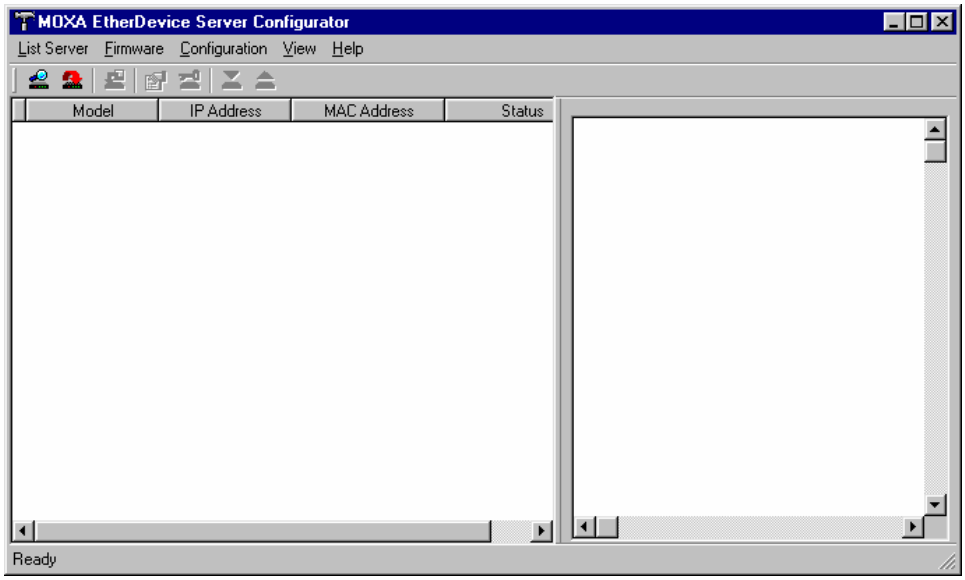
Starting EDS Configurator

To start EDS Configurator, locate and then run the executable file **edscfgui.exe**.

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

For example, if the file was placed on the Windows desktop, it should appear as follows. Double click the icon to run the program.

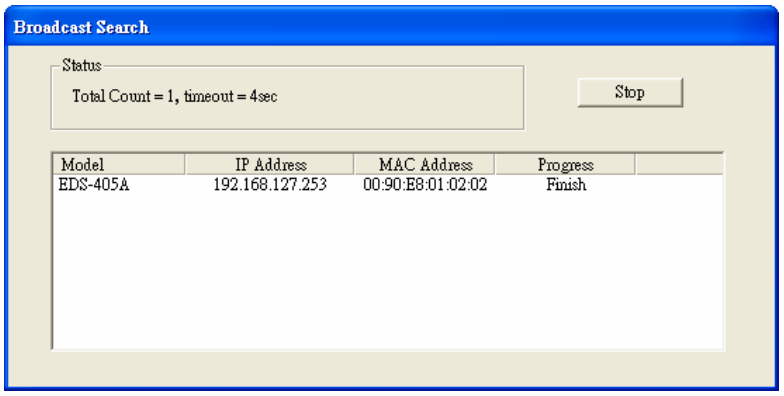
The Moxa EtherDevice Server Configurator window will open, as shown.



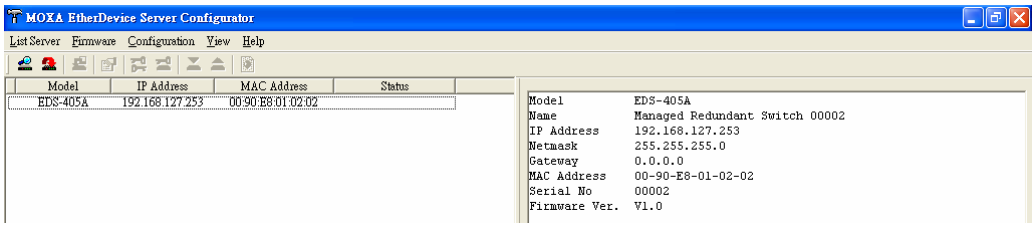
Broadcast Search

Use the Broadcast Search utility to search the LAN for all Moxa EtherDevice Switches that are connected to the LAN. Note that since the search is done by MAC address, Broadcast Search will not be able to locate EOMs connected outside the PC host's LAN. Start by clicking the Broadcast Search icon , or by selecting **Broadcast Search** from the **List Server** menu.

The Broadcast Search window will open, displaying a list of all switches located on the network, as well as the progress of the search.



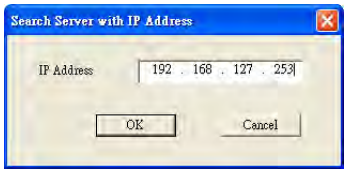
Once the search is complete, the Configurator window will display a list of all switches that were located.



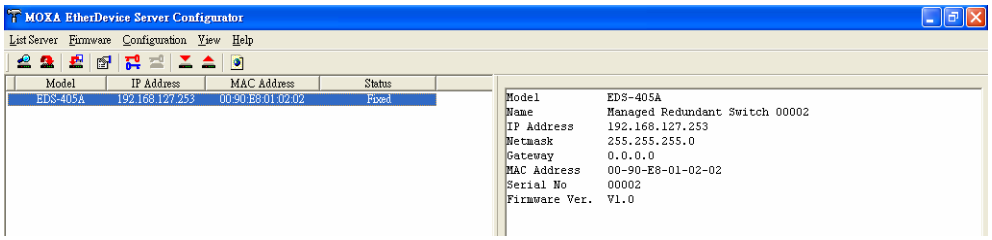
Search by IP address

This utility is used to search for EOMs one at a time. Note that the search is conducted by IP address, so you should be able to locate any EOM that is properly connected to your LAN, WAN, or even the Internet. Start by clicking the Specify by IP address icon, or by selecting **Specify IP address** from the **List Server** menu.

The **Search Server with IP Address** window will open. Enter the IP address of the switch you wish to search for, and then click **OK**.



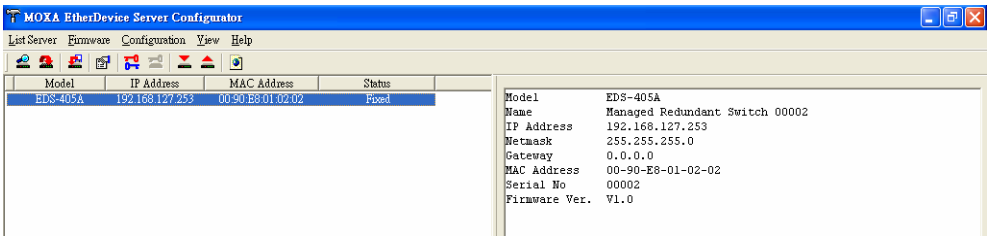
Once the search is complete, the Configurator window will add the switch to the list of switches.



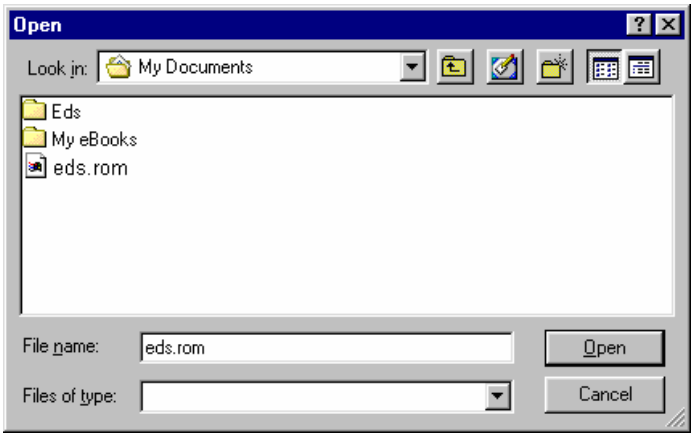
Upgrade Firmware

Keep your Moxa EtherDevice Switch up to date with the latest firmware from Moxa. Do the following to upgrade the firmware:

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



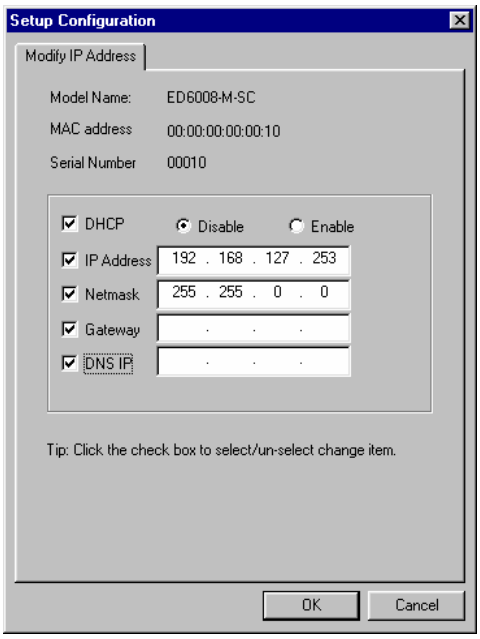
3. Click the **Upgrade Firmware** toolbar icon  , or select **Upgrade** from the **Firmware** menu. If the switch is locked, you will be prompted to input the switch's User Name and Password.
4. Click **Open** to navigate to the folder that contains the firmware upgrade file, and then click the correct "***.rom**" file (**eds.rom** in the example shown below) to select the file. Click **Open** to activate the upgrade process.



Modify IP Address

You may use the Modify IP Address function to reconfigure the EOM's network settings. Start by clicking the Modify IP address icon, or by selecting **Modify IP address** from the **Configuration** menu.

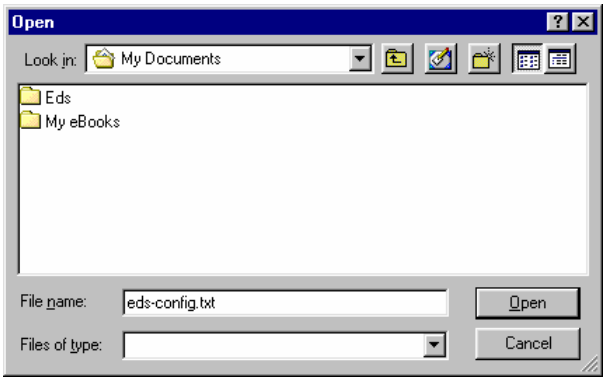
The **Setup Configuration** window will open. Select the box to the left of those items that you wish to modify, and then Disable or Enable DHCP, and enter the IP Address, Netmask, Gateway, and DNS IP. Click **OK** to accept the changes to the configuration.



Export Configuration

The **Export Configuration** utility is used to save the entire configuration of a particular EOM to a text file. Do the following to export a configuration:

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



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

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

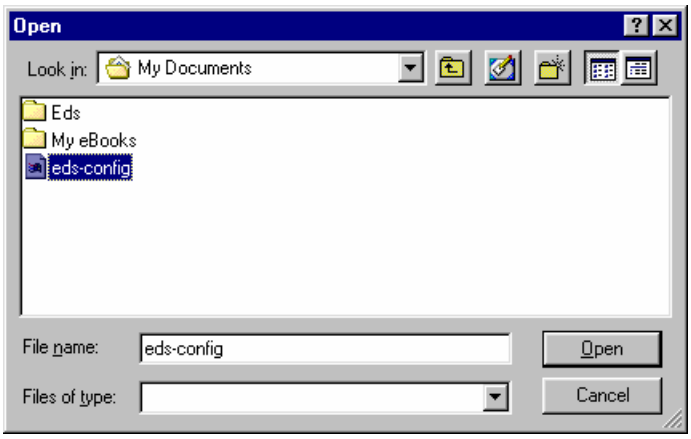
```
[EtherDevice Server Configuration File]
# Model Name
ModelName               EDS-405A

#######################################################
# System Identification                              #
#######################################################
# [SwitchName]: Switch Name
#       --> max. length = 30 words
SwitchName              Managed Redundant Switch 00002

# [Location]: Switch Location
#       --> max. length = 80 words
Location                Switch Location

# [SysDescr]: Switch Description
#       --> max. length = 30 words
SysDescr

# [Contact]: Maintainer Contact Info
#       --> max. length = 30 words
Contact

# [WebConfig]: Web Configuration
#       --> 0 : Disable Web Configuration
#       --> 1 : Enable Web Configuration
WebConfig               1
```

Import Configuration

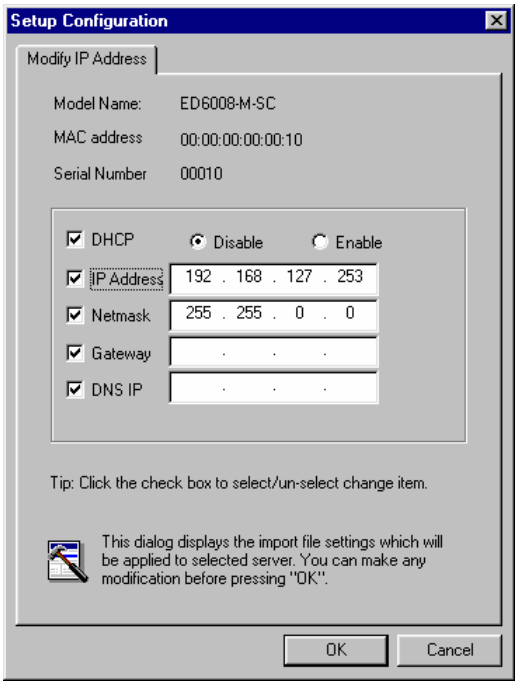
The **Import Configuration** function is used to import an entire configuration from a text file to the EOM. This utility can be used to transfer the configuration from one EOM to another, by first using the Export Configuration function (described in the previous section) to save a switch configuration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

1. Highlight the server (from the Moxa EtherDevice Switch list in the Configurator window's left pane), and then click the **Import** toolbar icon , or select **Import Configuration** from the **Configuration** menu.

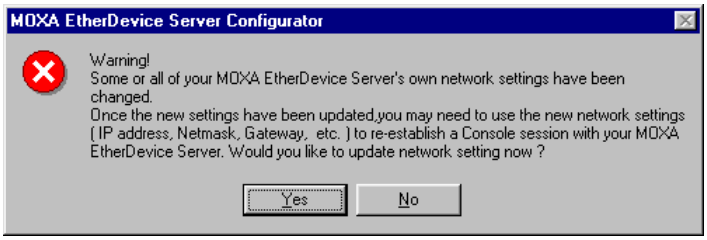
2. Click **Open** to navigate to the text file that contains the desired configuration. Once the file is selected, click **Open** again to initiate the import procedure.



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



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



Unlock Server

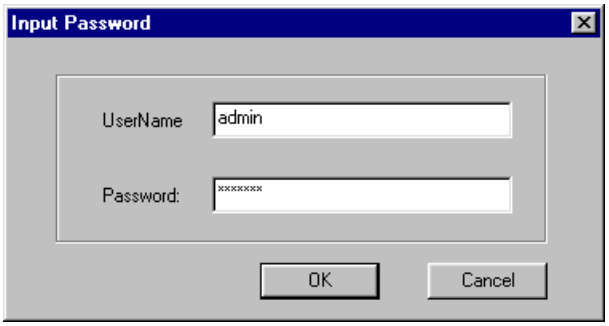
The Unlock Server function is used to open a password protected switch so that the user can modify its configuration, import/export a configuration, etc. There are six possible responses under the **Status** column. The **Status** of a Moxa Ethernet-On-Module Switch indicates how the switch was located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

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

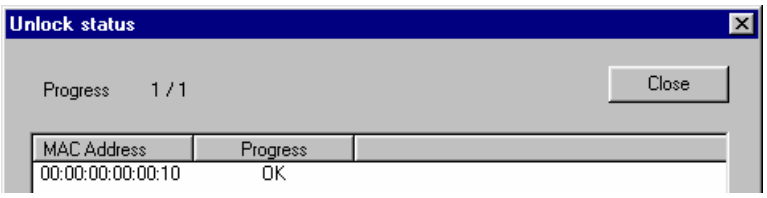
- **Locked**
  The switch is password protected, ***Broadcast Search*** was used to locate it, and the password has not yet been entered from within the current Configurator session.
- **Unlocked**
  The switch is password protected, ***Broadcast Search*** was used to locate it, and the password has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

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

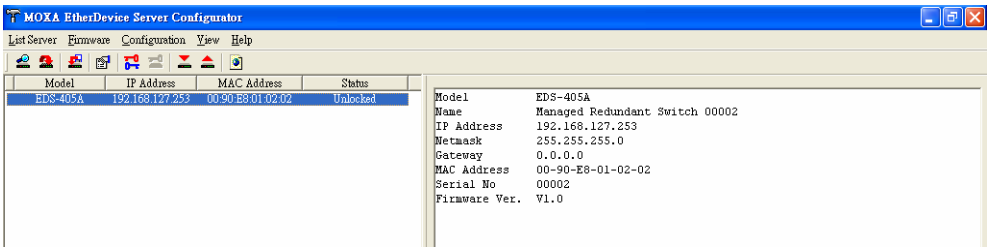
1. Enter the switch's **User Name** and **Password** when prompted, and then click **OK**.



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



3. The status of the switch will now read **Unlocked**.



A

MIB Groups

Moxa Ethernet-On-Module Switches come 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 EOM-104 Series support are:

MIB II.1 – System Group

MIB II.2 – Interfaces Group

MIB II.4 – IP Group

MIB II.5 – ICMP Group

MIB II.6 – TCP Group

MIB II.7 – UDP Group

MIB II.10 – Transmission Group

MIB II.11 – SNMP Group

MIB II.16 – RMON

MIB II.17 – Dot1dBridge Group

MIB II.17.2 – RSTP-MIB Group

MIB II.17.6 – pBridge Group

The EOM-104 Series also provides a private MIB file, where EOM-104's MIB is located at **MOXA-EOM104-MIB.my**, and EOM-104-FO's MIB is located at **MOXA-EOM104-FO-MIB.my.**

B

Specifications

Technology	
Standards	IEEE 802.3 for 10BaseT
	IEEE 802.3u for 100BaseT(X) and 100BaseFX
	IEEE 802.3x for flow control
	IEEE 802.1D for Spanning Tree Protocol
	IEEE 802.1w for Rapid STP
	IEEE 802.1p for Class of service
Protocols	SNMPv1/v2c/v3, DHCP Client, BootP, TFTP, SMTP, RARP, RMON, HTTP, Telnet, Syslog
MIB	MIB-II, Ethernet-Like MIB, P-Bridge MIB, Bridge MIB, RSTP MIB, RMON MIB Group 1, 2, 3, 9
Interface	
Ethernet Ports	EOM-104: 4 10/100BaseT(X)
	EOM-104-FO: 2 10/100BaseT(X) and 2 100BaseFX
Connectors	1 connector with 2 x 20 pins and 2 connectors with 1 x 9 pins
Console Port	RS-232 (TxD, RxD, DTR, DSR)
GPIO	4 programmable I/O pins
Power Requirements	
Input Voltage	3.3V
Input Current	EOM-104: 0.59 A @ 3.3 V
	EOM-104-FO: 1.22 A @ 3.3 V
Physical Characteristics	
Dimensions	54 x 60 x 8.25 mm (2.13 x 2.36 x 0.32 in)
Environmental Limits	
Operating Temperature	-40 to 75°C (-40 to 167°F)
Storage Temperature	-40 to 85°C (-40 to 185°F)
Ambient Relative Humidity	5 to 95% (non-condensing)
Regulatory Approvals	
EMI	FCC Part 15, CISPR (EN55022) class A, CE class A
Note: Please check Moxa's website for the most up-to-date certification status.	
WARRANTY	5 years
	Details: See www.moxa.com/warranty