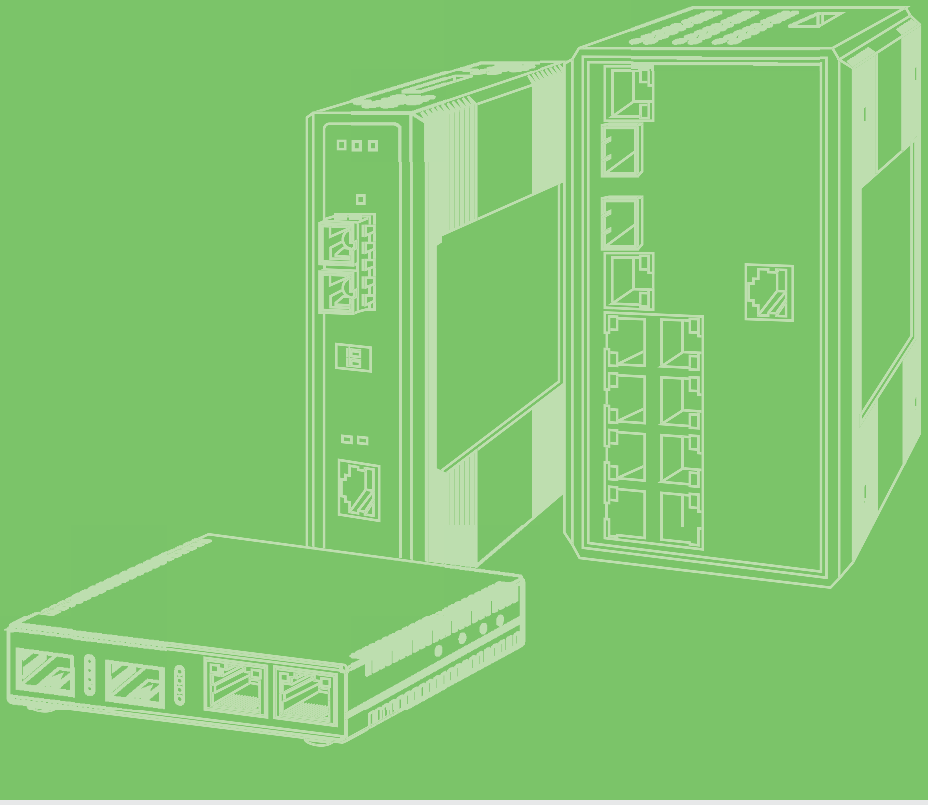


User Manual

IMC-574I-SFP

10/100/1000 Mbps 2TX/2SFP Intelligent Media Converter

ADVANTECH

Enabling an Intelligent Planet

Copyright

Acknowledgements

Intel and Pentium are trademarks of Intel Corporation.

Microsoft Windows and MS-DOS are registered trademarks of Microsoft Corp.

All other product names or trademarks are properties of their respective owners.

Product Warranty (2 years)

Advantech warrants to you, the original purchaser, that each of its products will be free from defects in materials and workmanship for two years from the date of purchase.

This warranty does not apply to any products which have been repaired or altered by persons other than repair personnel authorized by Advantech, or which have been subject to misuse, abuse, accident or improper installation. Advantech assumes no liability under the terms of this warranty as a consequence of such events.

Because of Advantech's high quality-control standards and rigorous testing, most of our customers never need to use our repair service. If an Advantech product is defective, it will be repaired or replaced at no charge during the warranty period. For out of-warranty repairs, you will be billed according to the cost of replacement materials, service time and freight. Please consult your dealer for more details.

If you think you have a defective product, follow these steps:

1. Collect all the information about the problem encountered. (For example, CPU speed, Advantech products used, other hardware and software used, etc.) Note anything abnormal and list any on screen messages you get when the problem occurs.
2. Call your dealer and describe the problem. Please have your manual, product, and any helpful information readily available.
3. If your product is diagnosed as defective, obtain an RMA (return merchandize authorization) number from your dealer. This allows us to process your return more quickly.
4. Carefully pack the defective product, a fully-completed Repair and Replacement Order Card and a photocopy proof of purchase date (such as your sales receipt) in a shippable container. A product returned without proof of the purchase date is not eligible for warranty service.
5. Write the RMA number visibly on the outside of the package and ship it prepaid to your dealer.

Edition 1

Printed in Taiwan January 2022

Declaration of Conformity

CE

This product has passed the CE test for environmental specifications. Test conditions for passing included the equipment being operated within an industrial enclosure. In order to protect the product from being damaged by ESD (Electrostatic Discharge) and EMI leakage, we strongly recommend the use of CE-compliant industrial enclosure products.

FCC Class A

Note: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

Technical Support and Assistance

1. Visit the Advantech web site at www.advantech.com/support where you can find the latest information about the product.
2. Contact your distributor, sales representative, or Advantech's customer service center for technical support if you need additional assistance. Please have the following information ready before you call:
   - Product name and serial number
   - Description of your peripheral attachments
   - Description of your software (operating system, version, application software, etc.)
   - A complete description of the problem
   - The exact wording of any error messages

Warnings, Cautions and Notes

Warning! *Important safety instructions save these instructions - this manual contains important safety instructions.*

Caution! *For use in a controlled environment. Refer to manual for environmental conditions.*

Note! *Notes provide optional additional information.*

Document Feedback

To assist us in making improvements to this manual, we would welcome comments and constructive criticism. Please send all such - in writing to: ICG.Support@advantech.com

Packing List

Before setting up the system, check that the items listed below are included and in good condition. If any item does not accord with the table, please contact your dealer immediately.

- 1 x IMC-574I-SFP device
- 1 x Universal power adapter with US/EU/UK/AU/JP plugs (optional)
- 1 x M cable D-SUB 9P/JACK
- 1 x Startup manual

Safety Instructions

- Read these safety instructions carefully.
- Keep this User Manual for later reference.
- Disconnect this equipment from any DC outlet before cleaning. Use a damp cloth. Do not use liquid or spray detergents for cleaning.
- For plug-in equipment, the power outlet socket must be located near the equipment and must be easily accessible.
- Keep this equipment away from humidity.
- Put this equipment on a reliable surface during installation. Dropping it or letting it fall may cause damage.
- The openings on the enclosure are for air convection. Protect the equipment from overheating. DO NOT COVER THE OPENINGS.
- Make sure the voltage of the power source is correct before connecting the equipment to the power outlet.
- Position the power cord so that people cannot step on it. Do not place anything over the power cord.
- All cautions and warnings on the equipment should be noted.
- If the equipment is not used for a long time, disconnect it from the power source to avoid damage by transient overvoltage.
- Never pour any liquid into an opening. This may cause fire or electrical shock.
- Never open the equipment. For safety reasons, the equipment should be opened only by qualified service personnel.
- If one of the following situations arises, get the equipment checked by service personnel:
  - The power cord or plug is damaged.
  - Liquid has penetrated into the equipment.
  - The equipment has been exposed to moisture.
  - The equipment does not work well, or you cannot get it to work according to the user's manual.
  - The equipment has been dropped and damaged.
  - The equipment has obvious signs of breakage.
- DO NOT LEAVE THIS EQUIPMENT IN AN ENVIRONMENT WHERE THE STORAGE TEMPERATURE MAY GO -40°C (-40°F) ~ 85°C (185°F). THIS COULD DAMAGE THE EQUIPMENT. THE EQUIPMENT SHOULD BE IN A CONTROLLED ENVIRONMENT.

Wichtige Sicherheishinweise

- Bitte lesen sie Sich diese Hinweise sorgfältig durch.
- Heben Sie diese Anleitung für den späteren Gebrauch auf.
- Vor jedem Reinigen ist das Gerät vom Stromnetz zu trennen. Verwenden Sie Keine Flüssig-oder Aerosolreiniger. Am besten dient ein angefeuchtetes Tuch zur Reinigung.
- Die NetzanschluBsteckdose soll nahe dem Gerät angebracht und leicht zugänglich sein.
- Das Gerät ist vor Feuchtigkeit zu schützen.
- Bei der Aufstellung des Gerätes ist auf sicheren Stand zu achten. Ein Kippen oder Fallen könnte Verletzungen hervorrufen.
- Die Belüftungsöffnungen dienen zur Luftzirkulation die das Gerät vor überhitzung schützt. Sorgen Sie dafür, daB diese Öffnungen nicht abgedeckt werden.
- Beachten Sie beim. AnschluB an das Stromnetz die AnschluBwerte.
- Verlegen Sie die NetzanschluBleitung so, daB niemand darüber fallen kann. Es sollte auch nichts auf der Leitung abgestellt werden.
- Alle Hinweise und Warnungen die sich am Geräten befinden sind zu beachten.
- Wird das Gerät über einen längeren Zeitraum nicht benutzt, sollten Sie es vom Stromnetz trennen. Somit wird im Falle einer Überspannung eine Beschädigung vermieden.
- Durch die Lüftungsöffnungen dürfen niemals Gegenstände oder Flüssigkeiten in das Gerät gelangen. Dies könnte einen Brand bzw. elektrischen Schlag auslösen.
- Öffnen Sie niemals das Gerät. Das Gerät darf aus Gründen der elektrischen Sicherheit nur von authorisiertem Servicepersonal geöffnet werden.
- Wenn folgende Situationen auftreten ist das Gerät vom Stromnetz zu trennen und von einer qualifizierten Servicestelle zu überprüfen:
  - Netzkabel oder Netzstecker sind beschädigt.
  - Flüssigkeit ist in das Gerät eingedrungen.
  - Das Gerät war Feuchtigkeit ausgesetzt.
  - Wenn das Gerät nicht der Bedienungsanleitung entsprechend funktioniert oder Sie mit Hilfe dieser Anleitung keine Verbesserung erzielen.
  - Das Gerät ist gefallen und/oder das Gehäuse ist beschädigt.
  - Wenn das Gerät deutliche Anzeichen eines Defektes aufweist.

Safety Precaution - Static Electricity

Static electricity can cause bodily harm or damage electronic devices. To avoid damage, keep static-sensitive devices in the static-protective packaging until the installation period. The following guidelines are also recommended:

- Wear a grounded wrist or ankle strap and use gloves to prevent direct contact to the device before servicing the device. Avoid nylon gloves or work clothes, which tend to build up a charge.
- Always disconnect the power from the device before servicing it.
- Before plugging a cable into any port, discharge the voltage stored on the cable by touching the electrical contacts to the ground surface.

Contents

List of Figures

Chapter 1

Product Overview

1.1 Features and Configuration

The IMC-574I-SFP offers a full feature set including Auto Negotiation, Selective Advertising, AutoCross, VLANs, SNMP Management, Loopback testing and OAM. Unit software updates can be downloaded through TFTP or iView^2 (iConfig view).

IMC-574I-SFP features include:

- SNMP manageable
- OAM AH
  - IEEE 802.3ah Link OAM for per port monitoring (OAM AH)
- OAM AH Functions
  - Discovery
  - Link Performance Monitoring
  - Remote Loopback
  - Fault Detection
  - Link Fault
  - Dying Gasp
  - Critical Event
- OAM CFM (SERVICE-OAM)
  - IEEE 802.1ag Connectivity Fault Management (OAM CFM)
  - OAM CFM Functions
  - Continuity Check
  - Loopback
- Speed/duplex modes
- 802.1q VLAN; trunk or access port-based
- EtherType 88A8 as defined in 802.1ad
- Command Line Interface capable (CLI), TELNET
- Link Fault Pass Through (LFPT)
- Password assignment via CLI, Telnet or iView^2
- DIP Switch configuration for Modes
- Bandwidth Limiting

The IMC-574I-SFP can be installed as a standalone device, back to back, or as a Remote when connected to an iMcV-Giga-FiberLinX-II configured as a Host.

As a CPE device, the IE-MultiWay can behave as a Remote to an iMcV-Giga-FiberLinX-II (or –III) Host when:

1. The iMcV-Giga-FiberLinX-II (or -III):
   - Is connected via the SFP ports on the IE-MultiWay.
   - Is configured as a Host.
2. The SNMP card (if present):
   - Uses SNMP firmware version 953-00D0 or higher.
3. The IMC-574I-SFP:

   When using iView^2, the IMC-574I-SFP can be fully managed without an IP address using a secure management channel. However, an IP address can be assigned through iView^2 (iConfig view), the CLI or Telnet using the default IP address of 10.10.10.10.

1.2 Operations, Administration, Maintenance (OAM)

OAM is a general term used in network management and typically applied to a series of standard protocols for installing, monitoring, and troubleshooting Metropolitan Area Networks (MANs).

When applied to Ethernet, OAM is typically assumed to refer to the layer 2 (MAC layer), management protocols (specifically 802.3ah and 802.1ag). Layer 2 management protocols do not need higher level transport protocols to operate, OAM data is transferred in standard multicast Ethernet frames.

- 802.3ah OAM (LINK-OAM):
  A point-to-point protocol designed to verify a specific link between two directly connected devices (over copper or fiber), that support 802.3ah OAM. One device must be configured as an active OAM device; the other as passive (typically a core switch would be the active device; the end device passive). 802.3ah OAM provides link status, remote fault detection and the ability to initiate a loopback circuit.
- 802.1ag (SERVICE-OAM):
  Often referred to as Connectivity Fault Management (CFM), is an end-to-end protocol designed to verify a specific network path between two devices that may be in different geographical locations. CFM allows the network operator to administer, monitor and debug the network using continuity check (a “heart beat” message), link trace (similar to traceroot, but operating at the MAC layer) and loopback (can be likened to a layer 2 ping).

1.3 Specifications

Specifications	Description	
Interface	I/O Port	2 x RJ45 + 2 x SFP ports
Physical	Dimensions (W x H x D)	22 x 93.8 x 99.4 mm (0.86” x 3.66” x 3.86”)
	Weight	0.45 kg (1.0 lb)
LED Display	SFP LED	FLT, Link, Activity, OAM
	RJ45 LED	Link, Activity, FDX
Environment	Operating Temperature	■ AC: -10 ~ 50 °C (+14 ~ 122 °F) ■ DC: -40 ~ 85 °C (-40 ~ 185 °F)
	Storage Temperature	-40 ~ 85°C (-40 ~ 185°F)
	Ambient Relative Humidity	10 ~ 95% (non-condensing)
Power	Power Input	■ AC: 100-240 V_{AC}, 50-60 Hz, 0.48A ■ DC: 48 V_{DC}
Certifications	Certifications	■ FCC Class A ■ UL/cUL ■ CE

1.4 Hardware Views

1.4.1 Front View

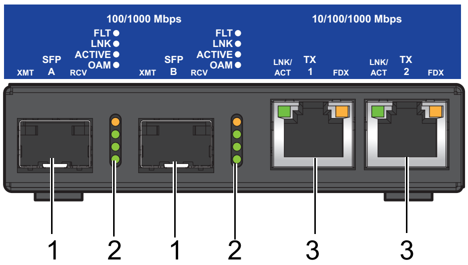


Figure 1.1 Front View

No.	Item	Description
1	ETH port	SFP x 2
2	System LED panel	See “System LED Panel” on page 4 for further details.
3	ETH port	RJ45 x 2

1.4.2 Rear View

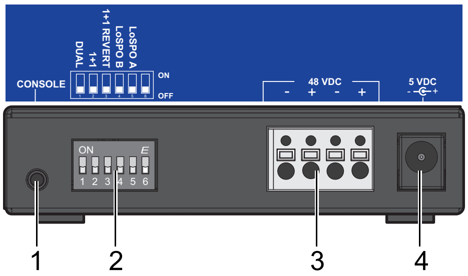


Figure 1.2 Rear View

No.	Item	Description
1	Console port	Console cable port to COM port (DB9 male) on computer to converter (3.5 mm jack).
2	DIP switch	Six-position DIP Switch. Use a small, flat-blade screwdriver (or similar device) to set the DIP switches according to requirements.
3	DC terminal block	Connect cabling for power and alarm wiring.
4	AC power in	Supports 100 ~ 240 VAC, 50 ~ 60 Hz.

1.4.2.1 System LED Panel

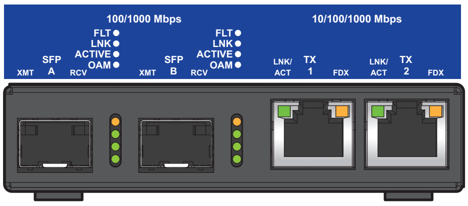


Figure 1.3 System LED Panel

LED Name	Description
SFP	
FLT	Glows amber when a fault is detected.

LED Name	Description
LNK	Glows green with a valid optical link.
ACTIVE	Glows green when the port is active. OFF when SFP is in standby (does not indicate activity).
OAM	Glows green when an active OAM AH channel is established.
RJ45	
LNK/ACT	Glows green when a link is established on the TX port; blinks green when activity is detected on the TX port.
FDX	Glows amber when an FDX link is established on the TX port. Not lit for HDX.

1.5 Dimensions

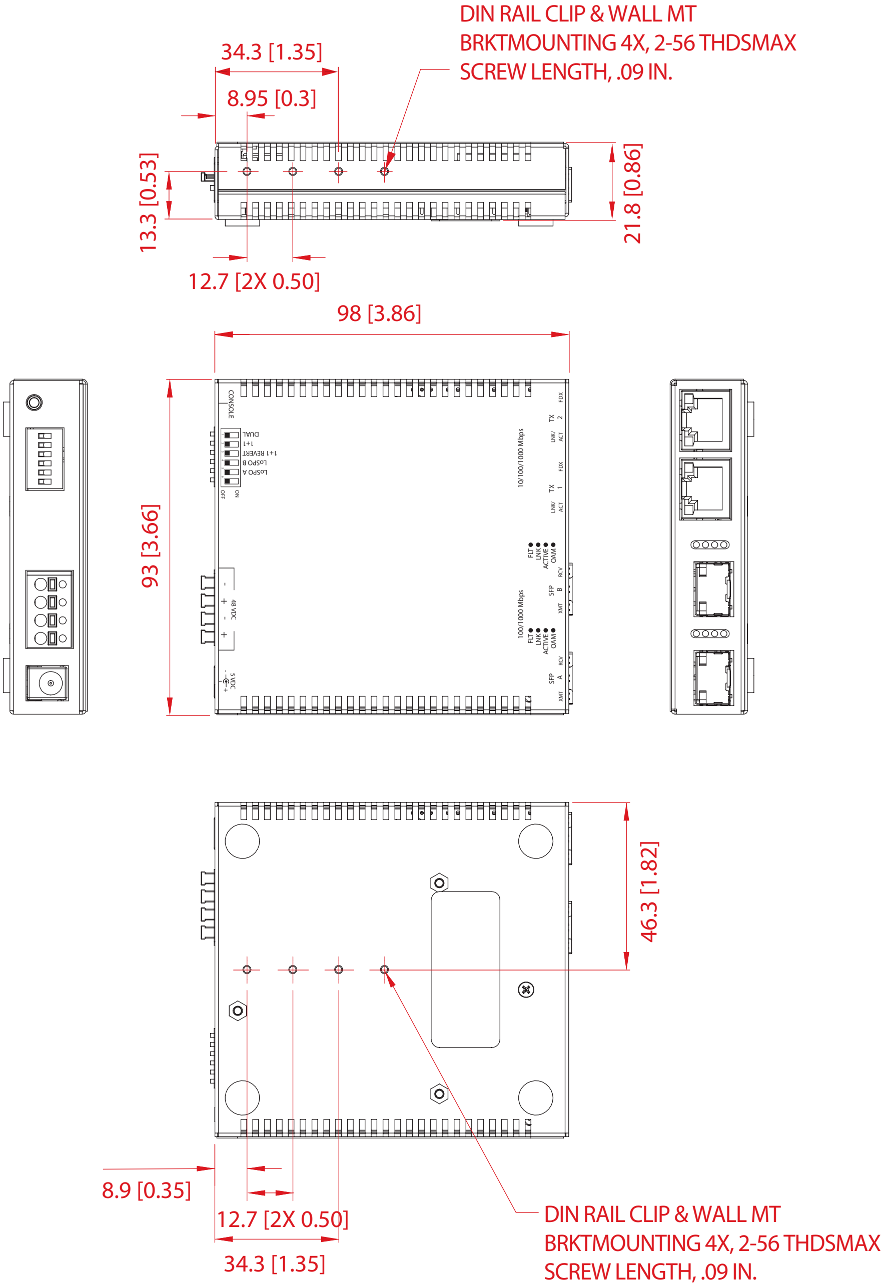


Figure 1.4 Dimensions

Chapter 2

Converter Installation

2.1 Installation Guidelines

The following guidelines are provided to optimize the device performance. Review the guidelines before installing the device.

- Make sure cabling is away from sources of electrical noise. Radios, power lines, and fluorescent lighting fixtures can interference with the device performance.
- Make sure the cabling is positioned away from equipment that can damage the cables.
- Operating environment is within the ranges listed range, see “Specifications” on page 3.
- Relative humidity around the converter does not exceed 95 percent (noncondensing).
- Altitude at the installation site is not higher than 10,000 feet.
- In 10/100 and 10/100/1000 fixed port devices, the cable length from the converter to connected devices can not exceed 100 meters (328 feet).
- Make sure airflow around the converter and respective vents is unrestricted. Without proper airflow the converter can overheat. To prevent performance degradation and damage to the converter, make sure there is clearance at the top and bottom and around the exhaust vents.

2.2 Installing the Converter

2.2.1 Wall-Mounting

The IMC-574I-SFP can mount on DIN rail or use a wall mount bracket (shown below). DIN rail clips and wall mount brackets are available for purchase from Advantech.

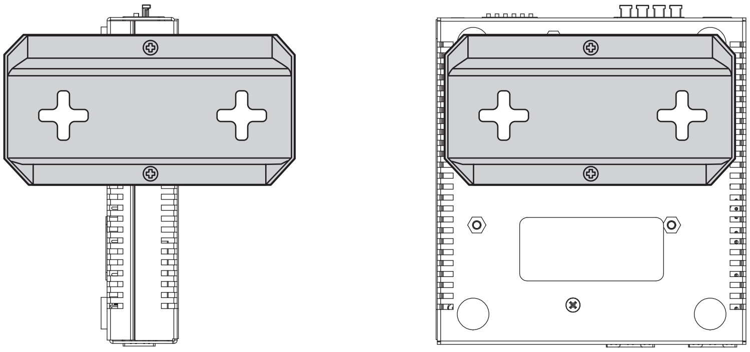


Figure 2.1 Installing Wall Mount Plates

The IMC-574I-SFP can be mounted with two DIN rail clips, (available from Advantech). The DIN rail clips include screws to allow the installation on a DIN rail. Install the screws into DIN rail clips (can be mounted parallel or perpendicular to the DIN rail). Snap the converter onto the clips. To remove the converter from the DIN rail, use a flat-head screwdriver into the slot to gently pry the converter from the rail.

Note! *DIN rail clips are designed for use on a DIN-35 rail.*

2.3 DIP Switch Configuration

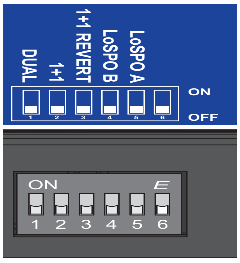


Figure 2.2 DIP Switch

No.	Name	Default	Description
1	Dual	OFF	Enable dual channel
2	1+1	OFF	Provides 1+1 protection with non-revertive switching
3	1+1 Revert	OFF	Provides 1+1 protection with revertive switching
4	LoSpd B	OFF	For future use (Optional)
5	LoSpd A	OFF	For future use (Optional)
6	Reserved	OFF	

2.3.1 DIP Switch Selectable Mode Configuration

Configuration Method	Description
4-Port Switch (Default)	In this mode, the unit acts as a standard 4-port MAC-layer switch.
Dual Converter Mode	In this mode, the unit functions as two independent (SFP to TX) media converters and traffic never passes between the two converters.
1+1 SFP Protection Non-Revertive Mode	In this mode, the "SFP A" port (fiber or copper) is connected through the switch to the drop ports as the main link. The "SFP B" port (fiber or copper) is active into the MAC switch, but no connection inside the switch is made. In this way, the "SFP B" line is held as the standby line. The "SFP B" line is held in the LINK state for testing and line verification, but does not actively carry user data. When a fault is detected on the active line, all customer traffic is switched to the "SFP B" port. With non-Revertive mode, data is not resumed by "SFP A" port until SFP B fails or is disconnected.
1+1 SFP Protection Revertive Mode	In this mode, the "SFP A" port (fiber or copper) is connected through the switch to the drop ports as the main link. The "SFP B" port (fiber or copper) is active into the MAC switch, but no connection inside the switch is made. In this way, the "SFP B" line is held as the standby line. The "SFP B" line is held in the LINK state for testing and line verification, but does not actively carry user data. When a fault is detected on the active line, all customer traffic is switched to the "SFP B" port. Once the "A" port is no longer in a fault condition, data is resumed on that port.

Note! *Revertive and Non-Revertive modes can only operate on ports with SFPs; not the fixed copper ports.*

2.4 Installing and Removing SFP Modules

IMC-574I-SFP SFP ports support Gigabit fiber SFPs and 100Mbps fiber SFPs, with or without Digital Diagnostics Monitoring Information (DDMI), as well as copper SFPs in 10/100/1000Mbps and 1000Mbps. DDMI statistics provide real-time access to transceiver operating parameters such as voltage, temperature, laser bias current, and both transmitter and receive optical power. This information can be accessed via the management system. SFPs must be MSA-compliant, (available from Advantech or other suppliers).

2.4.1 Installing SFP Modules

To connect the fiber transceiver and fiber cable, use the following guidelines:

1. Position the SFP transceiver with the handle on top, see the following figure.
2. Locate the triangular marking in the slot and align it with the bottom of the transceiver.
3. Insert the SFP transceiver into the slot until it clicks into place.
4. Make sure the module is seated correctly before sliding the module into the slot. A click sounds when it is locked in place.

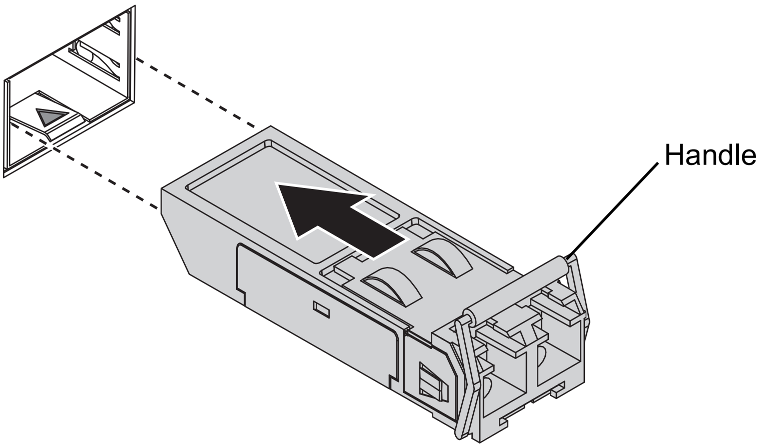


Figure 2.3 Installing an SFP Transceiver

Note! *If you are attaching fiber optic cables to the transceiver, continue with the following step. Otherwise, repeat the previous steps to install the remaining SFP transceivers in the device.*

5. Remove the protective plug from the SFP transceiver.

Note! *Do not remove the dust plug from the transceiver if you are not installing the fiber optic cable at this time. The dust plug protects hardware from dust contamination.*

6. Insert the fiber cable into the transceiver. The connector snaps into place and locks.

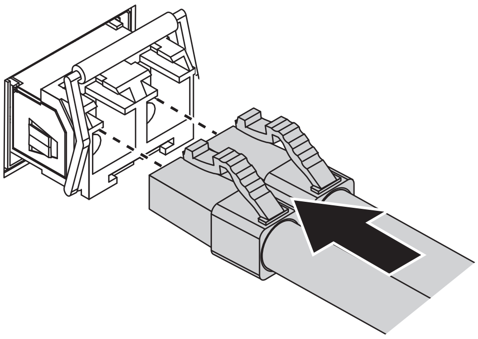


Figure 2.4 Attaching a Fiber Optic Cable to a Transceiver

7. Repeat the previous procedures to install any additional SFP transceivers in the converter.

   The fiber port is now setup.

2.4.2 Removing SFP Modules

To disconnect an fiber connector, use the following guidelines:

1. Press down and hold the locking clips on the upper side of the optic cable.
2. Pull the optic cable out to release it from the transceiver.

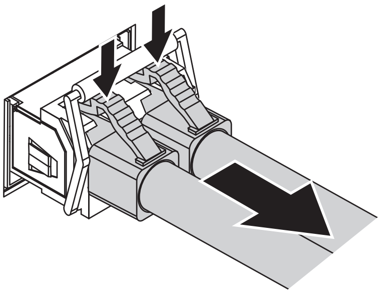


Figure 2.5 Removing a Fiber Optic Cable to a Transceiver

3. Hold the handle on the transceiver and pull the transceiver out of the slot.

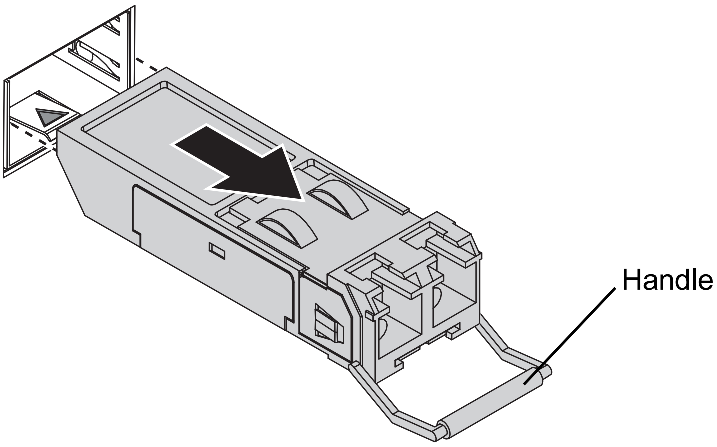


Figure 2.6 Removing an SFP Transceiver

2.5 Connecting the Converter to Ethernet Ports

2.5.1 RJ45 Ethernet Cable Wiring

The following table lists the pin configuration for the RJ45 data connector.

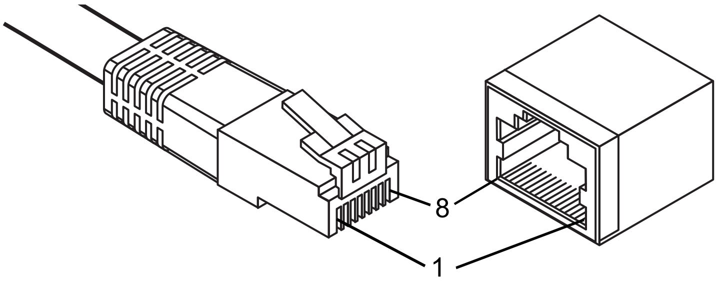


Figure 2.7 Ethernet Plug & Connector Pin Position

Pin	Signal Name 1000M	Signal Direction 10/100M
1	TXD1+	Out*
2	TXD1-	Out*
3	RXD2+	In*
4	D3+	
5	D3-	
6	RXD2-	In*
7	D4+	
8	D4-	

* The MDI/MDIX function will automatically adjust the direction of these signals to match the connected unit when running 10/100Base-T. 1000Base-T will use all 4 pairs in full duplex mode.

2.6 Connecting the Converter to Console Port

A console port, located next to the DIP Switch bay, allows the user to use of a local RS-232 serial interface for management. A mini-jack to DB9F cable is provided with the product for direct connection to a PC serial port.

Note! *To log on through the serial port, set the computer/terminal for VT-100 emulation, with: 38.4K baud, 8 data bits, 1 stop bit, no parity, no FlowControl.*

The IMC-574I-SFP includes an RS-232 mini jack for the console port allowing the end user to launch a serial session and access a list of commands. The serial port on the computer/terminal should be set for: 38.4K baud, 8 data bits, 1 stop bit, no parity, no flow control. The **F2** key functions as a **Delete** key on VT-100 emulators.

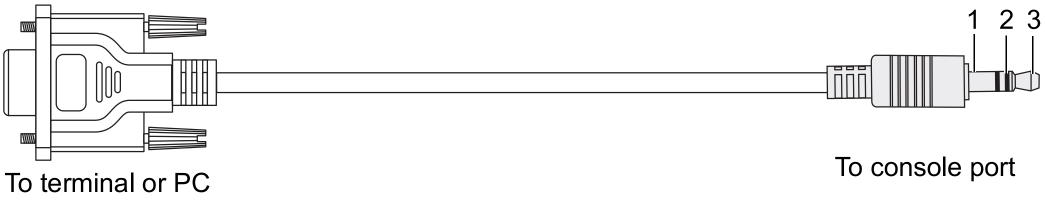


Figure 2.8 Serial Console Cable

No.	Pin	DB9-F Pin#	Signal Name	Direction
1	Tip	2	Transmit	Out of Unit
2	Ring	3	Receive	In to Unit
3	Sleeve	5	Return	Return

2.7 Power Supply Installation

The IMC-574I-SFP includes multiple powering options:

- AC adapter.
- 4-terminal DC power block.

2.7.1 AC Power In

Caution! *Disconnect the power cord before installation or cable wiring.*

Connect the AC power line with its AC connector.

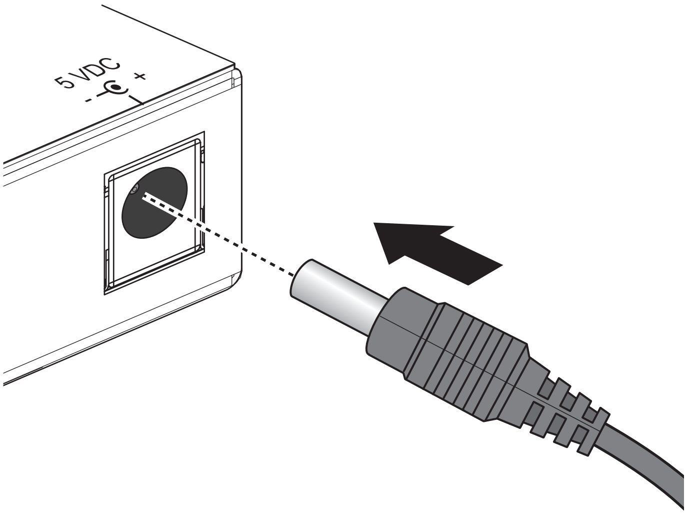


Figure 2.9 Connecting AC Power

2.7.2 DC Terminal

The IMC-574I-SFP can be powered with the DC terminal block. From a power source, connect to any one positive and any one negative terminal on the IMC-574I-SFP.

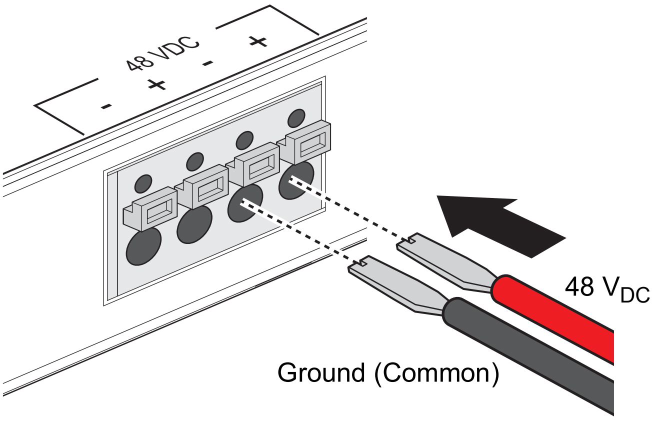


Figure 2.10 Connecting DC Power

Note! *When using stranded wire, the leads should be tinned. The DC terminal block is protected against polarity mis-wiring. AWG24 is recommended*

2.8 Autocross Feature for Twisted Pair Connections

All fixed twisted pair ports on the IMC-574I-SFP include AutoCross feature that automatically selects between a crossover workstation and a straight-through connection, depending on the connected device.

2.9 Product Application

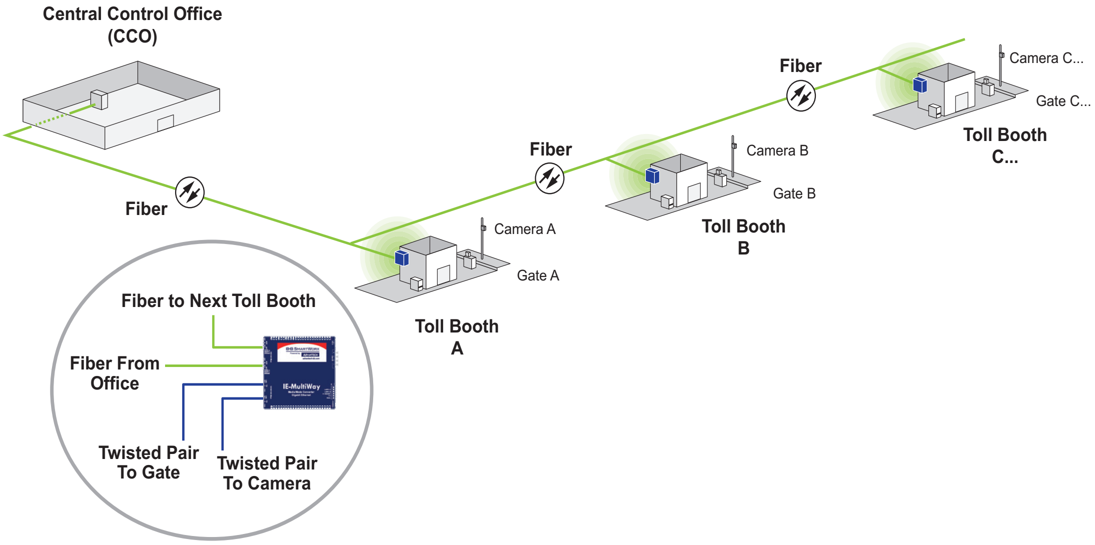


Figure 2.11 Product Application

Chapter 3

Managing Converter

3.1 Log In

To access the login window, connect the device to the network, see "Connecting the Converter to Ethernet Ports" on page 11. Once the converter is installed and connected, power on the converter see the following procedures to log into your converter.

When the converter is first installed, the default network configuration is set to DHCP enabled. You will need to make sure your network environment supports the converter setup before connecting it to the network.

1. Launch your web browser on a computer.
2. In the browser's address bar type in the converter's default IP address (10.10.10.10). The login screen displays.
3. Enter the default user name and password (admin/admin) to log into the management interface. You can change the default password after you have successfully logged in.
4. Click **Login** to enter the management interface.

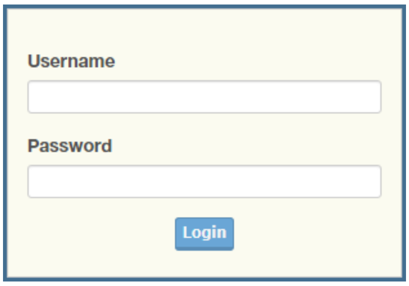


Figure 3.1 Login Screen

3.2 Recommended Practices

One of the easiest things to do to help increase the security posture of the network infrastructure is to implement a policy and standard for secure management. This practice is an easy way to maintain a healthy and secure network.

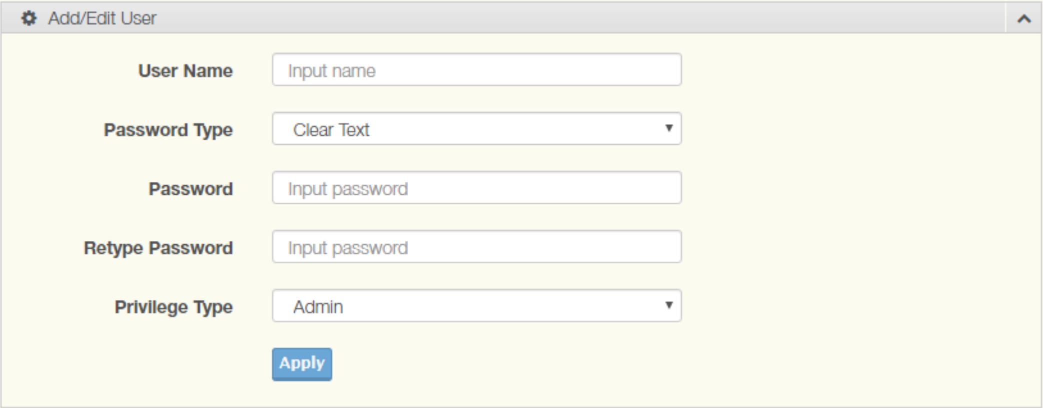
After you have performed the basic configurations on your converters, the following is a recommendation which is considered best practice policy.

3.2.1 Changing Default Password

In keeping with good management and security practices, it is recommended that you change the default password as soon as the device is functioning and setup correctly. The following details the necessary steps to change the default password.

To change the password:

1. Navigate to **Tools** > **User Account**.
2. In the **User Name** field, enter admin for this account. It is not necessary to change the user name, however, a change in the default settings increases the security settings.
3. In the **Password** field, type in the new password. Re-type the same password in the **Retype Password** field.
4. Click **Apply** to change the current account settings.



Add/Edit User

User Name	Input name
Password Type	Clear Text
Password	Input password
Retype Password	Input password
Privilege Type	Admin

Figure 3.2 Changing a Default Password

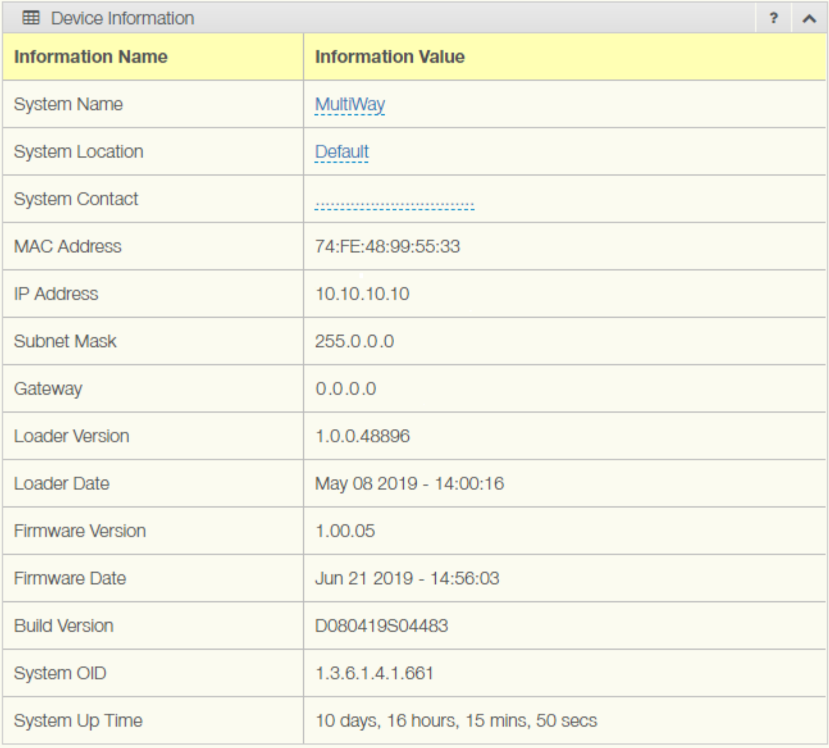
After saving all the desired settings, perform a system save (**Tools** > **Save Configuration**). The changes are saved.

3.3 Monitoring

3.3.1 Device Information

The Device Information menu lists information, such as: System Name, System Location, MAC Address, Firmware version, and more, pertaining to the system. The information is for review only. To modify the device information, see the respective item within the user interface.

To access this page, click **Monitoring** > **Device Information**.



Device Information

Information Name	Information Value
System Name	MultiWay
System Location	Default
System Contact	
MAC Address	74:FE:48:99:55:33
IP Address	10.10.10.10
Subnet Mask	255.0.0.0
Gateway	0.0.0.0
Loader Version	1.0.0.48896
Loader Date	May 08 2019 - 14:00:16
Firmware Version	1.00.05
Firmware Date	Jun 21 2019 - 14:56:03
Build Version	D080419S04483
System OID	1.3.6.1.4.1.661
System Up Time	10 days, 16 hours, 15 mins, 50 secs

Figure 3.3 Monitoring > Device Information

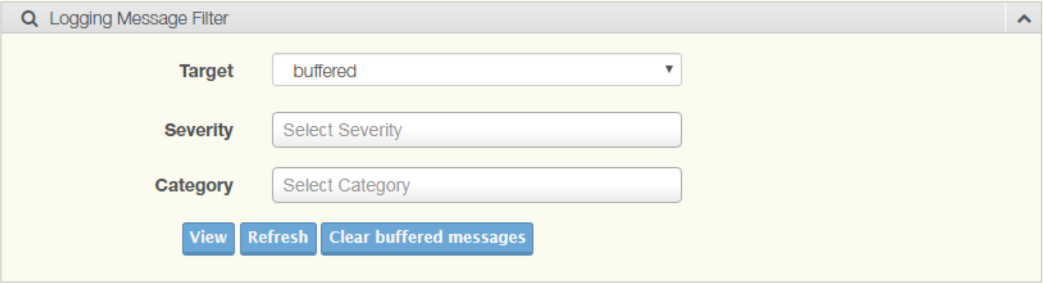
The following table describes the items in the previous figure.

Item	Description
System Name	Click **MultiWay** to enter the system name: up to 128 alphanumeric characters (default is MultiWay).
System Location	Click **Default** to enter the location: up to 256 alphanumeric characters (default is Default).
System Contact	Click the field to enter a description of the system contact profile: up to 128 alphanumeric characters.
MAC Address	Displays the MAC address of the converter.
IP Address	Displays the assigned IP address of the converter.
Subnet Mask	Displays the assigned subnet mask of the converter.
Gateway	Displays the assigned gateway of the converter.
Loader Version	Displays the current loader version of the converter.
Loader Date	Displays the current loader build date of the converter.
Firmware Version	Displays the current firmware version of the converter.
Firmware Date	Displays the current firmware build date of the converter.
Build Version	Displays the current build version of the converter.
System OID	Displays the base object ID of the converter.
System Up Time	Displays the time since the last converter reboot.

3.3.2 Logging Message

The Logging Message Filter page allows you to enable the display of logging message filter.

To access this page, click **Monitoring** > **Logging Message**.



Logging Message Filter

Target: buffered

Severity: Select Severity

Category: Select Category

Figure 3.4 Monitoring > Logging Message

The following table describes the items in the previous figure.

Item	Description
Target	Click the drop-down menu to select a target to store the log messages. ■ buffered: Store log messages in RAM. All log messages are cleared after system reboot. ■ file: Store log messages in a file.
Severity	The setting allows you to designate a severity level for the Logging Message Filter function. Click the drop-down menu to select the severity level target setting. The level options are: ■ emerg: Indicates system is unusable. It is the highest level of severity. ■ alert: Indicates action must be taken immediately. ■ crit: Indicates critical conditions. ■ error: Indicates error conditions. ■ warning: Indicates warning conditions. ■ notice: Indicates normal but significant conditions. ■ info: Indicates informational messages. ■ debug: Indicates debug-level messages.
Category	Click the drop-down menu to select the category level target setting.
View	Click **View** to display all Logging Information and Logging Message information.
Refresh	Click **Refresh** to update the screen.
Clear buffered messages	Click **Clear buffered messages** to clear the logging buffer history list.

The ensuing table for **Logging Information** table settings are informational only:

Target, Severity and Category.

The ensuing table for **Logging Message** table settings are informational only:

No., Time Stamp, Category, Severity and Message.

3.3.3 Port Monitoring

Port Network Monitor is a bandwidth and network monitoring tool for the purpose of capturing network traffic and measuring of network throughput. The monitoring functionality includes listing of port statistics as well as port utilization.

3.3.3.1 Port Statistics

To access this page, click **Monitoring** > **Port Monitoring** > **Port Statistics**.

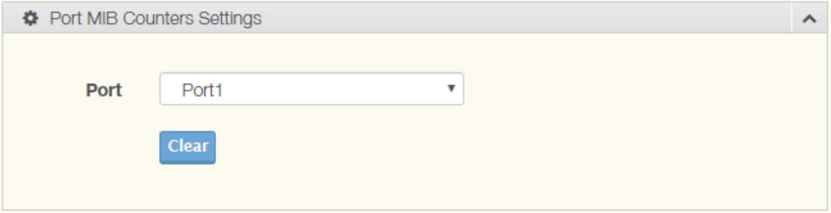


Figure 3.5 Monitoring > Port Monitoring > Port Statistics

The following table describes the items in the previous figure.

Item	Description
Port	Click the drop-down menu to select a port and its captured statistical setting values.
Clear	Click **Clear** to clear the counter selections.

The ensuing table for **IF MIB Counters** settings are informational only:

ifInOctets, ifInUcastPkts, ifInNUcastPkts, ifInDiscards, ifOutOctets, ifOutUcastPkts, ifOutNUcastPkts, ifOutDiscards, ifInMulticastPkts, ifInBroadcastPkts, ifOutMulticastPkts and ifOutBroadcastPkts.

The ensuing table for **Ether-Like MIB Counters** settings are informational only:

dot3StatsAlignmentErrors, dot3StatsFCSErrors, dot3StatsSingleCollisionFrames, dot3StatsMultipleCollisionFrames, dot3StatsDeferredTransmissions, dot3StatsLateCollisions, dot3StatsExcessiveCollisions, dot3StatsFrameTooLongs, dot3StatsSymbolErrors, dot3ControlInUnknownOpcodes, dot3InPauseFrames and dot3OutPauseFrames.

The ensuing table for **Rmon MIB Counters** settings are informational only:

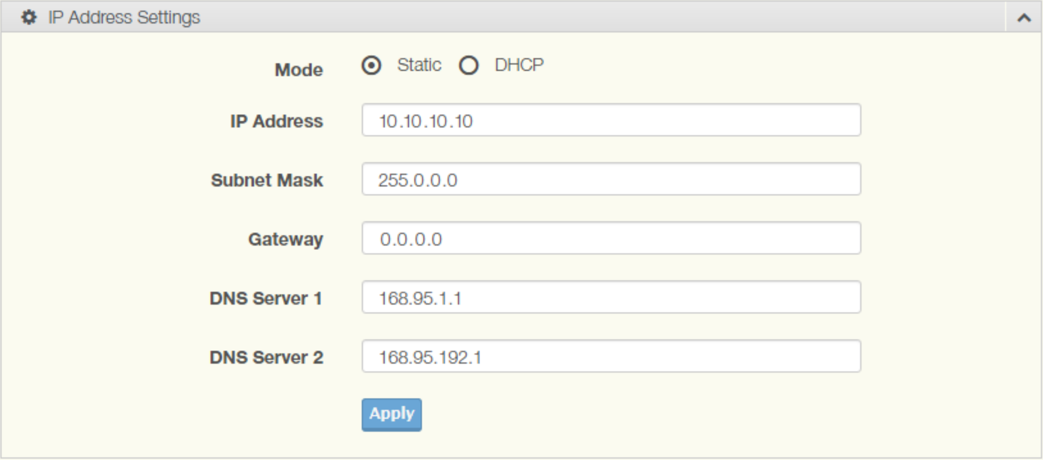
etherStatsDropEvents, etherStatsOctets, etherStatsPkts, etherStatsBroadcastPkts, etherStatsMulticastPkts, etherStatsCRCAlignErrors, etherStatsUnderSizePkts, etherStatsOverSizePkts, etherStatsFragments, etherStatsJabbers, etherStatsCollisions, etherStatsPkts64Octets, etherStatsPkts65to127Octets, etherStatsPkts128to255Octets, etherStatsPkts256to511Octets, etherStatsPkts512to1023Octets and etherStatsPkts1024to1518Octets.

3.4 System

3.4.1 IP Settings

The IP Settings menu allows you to select a static or DHCP network configuration. The Static displays the configurable settings for the static option.

To access this page, click **System** > **IP Settings**.



IP Address Settings

Mode ● Static ○ DHCP

IP Address 10.10.10.10

Subnet Mask 255.0.0.0

Gateway 0.0.0.0

DNS Server 1 168.95.1.1

DNS Server 2 168.95.192.1

Figure 3.6 System > IP Settings

The following table describes the items in the previous figure.

Item	Description
Mode	Click the radio button to select the IP Address Setting mode: Static or DHCP.
IP Address	Enter a value to specify the IP address of the interface. The default is 10.10.10.10.
Subnet Mask	Enter a value to specify the IP subnet mask for the interface. The default is 255.255.255.0.
Gateway	Enter a value to specify the default gateway for the interface. The default is 0.0.0.0.
DNS Server 1	Enter a value to specify the DNS server 1 for the interface. The default is 168.95.1.1.
DNS Server 2	Enter a value to specify the DNS server 2 for the interface. The default is 168.95.192.1.
Apply	Click **Apply** to save the values and update the screen.

The ensuing table for **IP Address Information** settings are informational only:

> DHCP State, Current IP Address, Current Subnet Mask, Current Gateway, Current DNS Server 1, Current DNS Server 2, Static IP Address, Static Subnet Mask, Static Gateway, Static DNS Server 1 and Static DNS Server 2.

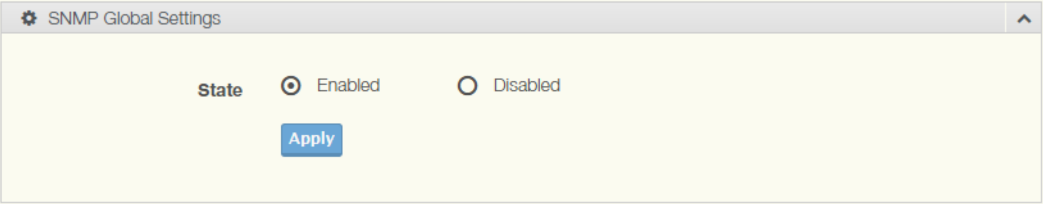
3.4.2 SNMP

Simple Network Management Protocol (SNMP) is a protocol to facilitate the monitoring and exchange of management information between network devices. Through SNMP, the health of the network or status of a particular device can be determined.

3.4.2.1 SNMP Settings

The SNMP Settings page allows you to set the SNMP daemon state (enabled or disabled).

To access this page, click **System** > **SNMP** > **SNMP Settings**.



SNMP Global Settings

State ● Enabled ○ Disabled

Figure 3.7 System > SNMP > SNMP Settings

The following table describes the items in the previous figure.

Item	Description
State	Click **Enabled** or **Disabled** to define the SNMP daemon.
Apply	Click **Apply** to save the values and update the screen.

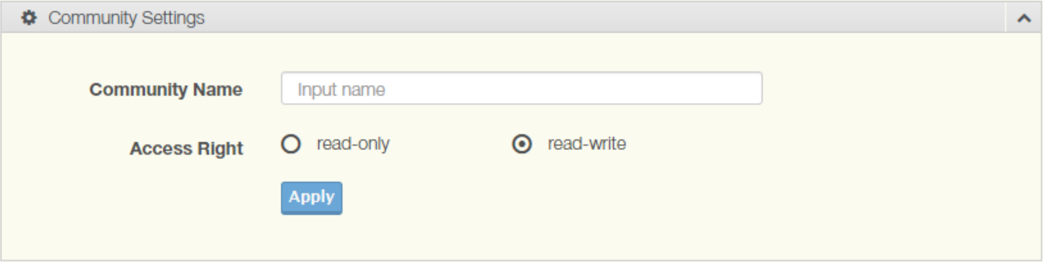
The ensuing table for **SNMP Information** settings are informational only: SNMP.

3.4.2.2 SNMP Community

The SNMP Community page provides configuration options for the community.

SNMP v1 and SNMP v2c use the group name (Community Name) certification. It's role is similar to the password function. If SNMP v1 and SNMP v2c are used, you can go directly from the configuration settings to this page to configure the SNMP community.

To access this page, click **System** > **SNMP** > **SNMP Community**.



Community Settings

Community Name: Input name

Access Right ○ read-only ● read-write

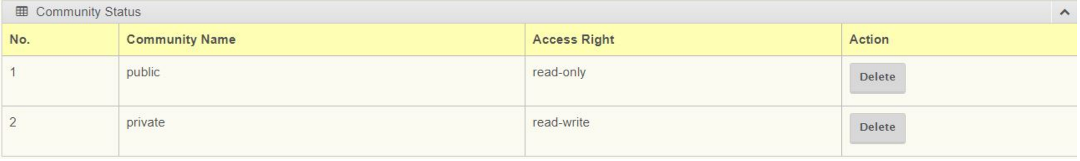
Figure 3.8 System > SNMP > SNMP Community

The following table describes the items in the previous figure.

Item	Description
Community Name	Enter a community name (up to 20 characters).
Access Right	Click the radio box to specify the access level (read only or read write).
Apply	Click **Apply** to save the values and update the screen.

To access this page, click **System** > **SNMP** > **SNMP Community**.

The following figure displays the **SNMP Community Status** settings.



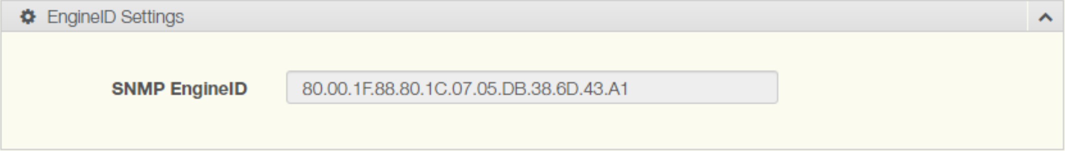
Community Status

No.	Community Name	Access Right	Action
1	public	read-only	Delete
2	private	read-write	Delete

Figure 3.9 System > SNMP > SNMP Community

3.4.2.3 SNMPv3 EngineID

To access this page, click **System** > **SNMP** > **SNMPv3 EngineID**.



EngineID Settings

SNMP EngineID 80.00.1F.88.80.1C.07.05.DB.38.6D.43.A1

Figure 3.10 System > **SNMP** > **SNMPv3 EngineID**

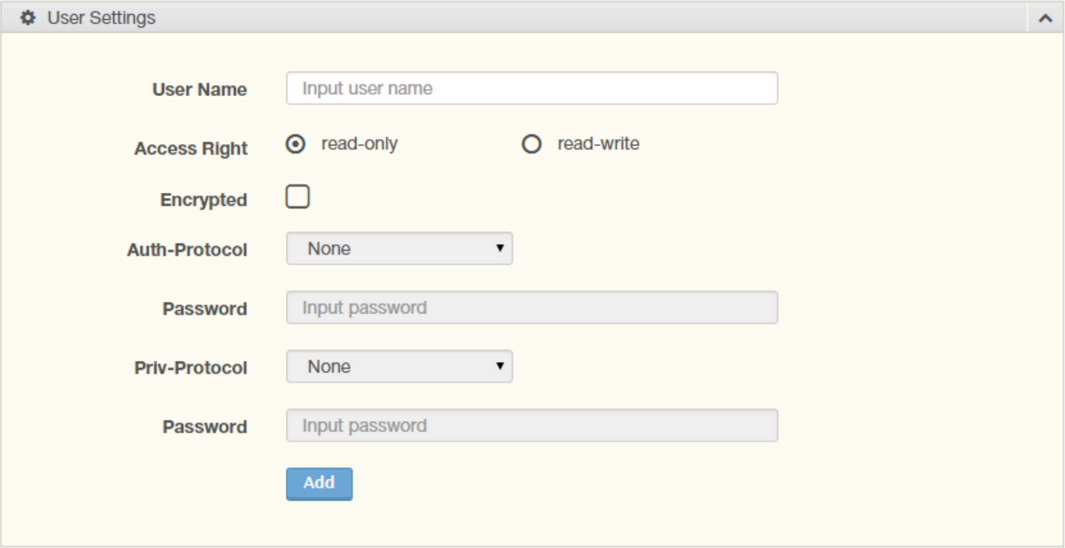
The following table describes the items in the previous figure.

Item	Description
SNMP EngineID	Enter the hexadecimal string to define the engine ID for SNMPv3 agent.

3.4.2.4 SNMPv3 Settings

The SNMPv3 Settings page allows you to create SNMP groups. The users have the same level of security and access control permissions as defined by the group settings.

To access this page, click **System** > **SNMP** > **SNMPv3 Settings**.



User Settings

User Name Input user name

Access Right ● read-only ○ read-write

Encrypted □

Auth-Protocol None

Password Input password

Priv-Protocol None

Password Input password

Add

Figure 3.11 System > **SNMP** > **SNMPv3 Settings**

The following table describes the items in the previous figure.

Item	Description
User Name	Enter a user name (up to 32 characters) to create an SNMP profile.
Access Right	Click **read-only** or **read-write** to define the access right for the profile.
Encrypted	Click the option to set the encrypted option for the user setting.

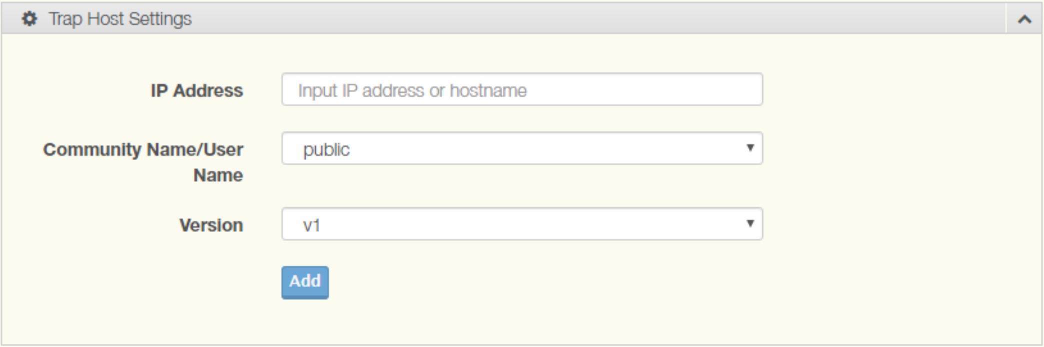
Item	Description
Auth-Protocol	Click the drop-down menu to select the authentication level: MD5 or SHA. The field requires a user password. ■ MD5: specify HMAC-MD5-96 authentication level ■ SHA: specify HMAC-SHA authentication protocol
Password	Enter the characters to define the password associated with the authentication protocol.
Priv-Protocol	Click the drop-down menu to select an authorization protocol: none or DES.The field requires a user password. ■ None: no authorization protocol in use ■ DES: specify 56-bit encryption in use
Password	Enter the characters to define the password associated with the authorization protocol.
Add	Click **Add** to save the values and update the screen.

The ensuing table for **User Status** settings are informational only: User Name, Access Right, Auth-Protocol, Priv-Protocol and **Delete** (click to delete the desired user name).

3.4.2.5 SNMP Trap

The SNMP Trap page allows you to set the IP address of the node and the SNMP credentials corresponding to the version that is included in the trap message.

To access this page, click **System** > **SNMP** > **SNMP Trap**.



Trap Host Settings

IP Address: Input IP address or hostname

Community Name/User Name: public

Version: v1

Figure 3.12 System > SNMP > SNMP Trap

The following table describes the items in the previous figure.

Item	Description
IP Address	Enter the IP address to designate the SNMP trap host.
Community Name	Click the drop-down menu to select a defined community name.
Version	Click the drop-down menu to designate the SNMP version credentials (v1 or v2c).
Add	Click **Add** to save the values and update the screen.

The ensuing table for **Trap Host Status** settings are informational only: No., IP Address, Community Name, Version and **Delete** (click to delete the desired IP address).

3.4.3 System Log

3.4.3.1 Logging Service

The Logging Service page allows you to setup the logging services feature for the system log.

To access this page, click **System** > **System Log** > **Logging Service**.

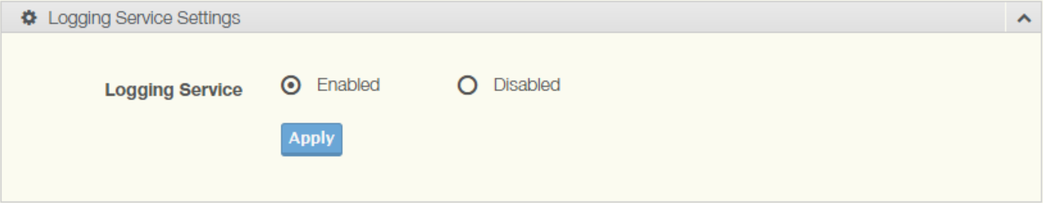


Figure 3.13 System > System Log > Logging Service

The following table describes the items in the previous figure.

Item	Description
Logging Service	Click **Enabled** or **Disabled** to set the Logging Service status.
Apply	Click **Apply** to save the values and update the screen.

The ensuing table for **Logging Information** settings are informational only:

Logging Service.

3.4.3.2 Local Logging

The Local Logging page allows you to designate a local target when the severity criteria is reached.

To access this page, click **System** > **System Log** > **Local Logging**.

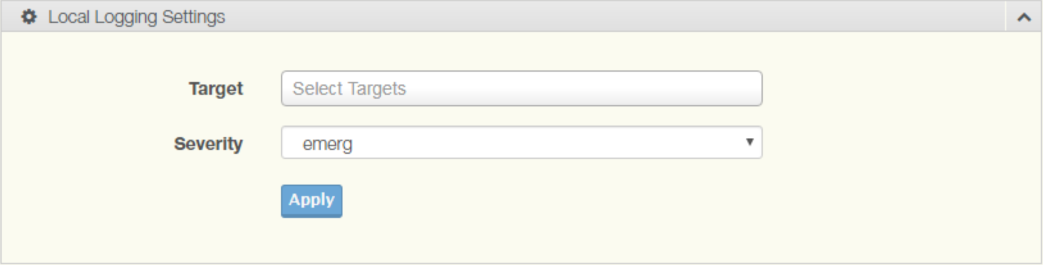


Figure 3.14 System > System Log > Local Logging

The following table describes the items in the previous figure.

Item	Description
Target	Enter the local logging target.
Severity	Click the drop-down menu to select the severity level for local log messages. The level options are: ■ emerg: Indicates system is unusable. It is the highest level of severity ■ alert: Indicates action must be taken immediately ■ crit: Indicates critical conditions ■ error: Indicates error conditions ■ warning: Indicates warning conditions ■ notice: Indicates normal but significant conditions ■ info: Indicates informational messages ■ debug: Indicates debug-level messages
Apply	Click **Apply** to save the values and update the screen.

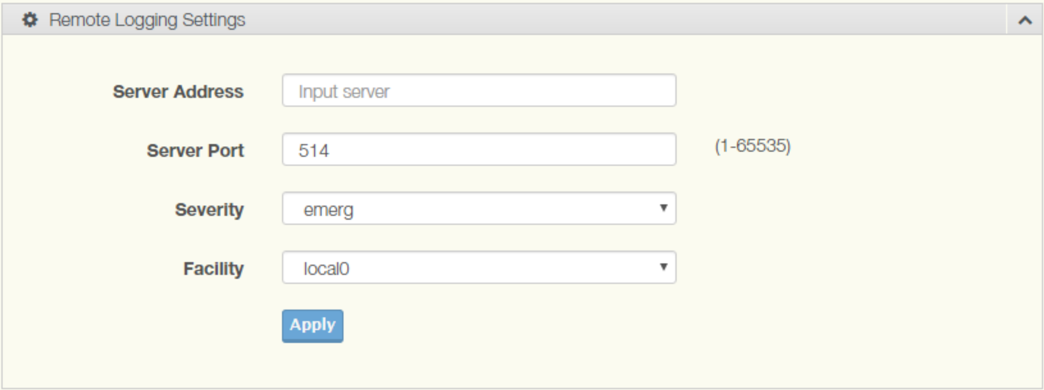
The ensuing table for **Local Logging Settings Status** settings are informational only:

Status, Target, Severity and **Delete** (click to delete the desired target).

3.4.3.3 System Log Server

The System Log Server page allows you to configure the log server.

To access this page, click **System** > **System Log** > **System Log Server**.



Server Address: Input server

Server Port: 514 (1-65535)

Severity: emerg

Facility: local0

Figure 3.15 System > System Log > System Log Server

The following table describes the items in the previous figure.

Item	Description
Server Address	Enter the IP address of the log server.
Server Port	Enter the Udp port number of the log server.
Severity	Click the drop-down menu to select the severity level for local log messages. The default is emerg. The level options are: ■ emerg: Indicates system is unusable. It is the highest level of severity ■ alert: Indicates action must be taken immediately ■ crit: Indicates critical conditions ■ error: Indicates error conditions ■ warning: Indicates warning conditions ■ notice: Indicates normal but significant conditions ■ info: Indicates informational messages ■ debug: Indicates debug-level messages
Facility	Click the drop-down menu to select facility to which the message refers.
Apply	Click **Apply** to save the values and update the screen.

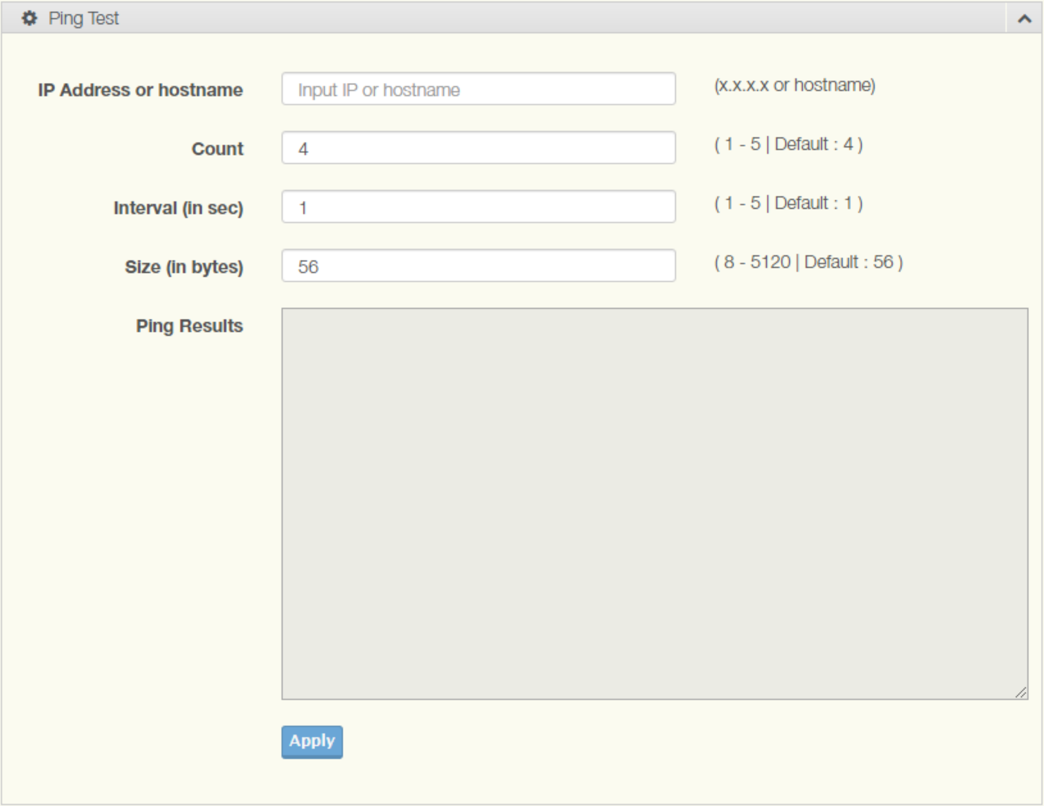
The ensuing table for **Remote Logging Setting Status** settings are informational only:

> Status, Server Info, Severity, Facility and **Delete** (click to delete the desired server address).

3.4.4 Ping Test

The Ping Test page allows you to configure the test log page.

To access this page, click **System** > **Ping Test**.



IP Address or hostname	Input IP or hostname	(x.x.x.x or hostname)
Count	4	(1 - 5 | Default : 4)
Interval (in sec)	1	(1 - 5 | Default : 1)
Size (in bytes)	56	(8 - 5120 | Default : 56)
Ping Results		

Figure 3.16 System > Ping Test

The following table describes the items in the previous figure.

Item	Description
IP Address	Enter the IP address or host name of the station to ping. The initial value is blank. The IP Address or host name you enter is not retained across a power cycle. Host names are composed of series of labels concatenated with periods. Each label must be between 1 and 63 characters long, maximum of 64 characters.
Count	Enter the number of echo requests to send. The default value is 4. The value ranges from 1 to 5. The count entered is not retained across a power cycle.
Interval (in sec)	Enter the interval between ping packets in seconds. The default value is 1. The value ranges from 1 to 5. The interval entered is not retained across a power cycle.
Size (in bytes)	Enter the size of ping packet. The default value is 56. The value ranges from 8 to 5120. The size entered is not retained across a power cycle.

Item	Description
Ping Results	Display the reply format of ping. PING 172.17.8.254 (172.17.8.254): 56 data bytes --- 172.17.8.254 ping statistics --- 4 packets transmitted, 0 packets received, 100% packet loss Or PING 172.17.8.93 (172.17.8.93): 56 data bytes 64 bytes from 172.17.8.93: icmp_seq=0 ttl=128 time=0.0 ms 64 bytes from 172.17.8.93: icmp_seq=1 ttl=128 time=0.0 ms 64 bytes from 172.17.8.93: icmp_seq=2 ttl=128 time=0.0 ms 64 bytes from 172.17.8.93: icmp_seq=3 ttl=128 time=0.0 ms --- 172.17.8.93 ping statistics --- 4 packets transmitted, 4 packets received, 0% packet loss round-trip min/avg/max = 0.0/0.0/0.0 ms
Apply	Click **Apply** to save the values and update the screen.

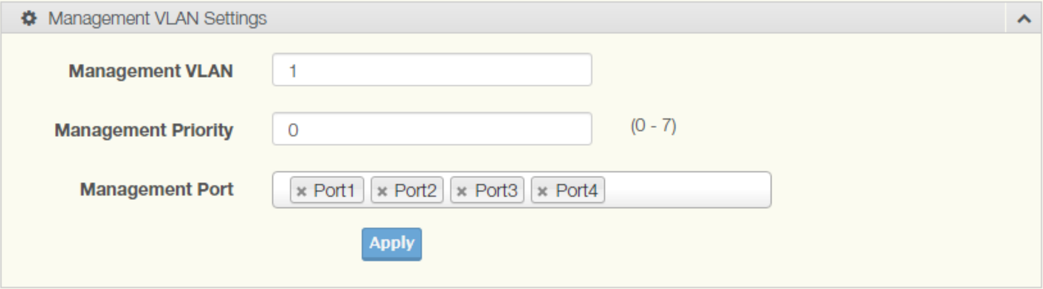
3.5 Switching

3.5.1 VLAN

3.5.1.1 Management VLAN

By default the VLAN is the management VLAN providing communication with the converter management interface.

To access this page, click **Switching** > **VLAN** > **Management VLAN**.



Management VLAN: 1

Management Priority: 0 (0 - 7)

Management Port: × Port1 × Port2 × Port3 × Port4

Figure 3.17 Switching > VLAN > Management VLAN

The following table describes the items in the previous figure.

Item	Description
Management VLAN	Click the drop-down menu to select a defined VLAN.
Management Priority	Enter a variable (0-7) to designate the priority of the defined VLAN. The priority settings assigns a priority to outbound packets containing a specified VLAN ID (VID). Any packet with a VID are marked with the priority level configured for that VID classifier.
Management Port	Select the port to designate as an isolated network for managing the device.
Apply	Click **Apply** to save the values and update the screen.

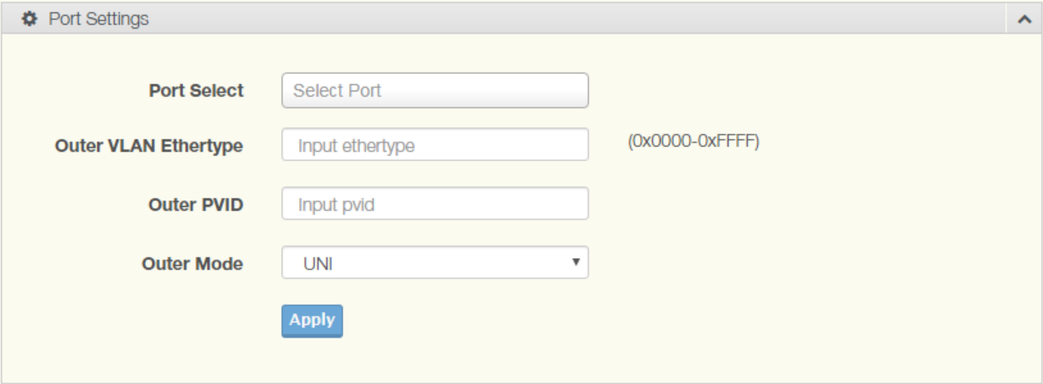
The ensuing table for **Management VLAN Information** settings are informational only:

Management VLAN, Management Priority, Management Tag Mode and Management Allow Ports.

3.5.1.2 Port Settings

The Port Settings page allows you to define the outer PVID and outer mode for a selected port.

To access this page, click **Switching** > **VLAN** > **Port Settings**.



Port Settings

Port Select	Select Port
Outer VLAN Ethertype	Input ethertype (0x0000-0xFFFF)
Outer PVID	Input pvid
Outer Mode	UNI

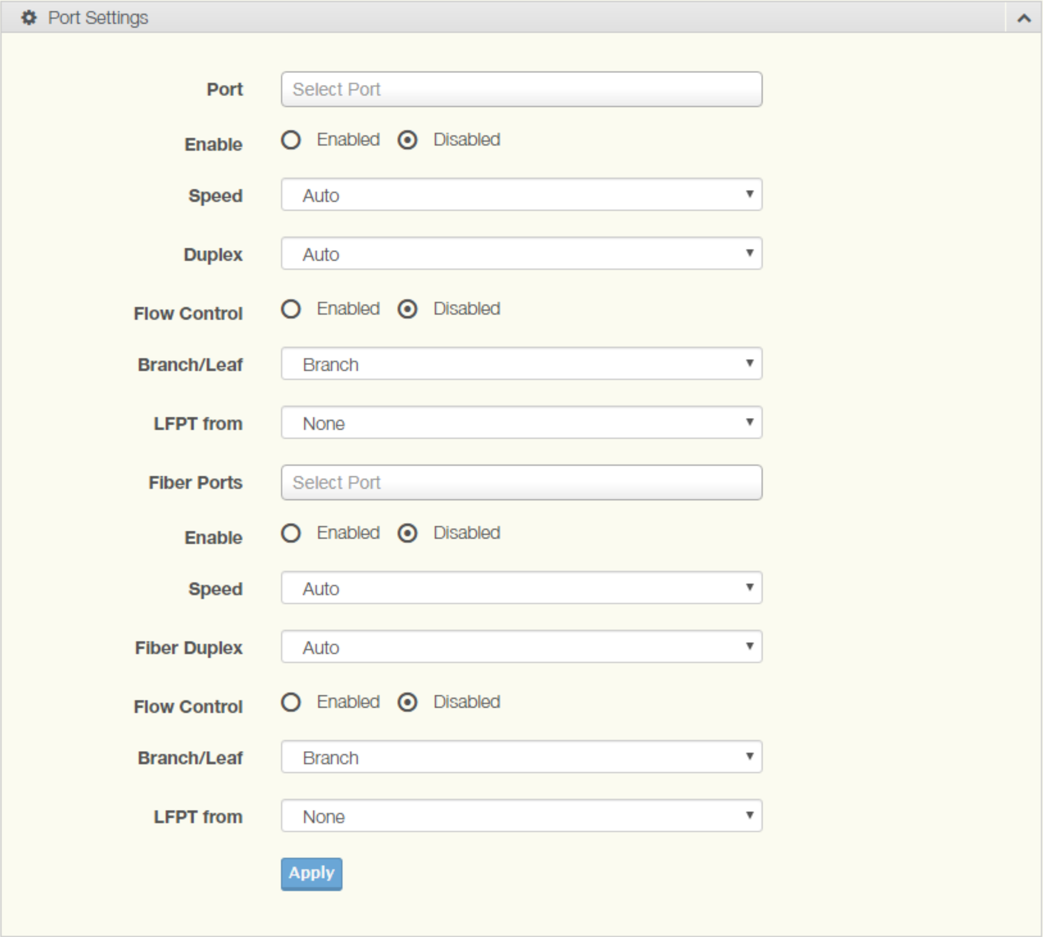
Figure 3.18 Switching > VLAN > Port Settings

The following table describes the items in the previous figure.

Item	Description
Port Select	Enter the converter port (part of VLAN configuration) to configure the selection as a tunnel port.
Outer VLAN Ethertype	Enter the outer VLAN handled by the converter giving the attached machine a single-tagged 802.1Q VLAN frame.
Outer PVID	Enter the Port VLAN ID (PVID) to assigned the native VLAN ID. All untagged traffic coming in or out of the 802.1Q port is forwarded based on the PVID value.
Outer Mode	Click the drop-down menu to select between UNI or NNI role. ■ UNI: Selects a user-network interface which specifies communication between the specified user and a specified network. ■ NNI: Selects a network-to-network interface which specifies communication between two specified networks.
Apply	Click **Apply** to save the values and update the screen.

3.5.2 Port Configuration

To access this page, click **Switching** > **Port Configuration**.



Port	Select Port
Enable	○ Enabled ● Disabled
Speed	Auto
Duplex	Auto
Flow Control	○ Enabled ● Disabled
Branch/Leaf	Branch
LFPT from	None
Fiber Ports	Select Port
Enable	○ Enabled ● Disabled
Speed	Auto
Fiber Duplex	Auto
Flow Control	○ Enabled ● Disabled
Branch/Leaf	Branch
LFPT from	None

Figure 3.19 Switching > Port Configuration

The following table describes the items in the previous figure.

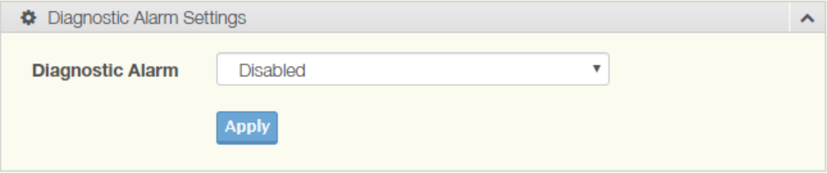
Item	Description
Port	Click the drop-down menu to select the port for the L2 Switch setting.
Enabled	Click the radio-button to enable or disable the Port Setting function.
Speed	Click the drop-down menu to select the port speed: Auto, Auto-10M, Auto-100M, Auto-1000M, Auto-10/100M, 10M, 100M, or 1000M.
Duplex	Click the drop-down menu to select the duplex setting: Auto, Half or Full.
Flow Control	Click the radio button to enable or disable the flow control function.
Branch/Leaf	Click the drop-down menu to select the port type: Branch or Leaf.
LFPT from	Define the Link Fault Pass Through (LFPT) segment to be used as the point of failure for the local network equipment location. Options include: None, Port 1 ~ 4.
Fiber Port	Click the drop-down menu to select the port for the L2 Switch Fiber port setting.
Enabled	Click the radio-button to enable or disable the Fiber Port Setting function.
Speed	Click the drop-down menu to select the fiber port speed: Auto, Auto-1000M, 100M, or 1000M.
Fiber Duplex	Click the drop-down menu to select the duplex setting: Full or Auto.
Flow Control	Click the radio button to enable or disable the flow control function.

Item	Description
Branch/Leaf	Click the drop-down menu to select the fiber port type: Branch or Leaf.
LFPT from	Define the Link Fault Pass Through (LFPT) segment to be used as the point of failure for the fiber port. Options include: None, Port 1 ~ 4.
Apply	Click **Apply** to save the values and update the screen.

3.5.3 DDM

The DDM page allows you to setup the diagnostic alarm status.

To access this page, click **Switching** > **DDM**.



Diagnostic Alarm Settings

Diagnostic Alarm: Disabled ▾

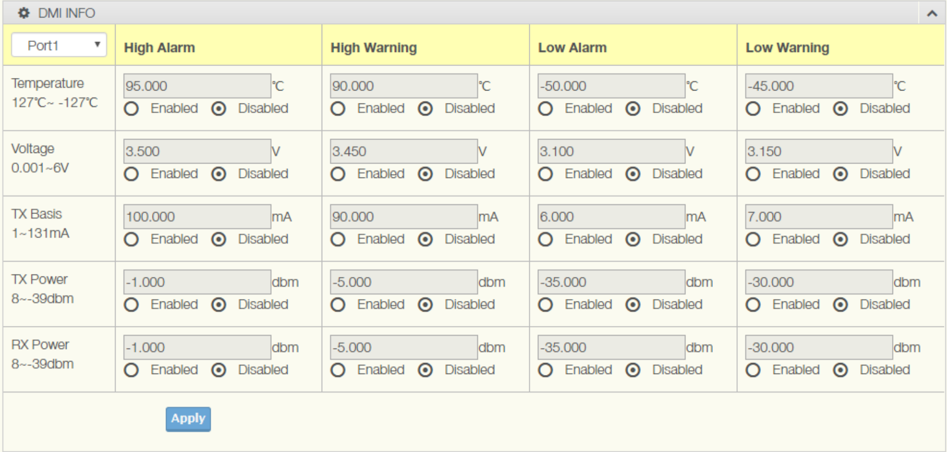
Figure 3.20 Switching > DDM > Diagnostic Alarm Settings

The following table describes the items in the previous figure.

Item	Description
Diagnostic Alarm	Click the drop-down menu to designate the announcement method: Disabled, SysLog, or SNMP.
Apply	Click **Apply** to save the values and update the screen.

The ensuing table for **Diagnostic Alarm Information** settings are informational only:

Diagnostic Alarm.



DMI INFO

Port1 ▾	High Alarm	High Warning	Low Alarm	Low Warning
Temperature 127℃~ -127℃	95.000 ℃ ○ Enabled ● Disabled	90.000 ℃ ○ Enabled ● Disabled	-50.000 ℃ ○ Enabled ● Disabled	-45.000 ℃ ○ Enabled ● Disabled
Voltage 0.001~6V	3.500 V ○ Enabled ● Disabled	3.450 V ○ Enabled ● Disabled	3.100 V ○ Enabled ● Disabled	3.150 V ○ Enabled ● Disabled
TX Basis 1~131mA	100.000 mA ○ Enabled ● Disabled	90.000 mA ○ Enabled ● Disabled	6.000 mA ○ Enabled ● Disabled	7.000 mA ○ Enabled ● Disabled
TX Power 8~-39dbm	-1.000 dbm ○ Enabled ● Disabled	-5.000 dbm ○ Enabled ● Disabled	-35.000 dbm ○ Enabled ● Disabled	-30.000 dbm ○ Enabled ● Disabled
RX Power 8~-39dbm	-1.000 dbm ○ Enabled ● Disabled	-5.000 dbm ○ Enabled ● Disabled	-35.000 dbm ○ Enabled ● Disabled	-30.000 dbm ○ Enabled ● Disabled

Figure 3.21 Switching > DDM > DMI INFO

The following table describes the items in the previous figure.

Item	Description
High Alarm	Click **Enabled** or **Disabled** to set the alarm state.
High Warning	Click **Enabled** or **Disabled** to set the alarm state.
Low Alarm	Click **Enabled** or **Disabled** to set the alarm state.
Low Warning	Click **Enabled** or **Disabled** to set the alarm state.
Apply	Click **Apply** to save the values and update the screen.

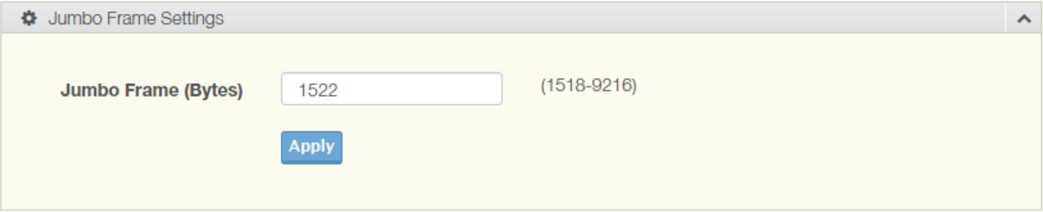
The ensuing table for **Vendor Info** settings are informational only:

Refresh (click to reload the vendor information), Port, Connector, Speed, VendorName, VendorOui, VendorPn, VendorRev, VendorSn and DateCode.

3.5.4 Jumbo Frame

Jumbo frames are frames larger than the standard Ethernet frame size of 1518 bytes. The Jumbo Frame function allows the configuration of Ethernet frame size.

To access this page, click **Switching** > **Jumbo Frame**.



Jumbo Frame Settings

Jumbo Frame (Bytes): 1522 (1518-9216)

Figure 3.22 Switching > Jumbo Frame

The following table describes the items in the previous figure.

Item	Description
Jumbo Frame (Bytes)	Enter the variable in bytes (1518 to 9216) to define the jumbo frame size.
Apply	Click **Apply** to save the values and update the screen.

The ensuing table for **Jumbo Frame Config** settings are informational only:

Jumbo Frame (Bytes).

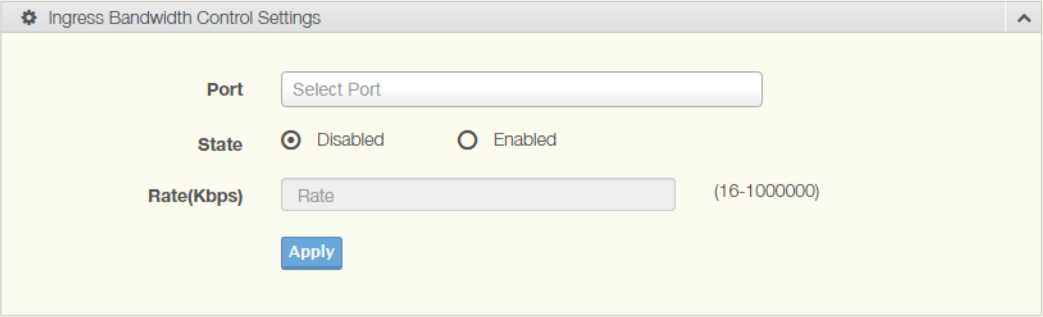
3.5.5 Rate Limit

Rate Limits features control on a per port basis. Bandwidth control is supported for the following: Ingress Bandwidth Control and Egress Bandwidth Control.

3.5.5.1 Ingress Bandwidth Control

The Ingress Bandwidth Control page allows you to configure the bandwidth control for a listed port.

To access this page, click **Switching** > **Rate Limit** > **Ingress Bandwidth Control**.



Ingress Bandwidth Control Settings

Port: Select Port

State: ● Disabled ○ Enabled

Rate(Kbps): Rate (16-1000000)

Figure 3.23 Switching > Rate Limit > Ingress Bandwidth Control

The following table describes the items in the previous figure.

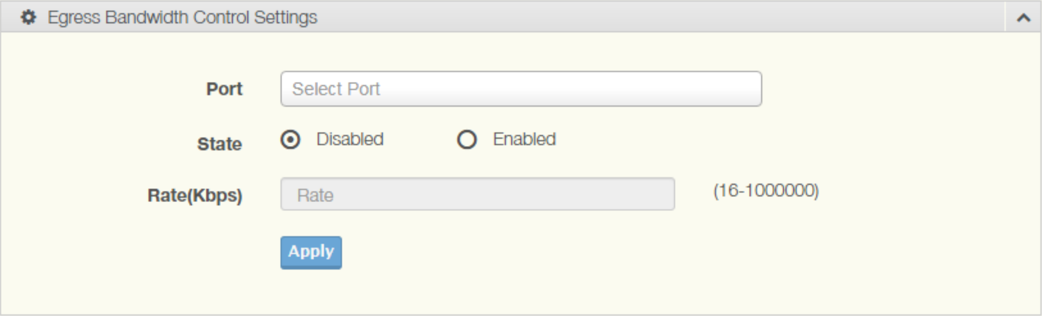
Item	Description
Port	Enter the port number for the rate limit setup.
State	Click **Enabled** or **Disabled** to set the port's state status.
Rate (Kbps)	Enter the value in Kbps (16 to 1000000) to set as the bandwidth rate for the selected port.
Apply	Click **Apply** to save the values and update the screen.

The ensuing table for **Ingress Bandwidth Control Status** settings are informational only: Port and Ingress Rate Limit (Kbps).

3.5.5.2 Egress Bandwidth Control

The Egress Bandwidth Control page allows you to set the egress bandwidth control for a listed port.

To access this page, click **Switching** > **Rate Limit** > **Egress Bandwidth Control**.



Egress Bandwidth Control Settings

Port: Select Port

State: ● Disabled ○ Enabled

Rate(Kbps): Rate (16-1000000)

Apply

Figure 3.24 Switching > Rate Limit > Egress Bandwidth Control

The following table describes the items in the previous figure.

Item	Description
Port	Enter the port number to set the Egress Bandwidth Control.
State	Click **Enabled** or **Disabled** to set the Egress Bandwidth Control state.
Rate (Kbps)	Enter the value in Kbps (16 to 1000000) to set the Egress Bandwidth rate.
Apply	Click **Apply** to save the values and update the screen.

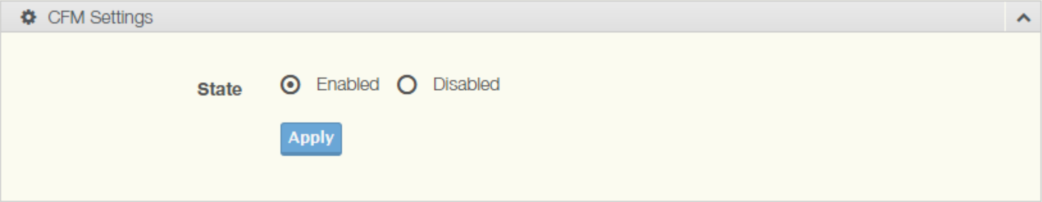
The ensuing table for **Egress Bandwidth Control Status** settings are informational only:

Port and Egress Rate Limit (Kbps).

3.5.6 CFM

3.5.6.1 CFM Settings

To access this page, click **Switching** > **CFM** > **CFM Settings**.



CFM Settings

State: ● Enabled ○ Disabled

Apply

Figure 3.25 Switching > CFM > CFM Settings

The following table describes the items in the previous figure.

Item	Description
State	Click **Enabled** or **Disabled** to enable CFM settings.
Apply	Click **Apply** to save the values and update the screen.

The ensuing table for **Information** settings are informational only:

CFM State.

3.5.6.2 MD Groups

To access this page, click **Switching** > **CFM** > **MD Groups**.

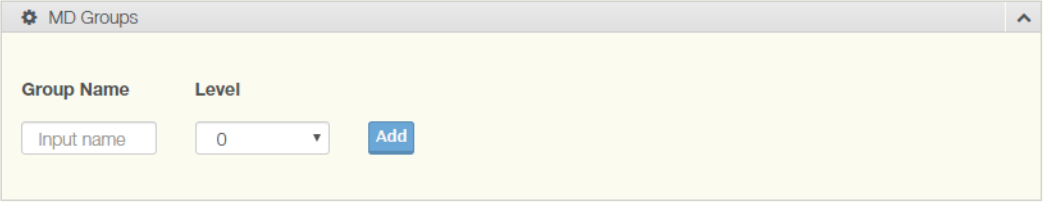


Figure 3.26 Switching > CFM > MD Groups

The following table describes the items in the previous figure.

Item	Description
Group Name	Enter a string to define the managed domains group entry.
Level	Click the drop-down menu to select the minimal level of privilege needed for a user to gain access to the check point. Options: 0 ~ 7. The higher the domain, the higher the value. ■ Customer Domain: Largest (e.g., 7) ■ Provider Domain: In between (e.g., 3) ■ Operator Domain: Smallest (e.g., 1)
Add	Click **Add** to add a MD group.

The ensuing table for **Information** settings are informational only:

Group Name, Level and **Delete** (click to delete the desired group).

3.5.6.3 MA Settings

To access this page, click **Switching** > **CFM** > **MA Settings**.

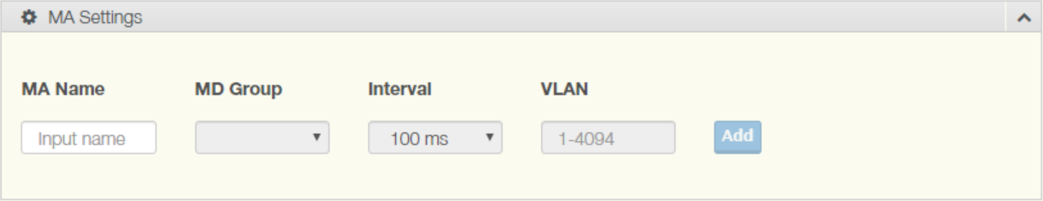


Figure 3.27 Switching > CFM > MA Settings

The following table describes the items in the previous figure.

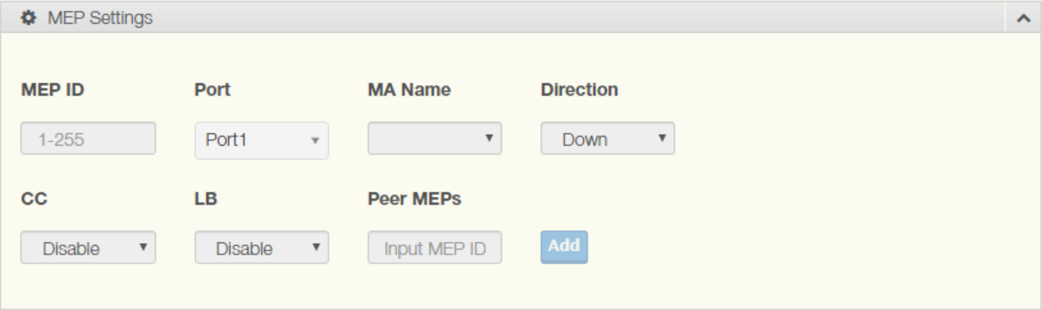
Item	Description
MA Name	Enter a string to define the maintenance association (MA) - defined as a set of maintenance association end points (MEPs), configured with the same maintenance association identifier (MAID) and MD level.
MD Group	Click the drop-down menu to select a previously defined MD Group to assign the MA entry.
Interval	Click the drop-down menu to specify the interval drop-period for continuity check messages between a port and its peer. Available options: 100 ms, 1 s, 10 s, 1 min, 10 min.
VLAN	Enter a variable to define the VLAN for continuity check messages for the MA setting.
Add	Click **Add** to add a MA setting.

The ensuing table for **Information** settings are informational only:

MA Name, VLAN, MD Group, MD Level, Interval and **Delete** (click to delete the desired setting).

3.5.6.4 MEP Settings

To access this page, click **Switching** > **CFM** > **MEP Settings**.



MEP Settings

MEP ID: 1-255
Port: Port1
MA Name:
Direction: Down
CC: Disable
LB: Disable
Peer MEPs: Input MEP ID
Add

Figure 3.28 Switching > CFM > MEP Settings

The following table describes the items in the previous figure.

Item	Description
MEP ID	Enter the value to set as the identifier for the maintenance end point.
Port	Click the drop-down menu to configure the port MEP - a down MEP that is untagged and not associated with a VLAN. Options: Port 1 ~ 4.
MA Name	Click the drop-down menu to select the associated maintenance association previously defined.
Direction	Click the drop-down menu to define the communication mode for the setting. Options include Down or Up. Down MEPs communicate through the wire side (connected to the port), while the up setting determines communication through the relay function side, not the wire side.
CC	Click the drop-down menu to enable the sending and receiving of continuity check messages. Options: Disable or Enable.
LB	Click the drop-down menu to enable the loopback function--similar to IP ping for maintenance. Options Disable or Enable.
Peer MEPs	Enter a string to define the MEP name.
Add	Click **Add** to add a MEP setting.

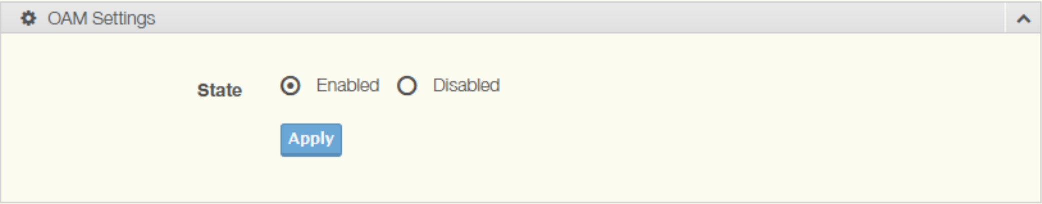
The ensuing table for **MEP Information** settings are informational only:

> MEP ID, Port, Direction, MA Name / Vlan, MD Group / Level, **Delete** (click to delete the desired setting), CC State, TX CCM, RX CCM, Loss of Continuity, Unexpected MD Level, MD Mismerge, MA Mismerge, Unexpected mep, Unexpected period, LB State, LBM TX Unicast, LBM TX Multicast, LBM RX Unicast, LBM RX Multicast, Invalid LBR Frame and Invalid LTR Frame.

3.5.7 OAM

3.5.7.1 OAM State

To access this page, click **Switching** > **OAM** > **OAM State**.



OAM Settings

State ● Enabled ○ Disabled

Apply

Figure 3.29 Switching > OAM > OAM State

The following table describes the items in the previous figure.

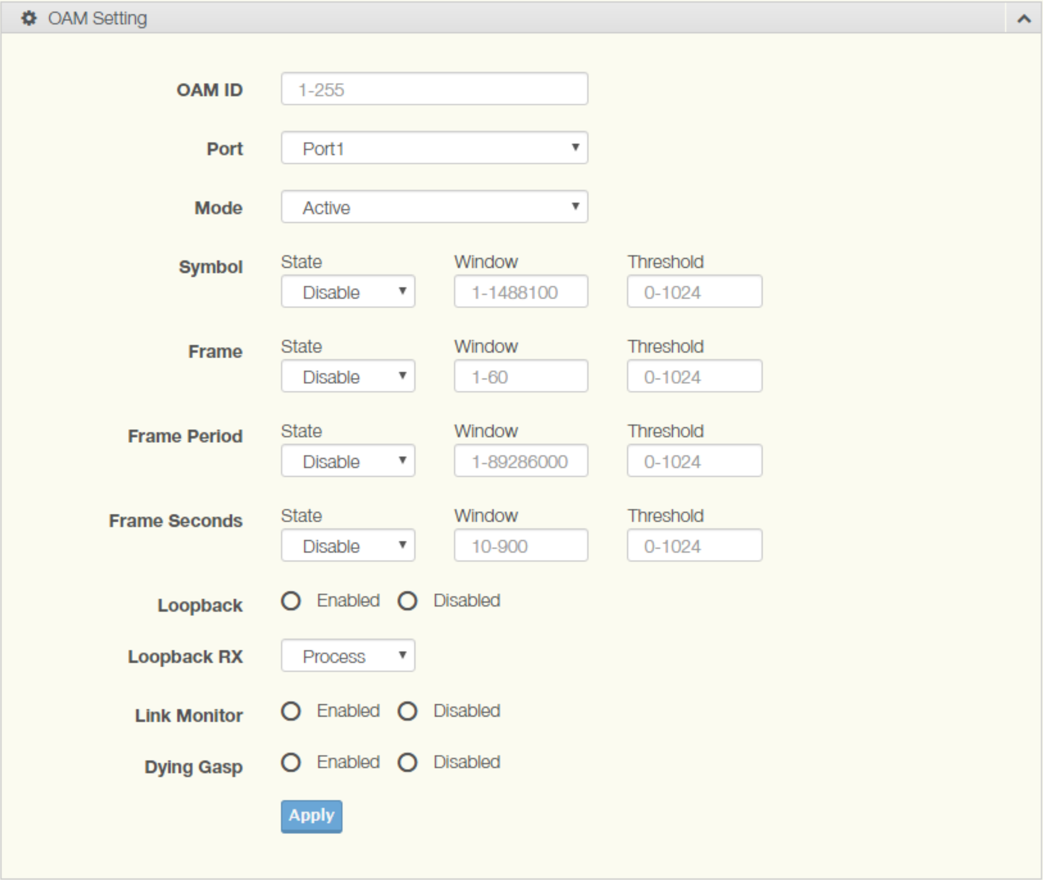
Item	Description
State	Click **Enabled** or **Disabled** to enable the operation and administration management (OAM) function.
Apply	Click **Apply** to save the values and update the screen.

The ensuing table for **Information** settings are informational only:

OAM State.

3.5.7.2 OAM Setting

To access this page, click **Switching** > **OAM** > **OAM Setting**.



OAM Setting

OAM ID	1-255		
Port	Port1		
Mode	Active		
Symbol	State: Disable	Window: 1-1488100	Threshold: 0-1024
Frame	State: Disable	Window: 1-60	Threshold: 0-1024
Frame Period	State: Disable	Window: 1-89286000	Threshold: 0-1024
Frame Seconds	State: Disable	Window: 10-900	Threshold: 0-1024
Loopback	○ Enabled ○ Disabled		
Loopback RX	Process		
Link Monitor	○ Enabled ○ Disabled		
Dying Gasp	○ Enabled ○ Disabled		

Figure 3.30 Switching > OAM > OAM Setting

The following table describes the items in the previous figure.

Item	Description
OAM ID	Enter the variable to define the Operation, Administration, and Maintenance (OAM) protocol identifier. Options: 1 ~ 255.
Port	Click the drop-down menu to select the proxy-port (not OAM managed server port). Options: Port 1 ~ 4.
Mode	Click the drop-down menu to select the OAM mode for the port. ■ Active: In this mode, the port can initiate a OAM connection. It is the default setting. ■ Passive: In this mode, the port cannot initiate an OAM connection or send loopback control OAMPDUs. *Note: An OAM connection cannot be established between two ports in passive mode. At least one side must be configured to active mode to initiate a connection.*

Item	Description
Symbol	■ State: Click the drop-down menu to enable the symbol period event timestamp. Options: Disable or Enable. ■ Window: Enter an octet variable (1 ~ 1488100) to indicate the number or error symbols in the period. ■ Threshold: Enter an octet variable (0 ~ 1024) to indicate the required error symbols in the period, equal to or greater than, to trigger the event generation.
Frame	■ State: Click the drop-down menu to enable the detection or erred frames within a period. Options: Disable or Enable. ■ Window: Enter the octet variable to define the duration of period (1 ~ 60 seconds) in terms of frames. ■ Threshold: Enter the octet variable to indicate the required define the number of erred frames (0 to 1024 frame errors), equal to or greater than, to trigger the event generation.
Frame Period	■ State: Click the drop-down menu to enable the frame period error event function. Options: Disable or Enable. ■ Window: Enter the octet variable to define the duration ((1 ~ 89286000) of period in terms of frames. ■ Threshold: Enter the octet variable to define the required number of erred frames in a period (0 ~ 1024), equal to or greater than, to trigger an event generation.
Frame Seconds	■ State: Click the drop-down menu to enable the frame seconds summary function. Options: Disable or Enable. ■ Window: Enter an octet variable to indicate the duration (10 ~ 900) in terms of 100 ms intervals, encoded as a 16-bit unsigned integer. ■ Threshold: Enter an octet variable to define the required number of erred frame seconds (0 ~ 1024), equal to or greater than, to trigger an event generation.
Loopback	Select to enable or disable the loopback to the remote.
Loopback RX	Click the drop-down menu to set the mode for the Loopback policy. ■ Process: Enables a packet to be sent out of the loop to re-initialize the discovery process. ■ Ignored: A packed is ignored the exploratory message.
Link Monitor	Select to enable or disable. When enabled, the CPU must poll error counters.
Dying Gasp	Select to enable or disable. When enabled a notification is delivered if an unrecoverable condition occurs.
Apply	Click **Apply** to save the values and update the screen.

The ensuing table for **OAM Status** settings are informational only:

OAM ID, State, Port, Mode, Detail and **Delete** (click to delete the desired setting).

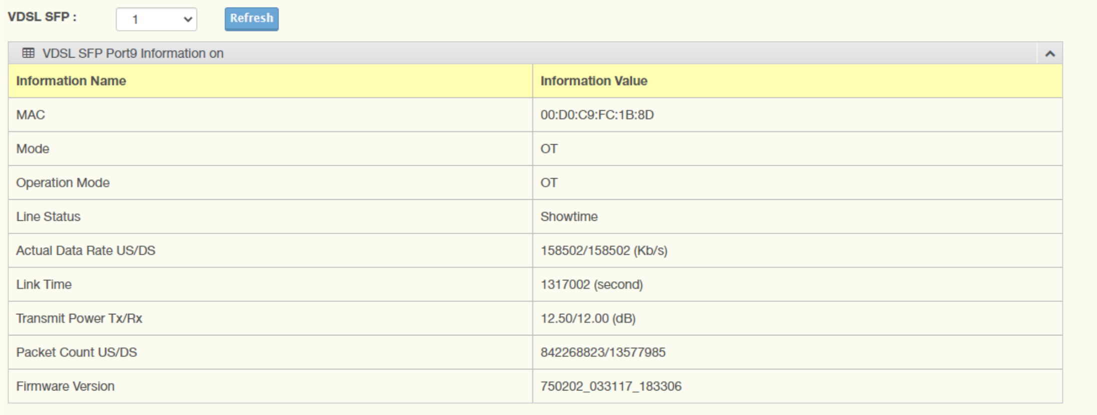
3.5.7.3 OAM Event Log

The ensuing table for **OAM Status** settings are informational only:

TimeStamp, Format, Type, Location, Window, Threshold, Value, RunTotal and EvtTotal.

3.5.8 VDSL SFP

To access this page, click **Switching** > **VDSL SFP**.



VDSL SFP Port9 Information on

Information Name	Information Value
MAC	00:D0:C9:FC:1B:8D
Mode	OT
Operation Mode	OT
Line Status	Showtime
Actual Data Rate US/DS	158502/158502 (Kb/s)
Link Time	1317002 (second)
Transmit Power Tx/Rx	12.50/12.00 (dB)
Packet Count US/DS	842268823/13577985
Firmware Version	750202_033117_183306

Figure 3.31 Switching > VDSL SFP

The following table describes the items in the previous figure.

Item	Description
VDSL SFP	Click the drop-down menu to view the corresponding port information.
Refresh	Click Refresh to update to the latest information.
Information Name	Displays the available port data.
Information Value	Displays the corresponding value for the listed information.

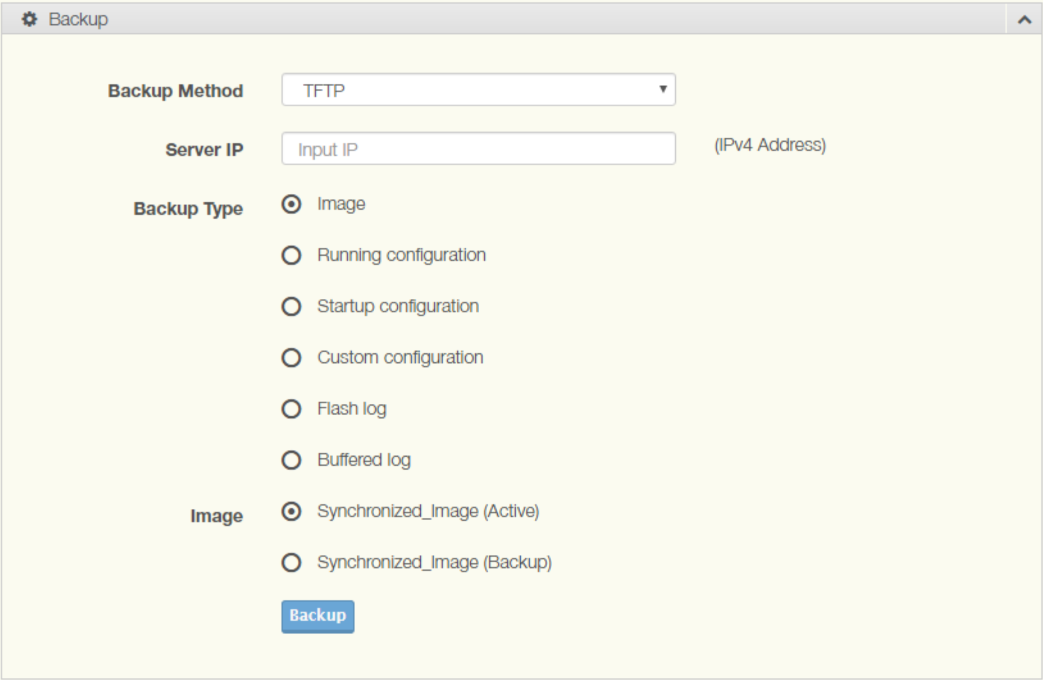
3.6 Tools

3.6.1 Backup Manager

The Backup Manager page allows you to configure a remote TFTP sever or host file system in order to backup the firmware image or configuration file.

To access this page, click **Tools** > **Backup Manager**.

The following figures represent multiple supported devices. Some interface screens may represent specific device models.



Backup

Backup Method: TFTP

Server IP: Input IP (IPv4 Address)

Backup Type:
- ● Image
- ○ Running configuration
- ○ Startup configuration
- ○ Custom configuration
- ○ Flash log
- ○ Buffered log

Image:
- ● Synchronized_Image (Active)
- ○ Synchronized_Image (Backup)

Figure 3.32 Tools > Backup Manager

The following table describes the items in the previous figure.

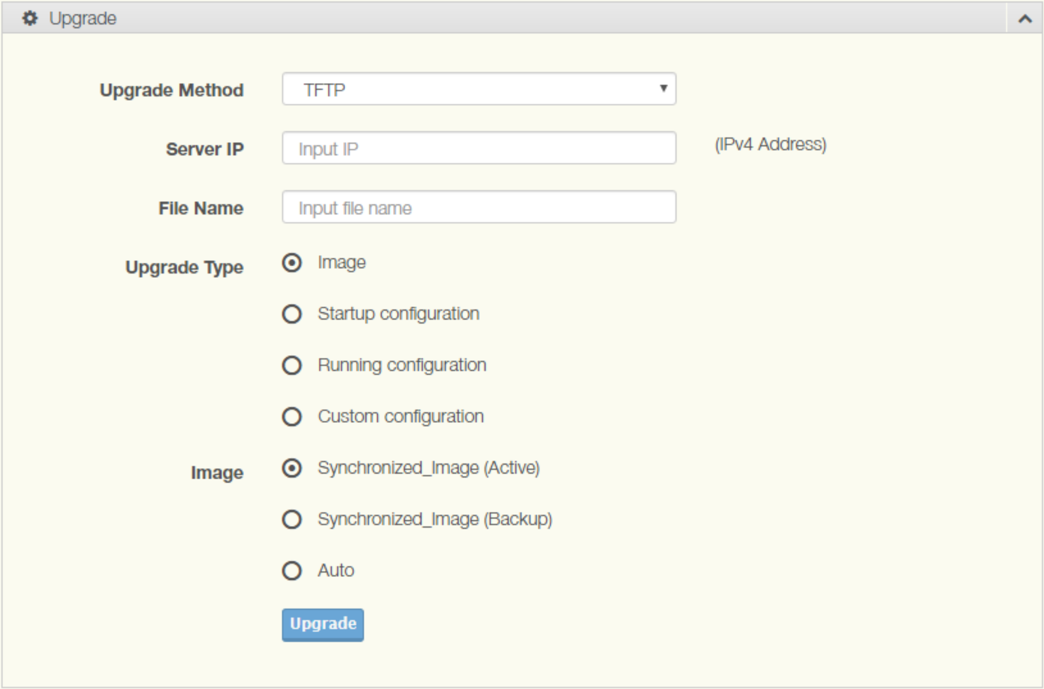
Item	Description
Backup Method	Click the drop-down menu to select the backup method: TFTP or HTTP.
Server IP	Enter the IP address of the backup server.
Backup Type	Click a type to define the backup method: image, running configuration, startup configuration, custom configuration, flash log, or buffered log.
Image	Click the format for the image type: **Active** or **Backup**.
Backup	Click **Backup** to backup the settings.

3.6.2 Upgrade Manager

The Upgrade Manager page allows you to configure a remote TFTP sever or host file system in order to upload firmware upgrade images or configuration files.

To access this page, click **Tools** > **Upgrade Manager**.

The following figures represent multiple supported devices. Some interface screens may represent specific device models.



Upgrade

Upgrade Method: TFTP

Server IP: Input IP (IPv4 Address)

File Name: Input file name

Upgrade Type:
● Image
○ Startup configuration
○ Running configuration
○ Custom configuration

Image:
● Synchronized_Image (Active)
○ Synchronized_Image (Backup)
○ Auto

Figure 3.33 Tools > Upgrade Manager

The following table describes the items in the previous figure.

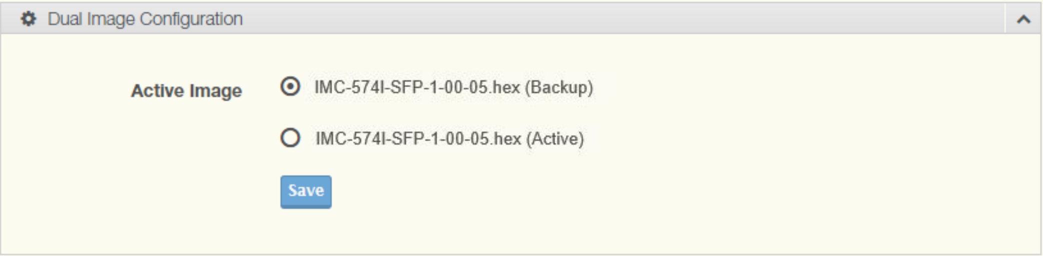
Item	Description
Upgrade Method	Click the drop-down menu to select the upgrade method: TFTP or HTTP.
Server IP	Enter the IP address of the upgrade server.
File Name	Enter the file name of the new firmware version.
Upgrade Type	Click a type to define the upgrade method: image, startup configuration, running configuration, or custom configuration.
Image	Click the format for the image type: **Active**, **Backup**, or **Auto**.
Upgrade	Click **Upgrade** to upgrade to the current version.

3.6.3 Dual Image

The Dual Image page allows you to setup an active and backup partitions for firmware image redundancy.

To access this page, click **Tools** > **Dual Image**.

The following figures represent multiple supported devices. Some interface screens may represent specific device models.



Active Image ● IMC-574I-SFP-1-00-05.hex (Backup)

○ IMC-574I-SFP-1-00-05.hex (Active)

Figure 3.34 Tools > Dual Image

The following table describes the items in the previous figure.

Item	Description
Active Image	Click the format for the image type: **Active** or **Backup**.
Save	Click **Save** to save and keep the new settings.

The ensuing table for **Image Information 0/1** settings are informational only:

Flash Partition, Image Name, Image Size and Created Time.

3.6.4 Save Configuration

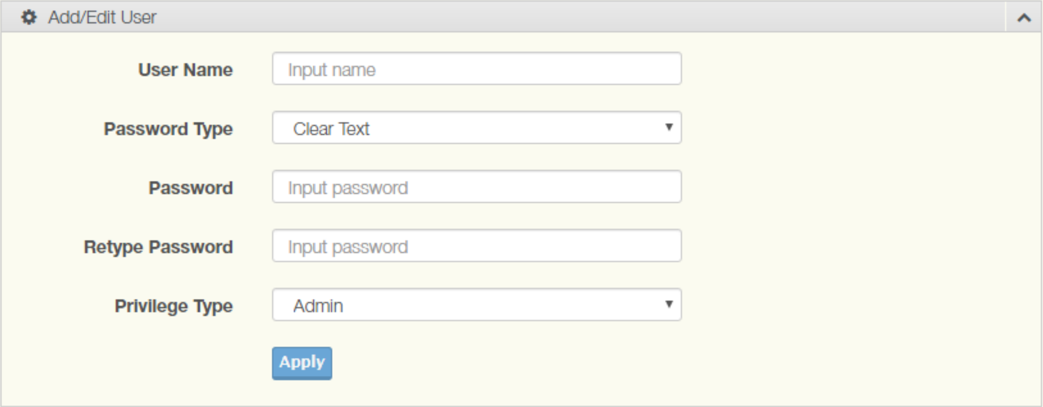
To access this page, click **Tools** > **Save Configuration**.

Click **Save Configuration to FLASH** to have configuration changes you have made to be saved across a system reboot. All changes submitted since the previous save or system reboot will be retained by the switch.

3.6.5 User Account

The User Account page allows you to setup a user and the related parameters.

To access this page, click **Tools** > **User Account**.



Add/Edit User

User Name	Input name
Password Type	Clear Text
Password	Input password
Retype Password	Input password
Privilege Type	Admin

Figure 3.35 Tools > User Account

The following table describes the items in the previous figure.

Item	Description
User Name	Enter the name of the new user entry.
Password Type	Click the drop-down menu to define the type of password: **Clear Text**, **Encrypted** or **No Password**.
Password	Enter the character set for the define password type.
Retype Password	Retype the password entry to confirm the profile password.
Privilege Type	Click the drop-down menu to designate privilege authority for the user entry: **Admin** or **User**.
Apply	Click **Apply** to create a new user account.

The ensuing table for **Local Users** settings are informational only:

User Name, Password Type, Privilege Type and **Delete** (click to delete the desired user account).

3.6.6 Reset System

To access this page, click **Tools** > **Reset System**.

Click **Restore** to have all configuration parameters reset to their factory default values. All changes that have been made will be lost, even if you have issued a save.

Click **Select Excepted Configuration** to keep the configuration you selected when resetting.

Reset settings take effect after a system reboot.

3.6.7 Reboot Device

To access this page, click **Tools** > **Reboot Device**.

Click **Reboot** to reboot the switch. Any configuration changes you have made since the last time you issued a save will be lost.

Chapter 4

Configuration

The IMC-574I-SFP includes many features that are configurable via a serial/Telnet session (CLI) or through iView^2 (SNMP Management view or iConfig view).

4.1 Configuration Feature Options

The below features are configurable through both iView^2 (iConfig view) and Serial/Telnet.

- Loopback
- Auto Negotiation
- Force Mode
- FlowControl
- VLANs
- IP Address
- Subnet Mask
- Default Gateway
- MIB Community
- Traps Assignment
- Users
- Passwords
- Access Level
- Reboot
- Frame Sizes
- Bandwidth Limiting
- LFPT (Link Fault Pass Through)

4.2 Configuration Management Options

The below table presents management options configurable via a serial/Telnet session.

Feature	Save Configuration	GUI
PROM Software Download/Upload		V
Telnet Session	V	V
Software Download Setup (TFTP)	V	V
DHCP	V	V
Restore Configuration	V	V
Save Configuration		V
MACTAB	V	V
Clear Counters	V	V
Disable/Enable Management on Ports	V	V

4.3 Basic Device Configuration Using the CLI

4.3.1 Port Configuration

Table 4.1: Port Configuration

Function	Privilege	Description	Example
`show sfp protection`	User EXEC	Display SFP protection state.	switch# show sfp protection
`[no] shutdown`	Admin EXEC	Use “shutdown” command to disable port and use “no shutdown” to enable port. If port is error disabled for any reason, use “no shutdown” command to recover the port manually.	This example shows how to modify port duplex configuration. switch(config)# interface GigabitEthernet 1 switch(config-if)# shutdown
`speed (10|100|1000)`	Admin EXEC	Use “speed” command to change port speed configuration. The speed is only able to configure to the physical maximum speed. For example, in fast Ethernet port, speed 1000 is not available.	This example shows how to modify port speed configuration. switch(config)# interface GigabitEthernet 2 switch(config-if)# speed auto 10/100
`speed auto [(10|100|10/100|1000)]`	Admin EXEC		
`[no] speed nonegotiate`	Admin EXEC		switch(config)# interface GigabitEthernet 1 switch(config-if)# speed nonegotiate
`duplex (auto|full|half)`	Admin EXEC	Use “duplex” command to change port duplex configuration.	This example shows how to modify port duplex configuration. switch(config)# interface GigabitEthernet 1 switch(config-if)# duplex full switch(config-if)# exit switch(config)# interface GigabitEthernet 2 switch(config-if)# duplex half
`description WORD<1-32>`	Admin EXEC	Use “description” command to give the port a name to identify it easily. If description includes space character, please use double quotes to wrap it.	This example shows how to modify port descriptions. switch(config)# interface GigabitEthernet 1 switch(config-if)# description “uplink port”
`no description`	Admin EXEC	Use no form to restore description to empty string.	imc(config)# interface GigabitEthernet 1 imc(config-if)# no description
`custom (enable)`	Admin EXEC	Use “custom” command to enable customized module configuration.	This example shows how to enable the port custom configuration. imc(config)# interface GigabitEthernet 1 imc(config-if)# custom enable imc(config-if)# exit imc(config-if)#

4.3.2 MAC Address Table

Table 4.2: MAC Address Table

Function	Privilege	Description	Example
`show mac address-table aging-time`	User EXEC	Display the aging time of the address table.	switch# show mac address-table aging-time
`show mac address-table A:B:C:D:E:F [vlan <1-4094>]`	User EXEC	Display entries for a specific MAC address (for all or VLAN).	switch# show mac address-table 0:1:2:3:4:5 vlan 1
`show mac address-table [vlan <1-4094>] [interfaces IF_PORTS]`	User EXEC	View MAC entry on specified interface or VLAN or all dynamic MAC entries in MAC address table.	switch# show mac address-table vlan 1 interface fa5
`show mac address-table dynamic [vlan <1-4094>] [interfaces IF_PORTS]`	User EXEC	View dynamic MAC entry on specified interface or VLAN or all dynamic MAC entries in MAC address table.	switch# show mac address-table dynamic vlan 1 interface fa5
`show mac address-table counters`	User EXEC	Display the number of addresses present in MAC address table.	switch# show mac address-table counters

4.3.3 Jumbo Frame

Table 4.3: Jumbo Frame

Function	Privilege	Description	Example
`jumbo-frame <1518-9216>`	Admin EXEC	Use “jumbo-frame” command to modify maximum frame size. The only way to show this configuration is by using “show running-config” command.	This example shows how to modify maximum frame size to 9216 bytes. switch(config)# jumbo-frame 9216
`no jumbo-frame`	Admin EXEC	Use no form to disable jumbo-frame.	switch(config)# no jumbo-frame

4.3.4 Flow Control

Table 4.4: Flow Control

Function	Privilege	Description	Example
`show flow-control`	User EXEC	Display port flow-control state.	switch# show flow-control
`flowcontrol (off|on)`	Admin EXEC	Use “flow-control” command to change port flow control configuration. Use off form to restore flow control to default (off) configuration.	This example shows how to modify port duplex configuration. switch(config)# interface GigabitEthernet 1 switch(config-if)# flowcontrol on switch(config-if)# flowcontrol off

Table 4.4: Flow Control (Continued)

Function	Privilege	Description	Example
`no flowcontrol`	Admin EXEC	Disable flow control with specified interface.	switch(config-if)# interface GigabitEthernet 1 switch(config-if)# no flowcontrol
`[no] flow-control`	Admin EXEC	Disable or enable flow control.	switch(config)# flow-control switch(config)# no flow-control

4.3.5 VLAN

Table 4.5: VLAN

Function	Privilege	Description	Example
`show vlan-mode`	User EXEC	Display VLAN mode state.	switch# show vlan-mode
`show interfaces IF_PORTS`	User EXEC	Use “show interface” command to show port counters, parameters and status.	switch# show interfaces GigabitEthernet 1
`show interfaces IF_PORTS status`	User EXEC	Use “show interface” command to show port status.	switch# show interfaces GigabitEthernet 1 status
`clear interfaces IF_PORTS counters`	User EXEC	Use "clear interfaces" comand to clear port counters.	switch# clear interfaces GigabitEthernet 1 counters
`show interfaces IF_PORTS statistics`	User EXEC	Use "clear interfaces" comand to show port statistics.	switch# show interfaces GigabitEthernet 1 statistics
`show interfaces switchport IF_PORTS`	User EXEC	Use “show interface switchport” command to show port VLAN status.	switch# show interfaces switchport GigabitEthernet 1
`show management-vlan (allow|priority|tagMode)`	User EXEC	Display information about management VLAN.	switch(config)# show management-vlan allow
`interface [range] IF_PORTS`	Admin EXEC	Use the “interface” [range] command to specify a range of interfaces to which subsequent commands can be applied. With the range keyword, the entered commands are applied to all interfaces within the specified range.	switch(config)# interface GigabitEthernet 1 switch(config)# interface range GigabitEthernet 1
`management-vlan vlan <1-4094>`	Admin EXEC	(1) Set <1-4094> as management VLAN ID; it is recommended to first create the VLAN and then assign the port to it. (2) To view the created management VLAN, use “show management-vlan”.	The following example specifies that management VLAN 2 is created. switch(config)# management-vlan vlan 2
`[no] management-vlan allow ports IF_PORTS`	Admin EXEC	Use the no form of this command to stop the port management address information.	switch(config)# management-vlan allow ports GigabitEthernet 1

Table 4.5: VLAN (Continued)

Function	Privilege	Description	Example
`management-vlan priority <0-7>`	Admin EXEC	This command sets the traffic priority class based on the VLAN value. A priority value of 0 is designated as best effort, while a higher value, such as 5, is considered time-sensitive traffic.	switch(config)# management-vlan prioritiy 0

4.3.6 Q-in-Q

Table 4.6: Q-in-Q

Function	Privilege	Description	Example
`switchport outerpvid <1-4094>`	Admin EXEC	This command configures the hybrid port's Outer PVID. Use "show interface switchport" command to show configuration.	This example sets GI2's Outer PVID to 1024. switch(config)# interface GigabitEthernet 2 switch(config-if)# switchport outerpvid 1024
`switchport outertpid <0x0000-0xFFFF>`	Admin EXEC	This command configures the hybrid port's OuterTPID. Use "show interface switchport" command to show the configuration.	This example sets GI2's Outer TPID to 0x0000. switch(config)# interface GigabitEthernet 2 switch(config-if)# switchport outertpid 0x0000
`switchport qinqmode (nni|uni)`	Admin EXEC	The qinqmode is used to configure the hybrid port for different port roles. Nni: transfer frame will be add outer tag Vlan-Identifier Uni: transfer frame will not be add outer tag Vlan-Identifier.	This example shows how to change GI1 to nni mode and GI2 to uni mode. switch(config)# interface GigabitEthernet 1 switch(config-if)# switchport qinqmode nni switch(config-if)# exit switch(config)# interface GigabitEthernet 2 switch(config-if)# switchport qinqmode uni

4.3.7 LFPT

Table 4.7: LFPT

Function	Privilege	Description	Example
`show lfpt`	User EXEC	Use the "show lfpt" command in Privileged EXEC mode to display the Link Fault Pass Through pairs.	switch# show lfpt
`lfpt port IF_NMLPORT lfptPort IF_NMLPORT`	Admin EXEC	Use the "lfpt port" command in Privileged Admin mode to enable LFPT for the described port.	switch(config)# lfpt port GigabitEthernet 1 lfptPort GigabitEthernet

Table 4.7: LFPT (Continued)

Function	Privilege	Description	Example
`lfpt port IF_NMLPORT lfptPort clear`	Admin EXEC	Use the “lfpt port clear” command in Privileged EXEC mode to reset lfpt port list.	switch(config)# lfpt port GigabitEthernet 1 lfptPort clear

4.3.8 Branch-leaf

Table 4.8: Branch-leaf

Function	Privilege	Description	Example
`show branch-leaf`	User EXEC	Use the “show branch-leaf” command in User mode to display the branch and leaf hierarchy of the configured ports.	switch# show branch-leaf
`branch-leaf status (branch|leaf)`	Admin EXEC	Use the “branch-leaf” command in Privileged EXEC mode to configure specific port configuration for branch and leaf settings.	switch(config)# interface GigabitEthernet 1 switch(config-if)# branch-leaf branch

4.3.9 Operations, Administration, and Maintenance

Table 4.9: OAM

Function	Privilege	Description	Example
`show oam [<1-255>]`	User EXEC	Use the “show oam” command in Privileged EXEC mode to display the Operation, Administration, and Management (OAM) link fault management information for Ethernet interfaces.	switch# show oam
`show oam log`	User EXEC	Use the “show oam log” command in Privileged EXEC mode to display the OAM information log.	switch# show oam log
`[no] oam`	Admin EXEC	Use the “no oam” command in Privileged EXEC mode to disable the OAM operation.	switch(config)# no oam
`oam <1-255> port IF_NMLPORT mode (active | passive)`	Admin EXEC	Use the “oam port IF_NMLPORT mode” command in Privileged EXEC mode to assign the normal port operation an active or passive state.	switch(config)# oam 1 port GigabitEthernet 1 mode active
`no oam <1-255>`	Admin EXEC	Use the “no oam” command in Privileged EXEC mode to disable the designated port <1-255> OAM operation.	switch(config)# no oam 1

Table 4.9: OAM (Continued)

Function	Privilege	Description	Example
`[no] oam <1-255> link-monitor (symbol | frame | frame-period | frame-seconds)`	Admin EXEC	Use the “oam link-monitor” command in Privileged EXEC mode to set error events: error symbols per second, error frames per second, and error frames per second.	switch(config)# oam 1 link-monitor symbol
`oam <1-255> symbol-window <1-1488100>`	Admin EXEC	Use the “oam symbol-window” command in Privileged EXEC mode to set symbol error events that occurred during a specified period exceeding the threshold.	switch(config)# oam 1 symbol-window 2
`oam <1-255> symbol-threshold <0-1024>`	Admin EXEC	Use the “oam symbol-threshold” command in Privileged EXEC mode to configure a period or a value at, above, or below which an action is triggered	switch(config)# oam 1 symbol-threshold 2
`oam <1-255> frame-window <1-60>`	Admin EXEC	Use the “oam frame-window” command in Privileged EXEC mode to set frame-window error events that are observed during a specified period exceeding the threshold.	switch(config)# oam 1 frame-window 2
`oam <1-255> frame-threshold <0-1024>`	Admin EXEC	Use the “oam frame-threshold” command in Privileged EXEC mode to configure a period or a value at, above, or below which an action is triggered.	switch(config)# oam 1 frame-threshold 2
`oam <1-255> frame-period-window <1-89286000>`	Admin EXEC	Use the “oam frame-period-window” command in Privileged EXEC mode to configure a period of time during which symbol error events are counted.	switch(config)# oam 1 frame-period-window 2
`oam <1-255> frame-period-threshold <0-1024>`	Admin EXEC	Use the “oam frame-period-threshold” command in Privileged EXEC mode to configure a frame period or a value at, above, or below which an action is triggered.	switch(config)# oam 1 frame-period-threshold 2
`oam <1-255> frame-seconds-window <10-900>`	Admin EXEC	Use the “oam frame-seconds-window” command in Privileged EXEC mode to configure a period of time in the range 10-900 seconds that is the monitoring period for frames.	switch(config)# oam 1 frame-seconds-window 2

Table 4.9: OAM (Continued)

Function	Privilege	Description	Example
`oam <1-255> frame-seconds-threshold <0-1024>`	Admin EXEC	Use the “oam frame-seconds-threshold” command in Privileged EXEC mode to configure a frame period in seconds which an action is triggered.	switch(config)# oam 1 frame-seconds-threshold 1024
`[no] oam <1-255> function (link-monitor | dying-gasp)`	Admin EXEC	Use the “oam function” command in Privileged EXEC mode to set error events: link monitor (link faults) and dying-gasp (an unrecoverable condition).To disable the command, use the no form.	switch(config)# oam 1 function link-monitor
`oam <1-255> loopback (initiate | terminate)`	Admin EXEC	Use the “oam loopback” command in Privileged EXEC mode to turn on or off remote loopback functionality on an interface.	switch(config)# oam 1 loopback initiate
`[no] oam <1-255> loopback ignore-rx`	Admin EXEC	Use the “oam loopback ignore” command in Privileged EXEC mode to ignore or to process the received remote loopback request. To disable the command, use the no form.	switch(config)# oam 1 ignore-rx
`[no] oam debug (handler | state | action | logic | packet | database | timer | locate)`	Admin EXEC	Use the “oam debug” command in Privileged EXEC mode to enable all Ethernet OAM debugging. To disable the command, use the no form.	switch(config)# oam debug handler

4.3.10 CFM

Table 4.10: CFM

Function	Privilege	Description	Example
`show cfm [mep <1-255>]`	User EXEC	Use the “show cfm” command in Privileged EXEC mode to display information about maintenance end points for peer MEPs.	switch# show cfm mep 2
`show cfm statistics`	User EXEC	Use the “show cfm statistics” command in Privileged EXEC mode to display statistics about maintenance end points for peer MEPs.	switch# show cfm statistics

Table 4.10: CFM (Continued)

Function	Privilege	Description	Example
show cfm hierarchy	User EXEC	Use the "show cfm hierarchy" command in Privileged EXEC mode to display the maintenance level defining the domain hierarchy about maintenance end points for peer MEPs.	switch# show cfm hierarchy
[no] cfm	Admin EXEC	Use the "no cfm" command in Privileged EXEC mode to disable cfm globally.	switch(config)# no cfm
cfm md WORD<1-22> level <0-7>	Admin EXEC	Use the "cfm md" command in Privileged EXEC mode to create a maintenance domain by specifying the name and the name format along with the maintenance level from 0 to 7.	switch(config)# cfm md 2 level 7
no cfm md WORD<1-22>	Admin EXEC	Use the "no cfm md" command in Privileged EXEC mode to disable cfm maintenance domain.	switch(config)# no cfm 2
cfm ma WORD<1-22> md WORD<1-22> interval (100ms | 1s | 10s | 1min | 10min) primary-vlan <1-4094>	Admin EXEC	Use the "cfm ma" command in Privileged EXEC mode to create a maintenance association as part of an MD instance by specifying the name and the name format along with the interval period for sending packets.	switch(config)# cfm ma 2 md 2 interval 10s
no cfm ma WORD<1-22>	Admin EXEC	Use the "no cfm ma" command in Privileged EXEC mode to disable cfm maintenance association.	switch(config)# no cfm ma 2
cfm mep <1-255> ma WORD<1-22>	Admin EXEC	Use the "cfm mep" command in Privileged EXEC mode to create a maintenance association end points at the ends of a maintenance channel.	switch(config)# cfm mep 5 ma 2
no cfm mep <1-255>	Admin EXEC	Use the "no cfm mep" command in Privileged EXEC mode to disable cfm maintenance association end points.	switch(config)# no cfm mep 5
cfm mep <1-255> port IF_NMLPORT	Admin EXEC	Use the "cfm mep" command in Privileged EXEC mode to configure a maintenance association end point to a port if operations is normal.	switch(config)# cfm mep 5 port GigabitEthernet 1

Table 4.10: CFM (Continued)

Function	Privilege	Description	Example
`cfm mep <1-255> direction (down | up)`	Admin EXEC	Use the “cfm mep” command in Privileged EXEC mode to configure the transmission to the bridge trunk direction of a packet. A down MEP indicates that the MEP transmits packets to the physical medium direction, while an up MEP indicates that the MEP transmits packets to the bridge trunk direction.	switch(config)# cfm mep 5 direction down
`[no] cfm mep <1-255> peer-mep <1-255>`	Admin EXEC	Use the “cfm mep peer-mep” command in Privileged EXEC mode to configure a MEP to a specific peer-MEP. To disable the command, use the no form.	switch(config)# cfm mep 5 peer-mep 5
`[no] cfm mep <1-255> enable (cc | lb)`	Admin EXEC	Use the “cfm mep” command in Privileged EXEC mode to enable a MEP specific alarm or loopback. To disable the command, use the no form.	switch(config)# cfm mep 5 enable cc
`cfm mep <1-255> start lb`	Admin EXEC	Use the “cfm mep” command in Privileged EXEC mode to start a remote loopback test.	switch(config)# cfm mep 5 start lb
`cfm mep <1-255> start lb peer-mep <1-255>`	Admin EXEC	Use the “cfm mep” command in Privileged EXEC mode to start a loopback with its peer MEP.	switch(config)# cfm mep 5 start lb peer-mep 5
`[no] cfm debug (handler | state | action | logic | packet | database | timer | identify)`	Admin EXEC	Use the “cfm debug” command in Privileged EXEC mode to enable CFM debug messages. To disable the command, use the no form.	switch(config)# cfm debug handler

4.4 QoS

4.4.1 Rate Limit

Table 4.11: Rate Limit

Function	Privilege	Description	Example
`show rate-limit`	User EXEC	Display rate-limit information.	switch# show rate-limit
`show rate-limit interfaces IF_PORTS`	User EXEC	Display rate-limit information in specified interface.	switch# show rate-limit interfaces GigabitEthernet 5

Table 4.11: Rate Limit (Continued)

Function	Privilege	Description	Example
`rate-limit ingress <16-1000000>`	Admin EXEC	Use the “rate-limit ingress” command in Privileged EXEC mode to set ingress rate-limit.	switch(config-if)# rate-limit ingress 10000
`no rate-limit ingress`	Admin EXEC	Use the “no rate-limit ingress” command in Privileged EXEC mode to disable the ingress rate limit.	switch(config-if)# no rate-limit ingress
`rate-limit egress <16-1000000>`	Admin EXEC	Use the “rate-limit egress” command in Privileged EXEC mode to set egress rate-limit.	switch(config-if)# rate-limit egress 10000
`[no] rate-limit`	Admin EXEC	Use the “no rate-limit” command in Privileged EXEC mode to disable the rate limit globally.	switch(config)# rate-limit
`no rate-limit egress`	Admin EXEC	Use the “no rate-limit egress” command in Privileged EXEC mode to disable the egress rate limit.	switch(config-if)# no rate-limit egress
`rate-limit egress queue <1-8> <16-1000000>`	Admin EXEC	Use the “rate-limit egress queue” command in Privileged EXEC mode to set egress queue rate-limits.	switch(config-if)# rate-limit egress queue 3 10000
`no rate-limit egress queue <1-8>`	Admin EXEC	Use the “rate-limit egress queue” command in Privileged EXEC mode to remove the egress rate-limit in queue.	switch(config-if)# no rate-limit egress queue 3

4.5 Security

4.5.1 Account Manager

Table 4.12: Account Manager

Function	Privilege	Description	Example
`show username`	User EXEC	Show all user accounts in local database.	switch# show username
`show users`	User EXEC	Show all user information.	switch# show users
`show privilege`	User EXEC	Show current privilege level.	switch# show privilege
`username WORD<0-32> [privilege (admin|user)|password WORD<0-32>|(secret (encrypted|PASSWORD)|nopassword`	Admin EXEC	Use “username” command to add a new user account or edit an existing user account.	switch(config)# username test privilege admin secret 1234

Table 4.12: Account Manager (Continued)

Function	Privilege	Description	Example
`no username WORD<0-32>`	Admin EXEC	Delete an existing user account.	switch(config)# no username test
`enable (password | (secret [encrypted|PASSWORD]))`	Admin EXEC	Use “enable” command to enable a password or encrypted password for each privilege level for authentication.	switch(config)# enable secret 1234
`no enable`	Admin EXEC	Restore enable password to default empty value.	switch(config)# no enable

4.6 Management

4.6.1 IP Management

Table 4.13: IP Management

Function	Privilege	Description	Example
`show ip`	User EXEC	Show system IPv4 address, net mask and default gateway.	switch# show ip
`show ip dhcp`	User EXEC	Show IPv4 DHCP client enable state.	switch# show ip dhcp
`[no] ip dhcp`	Admin EXEC	Use “IP DHCP” command to enable DHCP client to get IP address from remote DHCP server. Use “No IP DHCP” command to disable DHCP client and use static IP address.	switch(config)# ip dhcp switch(config)# no ip dhcp
`ip address A.B.C.D [mask A.B.C.D]`	Admin EXEC	Modify administration IPv4 address.	switch(config)# ip address 192.168.1.200 mask 255.255.255.0
`ip default-gateway A.B.C.D`	Admin EXEC	Modify default gateway address.	switch(config)# ip default-gateway 192.168.1.100

4.6.2 SNMP

Table 4.14: SNMP

Function	Privilege	Description	Example
`show snmp`	User EXEC	Display SNMP state.	switch# show snmp
`show snmp trap`	User EXEC	Display SNMP trap setting.	switch# show snmp trap
`[no] snmp`	Admin EXEC	Enable or disabled SNMP engine.	switch# configure switch(config)# snmp
`[no] snmp trap (auth|linkUpDown|warm-start|cold-start|port-security)`	Admin EXEC	Specify SNMP trap setting.	switch# configure switch(config)# snmp trap auth

Table 4.14: SNMP (Continued)

Function	Privilege	Description	Example
`snmp community NAME (ro|rw)`	Admin EXEC	SNMP v1/v2 community name. SNMP community read or readwrite attribute for basic mode.	switch# configure switch(config)# snmp community user rw
`no snmp community NAME`	Admin EXEC	Delete SNMP community name.	switch# configure switch(config)# no snmp community user
`snmp host (A.B.C.D|X:X::X:X|HOSTNAME) [version (1|2c)] NAME`	Admin EXEC	SNMP trap host IPv4/IPv6 address or host name. v1/v2c/v3 traps. SNMP community name or user name.	switch# configure switch(config)# snmp host 192.168.1.100 version 2c private
`no snmp host (A.B.C.D|X:X::X:X|HOSTNAME) [version (1|2c)]`	Admin EXEC	Delete SNMP host.	switch# configure switch(config)# no snmp host 192.168.1.100 version 2c

4.6.3 Configuration Management

Table 4.15: Configuration Management

Function	Privilege	Description	Example
`show (startup-config|running-config)`	Admin EXEC	Show startup/running configuration.	switch# show startup-config switch# show running-config
`show running-config interfaces IF_PORTS`	Admin EXEC	Show running configuration on selected ports.	switch# show running-config interfaces GigabitEthernet 1
`copy startup-config <running-config | tftp://)`	Admin EXEC	Copy startup configuration to the running configuration to merge with current system configuration or to a remote tftp server.	switch# copy startup-config running-config
`copy running-config (startup-config|tftp://)`	Admin EXEC	Copy running configuration to startup configuration.	switch# copy running-config startup-config
`copy custom-config (tftp://)`	Admin EXEC	Copy custom configuration to remote tftp server.	switch# copy custom-config tftp://192.168.1.111/test1.cfg
`copy flash:// (flash://|tftp://)`	Admin EXEC	Copy flash configuration to flash file system or remote tftp server.	switch# copy custom-config tftp://192.168.1.111/test1.cfg
`copy tftp:// (running-config|startup-config|custom-config)`	Admin EXEC	Upgrade running/startup configuration from remote tftp server.	switch# copy tftp:// 192.168.1.111/test2.cfg startup-config
`delete <custom-config|flash:// |startup-config | system)`	Admin EXEC	Restore factory defaults, equal to command “restore-defaults”.	switch# delete custom-config

Table 4.15: Configuration Management (Continued)

Function	Privilege	Description	Example
`reset [except for]`	Admin EXEC	Use the “reset” command in Privileged EXEC mode to restore factory default of all system and keep some settings.	switch# reset except for [settings]
`save`	Admin EXEC	Use “save” command to save the current configuration.	switch# save

4.6.4 Firmware Management

Table 4.16: Firmware Management

Function	Privilege	Description	Example
`boot system (image0|image1)`	Admin EXEC	Dual image stores a backup image in the flash partition. Use “boot system” command to select the active firmware image. The other firmware image will become a backup.	switch(config)# boot system image1
`delete system (image0|image1)`	Admin EXEC	Delete firmware image stored in flash.	switch# delete system image1
`copy (flash://|tftp://) (flash://|tftp://)`	Admin EXEC	Upgrade/backup firmware image from/to remote tftp server.	switch# copy tftp://192.168.1.100/vmlinux.bix flash://image0

4.6.5 System Log (SYSLOG)

Table 4.17: System Log (SYSLOG)

Function	Privilege	Description	Example
`show logging`	User EXEC	Display the global logging status.	switch# show logging
`show logging (buffered|file)`	User EXEC	Display log of buffer or file.	switch# show logging buffered
`clear logging (buffered|file)`	Admin EXEC	Clear logging information.	switch# clear logging buffered
`[no] logging`	Admin EXEC	Disable or enable logging service.	switch(config)# logging
`logging host (A.B.C.D|HOSTNAME) [port <0-65535>] [severity <0-7>] [facility (local0|local1|local2|local3|local4|local5|local6|local7)]`	Admin EXEC	Set remote log server information and specify the minimum severity mask and facility of logging message.	switch(config)# logging host 192.168.1.100 severity 6 facility local0

Table 4.17: System Log (SYSLOG) (Continued)

Function	Privilege	Description	Example
`logging ((buffered|console |file) [severity <0-7>]|host (A.B.C.D|HOSTNAME) )`	Admin EXEC	Enable logging into buffer or console of file and specify the minimum severity mask of logging message.	switch(config)# logging buffered severity 6
`no logging (buffered|console| file)`	Admin EXEC	Disable logging into buffer or console or file.	switch(config)# no logging buffered
`no logging host (A.B.C.D|HOSTNAME)`	Admin EXEC	Remove remote log server.	switch(config)# no logging host 192.168.1.100

4.6.6 IP Configuration

Table 4.18: IP Configuration

Function	Privilege	Description	Example
`ip address A.B.C.D [mask A.B.C.D]`	Admin EXEC	Use “IP address” command to modify administration IPv4 address.	switch(config)# ip address 192.168.1.200 mask 255.255.255.0
`ip default-gateway A.B.C.D`	Admin EXEC	Use “IP default-gateway” command to modify default gateway address.	switch(config)# ip default-gateway 192.168.1.100
`no ip default-gateway`	Admin EXEC	Use “No IP default-gateway” to restore default gateway address to factory default.	switch(config)# no ip default-gateway

4.6.7 TELNET

Table 4.19: TELNET

Function	Privilege	Description	Example
`ip telnet`	Admin EXEC	Use “IP telnet” command to enable telnet services.	switch(config)# ip telnet
`[no] ip telnet`	Admin EXEC	Use no ip telnet to disable service.	switch(config)# no ip telnet

4.6.8 HTTP

Table 4.20: HTTP

Function	Privilege	Description	Example
`ip http`	Admin EXEC	Use "IP http" command to enable http services.	switch(config)# ip http
`ip https`	Admin EXEC	Use "IP https" command to enable https services.	switch(config)# ip https
`[no] ip http`	Admin EXEC	Use no ip http to disable service.	switch(config)# no ip http
`[no] ip https`	Admin EXEC	Use no ip https to disable service.	switch(config)# no ip http

Table 4.20: HTTP (Continued)

Function	Privilege	Description	Example
`show ip (http|https)`	User EXEC	Show current https or http service information.	switch# show ip https
`ip (http|https) session-timeout <0-86400>`	Admin EXEC	Use “IP session-timeout” command to specify the session timeout value for http or https service.	switch(config)# ip http session-timeout 15 switch(config)# ip https session-timeout 20

4.7 Diagnostic

4.7.1 DMI

Table 4.21: DMI

Function	Privilege	Description	Example
`show dmi IF_PORTS information`	Admin EXEC	Use this command to display the information of EEPROM and Digital Diagnostic Monitoring Interface in SFP Optical Transceivers.	switch# show dmi GigabitEthernet 1 information
`[no] dmi (alarm|warning) (temperature|voltag|txbasis|txpower|rxpower) (high|low) state`	Admin EXEC	Use this command to enable/disable the mechanism that monitors SFP Optical Transceiver's Digital Diagnostic Monitoring interface information. Use no form to disable warning/alarm mechanism.	This example shows how to enable temperature's high threshold monitor mechanism with alarm level. (Current sfp plug-in in fa10). switch(config)# interface GigabitEthernet 2 switch(config-if)# dmi alarm temperature high state
`dmi (alarm|warning) (temperature|voltag|txbasis|txpower|rxpower) (high|low) value INPUT_VALUE`	Admin EXEC	Use this command to configure high/low threshold value used to compare with SFP Optical Transceiver's Digital Diagnostic Monitoring interface's value (temperature, voltage, etc).	This example shows how to configure the temperature high threshold value is 30.5 with alarm level. switch(config-if)# dmi alarm temperature high value 30.5
`[no] dmi alarm-warning message (log|snmp)`	Admin EXEC	Use this command to determine which method to use when notifying of user alarm/warning events.	This example shows how to configure alarm-warning message is system log. switch(config)# dmi alarm-warning message log

4.7.2 IP-based Diagnostic

Table 4.22: IP-based Diagnostic

Function	Privilege	Description	Example
`ping HOSTNAME [count <1-5>] [interval <1-5>] [size <8-5120>]`	User EXEC	Use “ping” command to do network ping diagnostic.	switch# ping 192.168.1.100 count 4 interval 4 size 128

4.7.3 System

Table 4.23: System

Function	Privilege	Description	Example
`show version`	User EXEC	Use “show version” command to show loader and firmware version and build date.	switch# show version
`show info`	User EXEC	Use “show info” command to show system summary information.	switch# show info
`reboot`	Admin EXEC	Use “reboot” command to make system hot restart.	switch# reboot
`show language`	User EXEC	Use “show language” command to show system language.	switch# language
`language (english | chinese)`	User EXEC	Use “language” command to set language.	switch(config)# language english
`exit`	User EXEC	Use “exit” to exit the device system.	switch(config)# exit
`show flash`	User EXEC	Use “show flash” command to show all files status which stored in flash.	switch# show flash
`clear line telnet`	Admin EXEC	Use “clear line” command in Privileged EXEC mode to disconnect a Telnet session.	switch# clear line telnet
`terminal length <0-24>`	User EXEC	Use “terminal length” command in Privileged EXEC mode to modify the terminal print length.	switch# terminal length 20
`system name NAME`	Admin EXEC	Use “system name” command to modify system name information of the switch.	switch(config)# system name myname
`system contact CONTACT`	Admin EXEC	Use “system contact” command to modify contact information of the switch.	switch(config)# system contact callme
`system contact CONTACT`	Admin EXEC	Use “system location” command to modify location information of the switch.	switch(config)# system location home
`system prompt (default | sys-name | sys-location | sys-contact)`	Admin EXEC	Use “system prompt” command to modify prompt of the switch.	switch(config)# system prompt default

Chapter 5

iView^2

5.1 iView^2 Management Software

iView^2 is the Advantech management software that features a Graphical User Interface (GUI) and gives network managers the ability to monitor and control manageable Advantech products.

iView^2 is available in several versions: Windows desktop version, WebServer version 3.0, and can also function as a snap-in module for HP OpenView Network Node Manager and other third party SNMP management software.

iView^2 supports the following platforms: Windows 2000, XP, Vista, 7.

Note! *For assistance in selecting the right version of iView^2 for a specific operating system, please visit the Advantech website or contact Technical Support.*

5.1.1 iView^2 (iConfig View)

iView^2 (iConfig view) is an in-band utility created by Advantech that is used for SNMP configuration for Advantech' SNMP manageable devices.

iView^2 (iConfig view) allows the following actions:

- Set an IP address, subnet mask and default gateway.
- Define community strings and SNMP Traps.

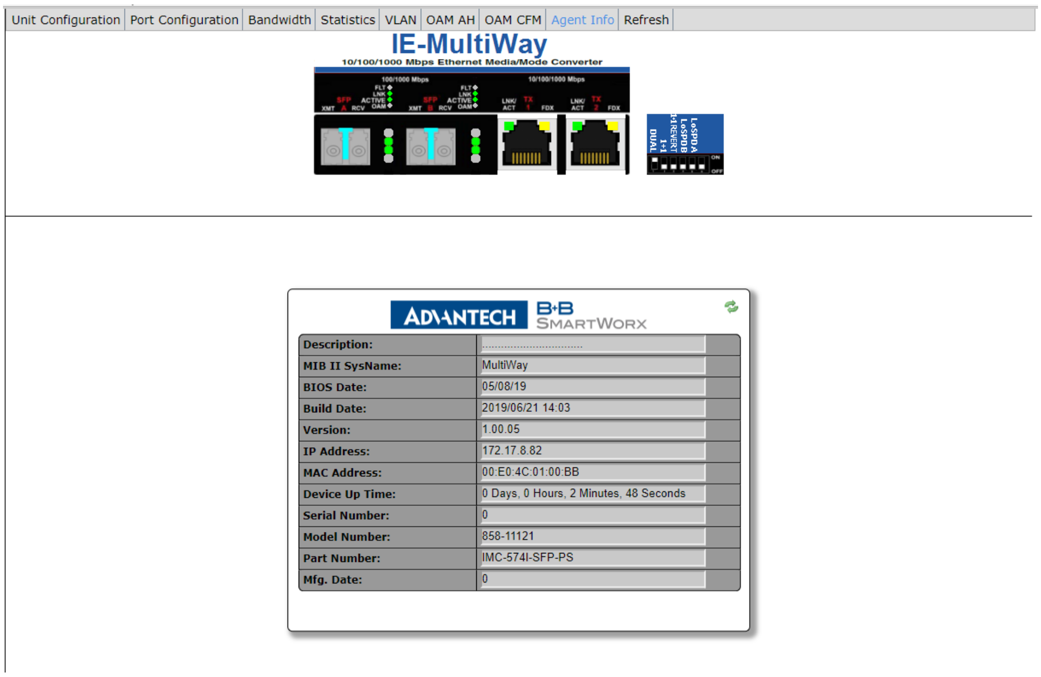
iView^2 (iConfig view) also includes an authorized IP address system and restricted access to MIB groups which are supported by Advantech' manageable devices. These extra layers of security do not affect SNMP compatibility. iView^2 (iConfig view) can upload new versions of the system software and new MIB information. It also includes diagnostic capabilities for faster resolution of technical support issues.

5.2 Using iView^2

iView^2 is Advantech' management software, providing network management in an easy to use GUI. Once iView^2 is installed on a network management PC using a Windows operating system, use the **Start** menu to access iView^2. iView^2 is available in a desktop or WebServer version.

Note! *Windows SNMP services must be installed to receive traps.*

The autoscan feature of iView^2 will detect Advantech' devices on an active subnet and list them in the network outline. Click the connection for the IMC-574I-SFP to open its iView^2 screen. To perform additional configuration, select the iView^2 iConfig view icon on the toolbar in iView^2. This allows a session to be launched, and the default password/username is admin/admin. Additional private usernames and passwords can be entered in the **USERS** tab. If the list of passwords is not maintained, the usernames and passwords can be reset by opening a CLI session and typing in the cleandb command. This will reset all but the IP address of the device.



Description:	....
MIB II SysName:	MultiWay
BIOS Date:	05/08/19
Build Date:	2019/06/21 14:03
Version:	1.00.05
IP Address:	172.17.8.82
MAC Address:	00:E0:4C:01:00:BB
Device Up Time:	0 Days, 0 Hours, 2 Minutes, 48 Seconds
Serial Number:	0
Model Number:	858-11121
Part Number:	IMC-574I-SFP-PS
Mfg. Date:	0

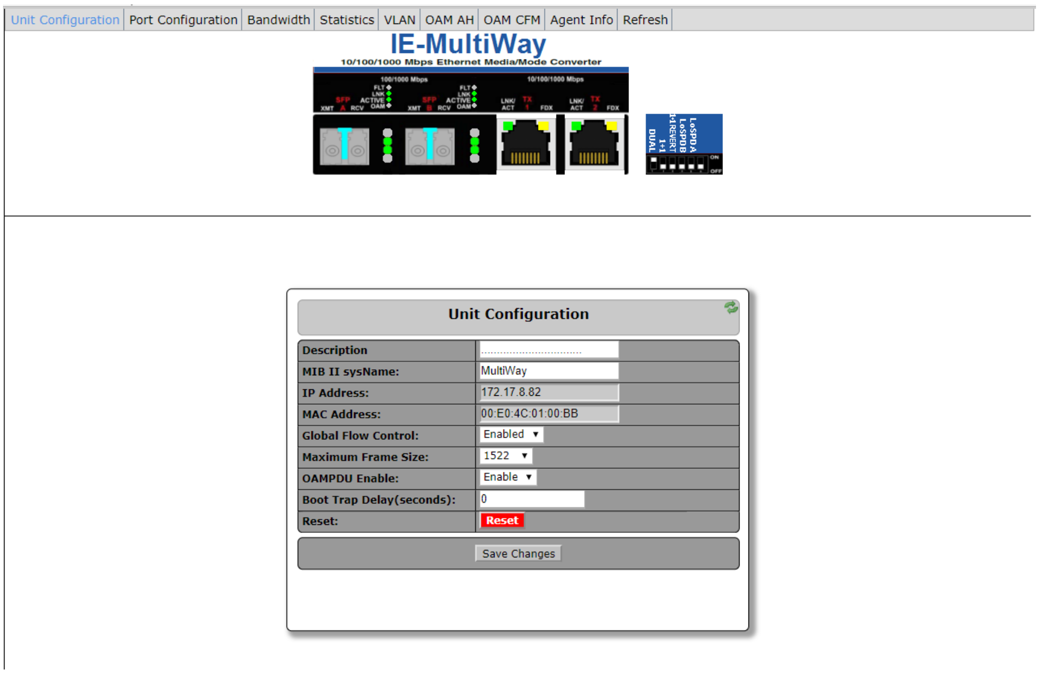
Figure 5.1 iView^2 Main Menu

The following functions can be performed via iView^2:

Function	Description
Unit Configuration	Display/modify unit information.
Port Configuration	Display/modify port data.
Bandwidth	Displays settings for bandwidth configuration.
Statistics	Display statistics tables, including unit and port tables, RMON statistics, MIB-II ifTable and SFP Info.
VLAN	Provides configuration for VLAN IDs per port.
OAM AH	Configure passive and active 802.3ah.
OAM CFM	Perform administrative configuration functions.
Agent Info	Displays SNMP agent data.
Refresh	Soft reboot to the system.

5.3 Unit Configuration

Select **Unit Configuration** to display/modify unit information including IP address (display only, modification not allowed), global flow control, maximum frame size and OAMPDU.



Unit Configuration

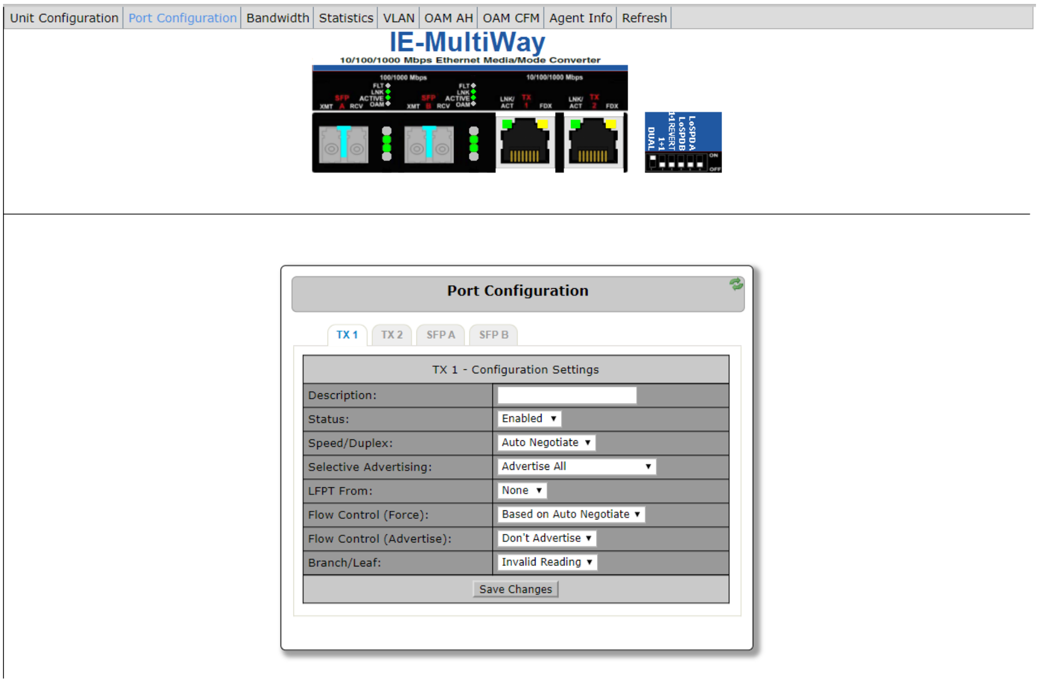
Description	....
MIB II sysName:	MultiWay
IP Address:	172.17.8.82
MAC Address:	00:E0:4C:01:00:BB
Global Flow Control:	Enabled ▾
Maximum Frame Size:	1522 ▾
OAMPDU Enable:	Enable ▾
Boot Trap Delay(seconds):	0
Reset:	Reset

Figure 5.2 Unit Configuration

Note! *Entering a descriptor in the Description field can make it easier to track down the source of a Trap.*

5.4 Port Configuration

Select **Port Configuration** to display/modify port information including description and flow control.



Port Configuration

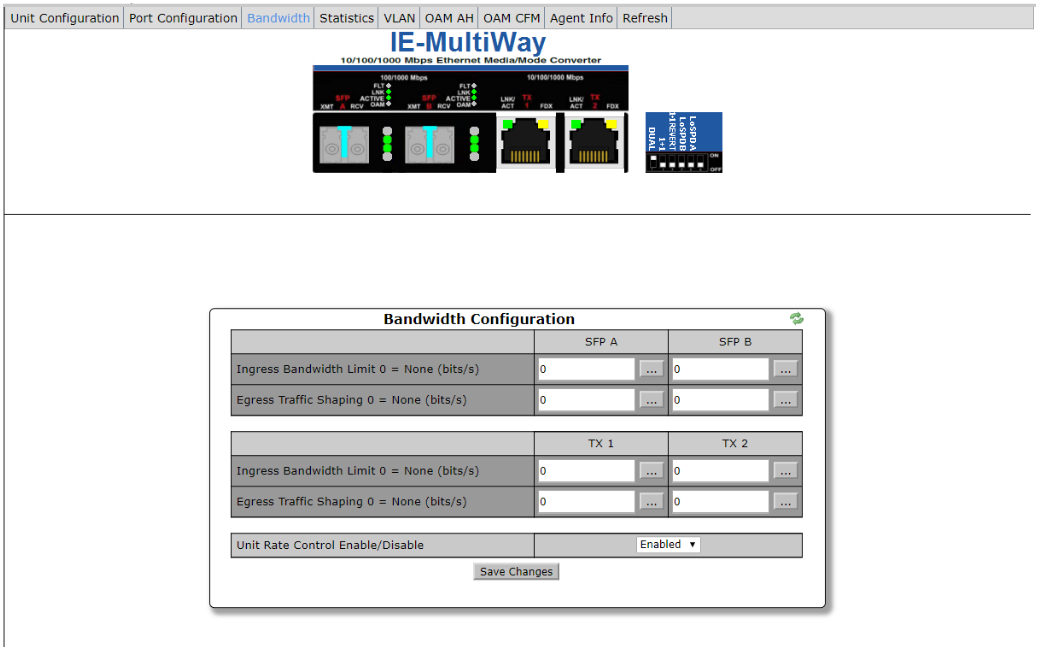
TX 1 - Configuration Settings	
Description:	
Status:	Enabled
Speed/Duplex:	Auto Negotiate
Selective Advertising:	Advertise All
LFPT From:	None
Flow Control (Force):	Based on Auto Negotiate
Flow Control (Advertise):	Don't Advertise
Branch/Leaf:	Invalid Reading

Figure 5.3 Port Configuration

Branch/Leaf: This option allows the end user to ensure that ports cannot directly talk to one another. One port must be selected to be the Branch, and at least two other ports as a Leaf. Each Leaf port can talk to the Branch, but cannot directly talk to each other.

5.5 Bandwidth

Select **Bandwidth** to display configure bandwidth settings for each port.



Bandwidth Configuration

	SFP A	SFP B
Ingress Bandwidth Limit 0 = None (bits/s)	0	0
Egress Traffic Shaping 0 = None (bits/s)	0	0

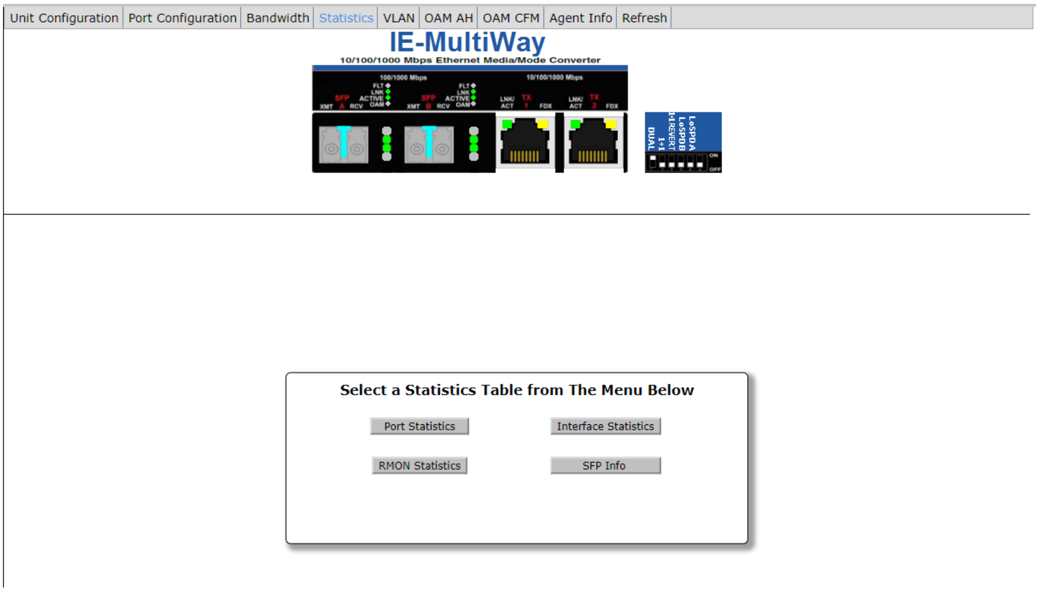
	TX 1	TX 2
Ingress Bandwidth Limit 0 = None (bits/s)	0	0
Egress Traffic Shaping 0 = None (bits/s)	0	0

Unit Rate Control Enable/Disable	Enabled

Figure 5.4 Bandwidth

5.6 Statistics

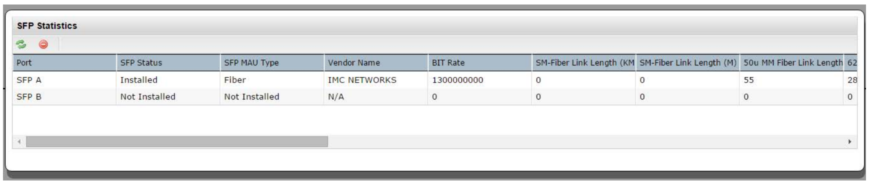
Select **Statistics** to display a screen and select specific statistics to view.



Select a Statistics Table from The Menu Below

Figure 5.5 Statistics

Select Statistics to access the SFP table to display the following information.


SFP Statistics

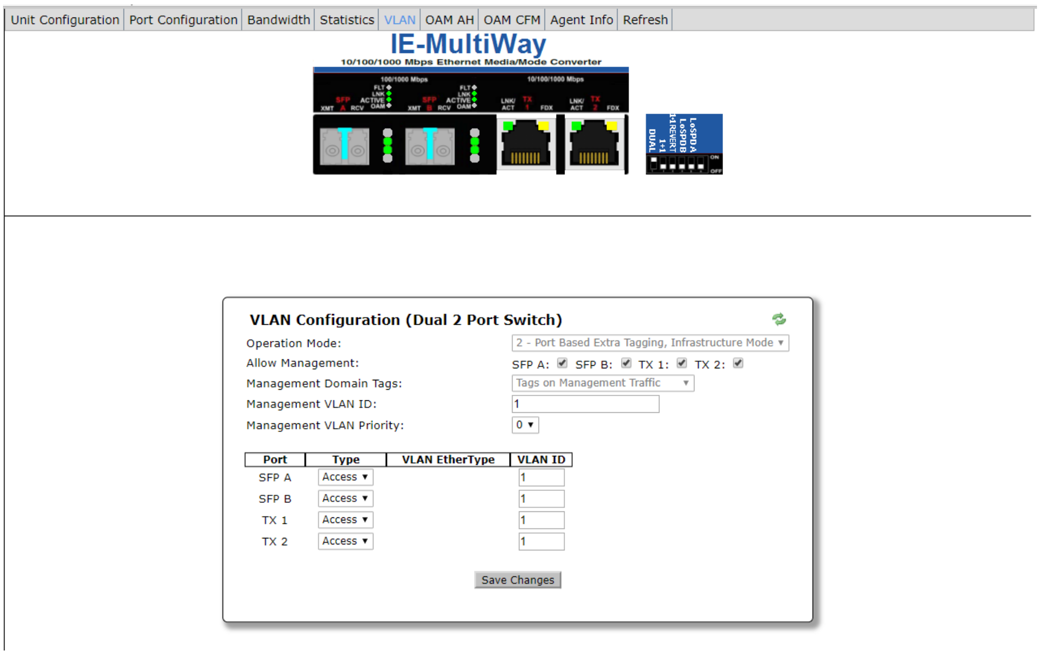
Port	SFP Status	SFP MAU Type	Vendor Name	BIT Rate	SM-Fiber Link Length (KM	SM-Fiber Link Length (M)	50u MM Fiber Link Length	62
SFP A	Installed	Fiber	IMC NETWORKS	1300000000	0	0	55	28
SFP B	Not Installed	Not Installed	N/A	0	0	0	0	0

Figure 5.6 SFP Statistics

5.7 VLAN

Select **VLAN** to display/modify VLAN information.

Enter a VLAN ID between 1 and 4094; possible priority settings are 0 (lowest priority) through 7 (highest priority).



VLAN Configuration (Dual 2 Port Switch)

Operation Mode: 2 - Port Based Extra Tagging, Infrastructure Mode ▾

Allow Management: SFP A: ☑ SFP B: ☑ TX 1: ☑ TX 2: ☑

Management Domain Tags: Tags on Management Traffic ▾

Management VLAN ID: 1

Management VLAN Priority: 0 ▾

Port	Type	VLAN EtherType	VLAN ID
SFP A	Access ▾		1
SFP B	Access ▾		1
TX 1	Access ▾		1
TX 2	Access ▾		1

Figure 5.7 VLAN

This screen also allows you to set up each port as a Trunk or Access port.

- A Trunk port will allow multiple VLANs to be transported.
- An Access port will allow one VLAN to be transported.

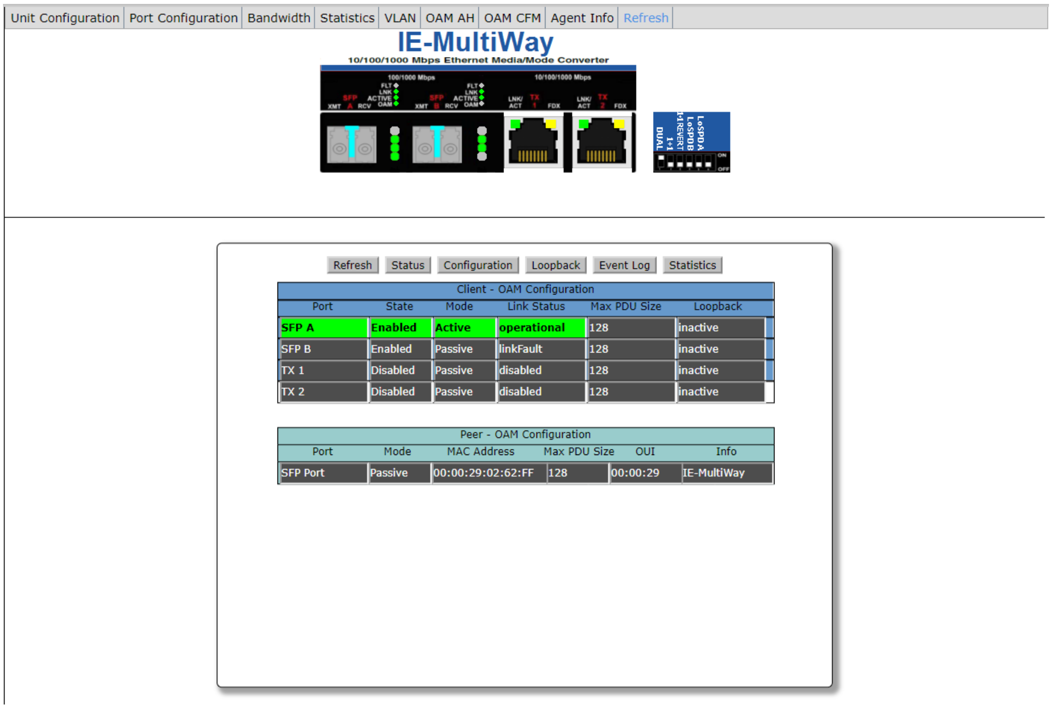
5.7.1 L2PT, Layer 2 Protocol Tunneling

This is a mechanism (L2PT) for sending frames from various protocols across a cloud. This mechanism will modify protocols, such as CDP and others, in order for the cloud to become transparent to the protocols. Firmware version B0 supports this feature. L2PT is enabled on a per-port basis in VLAN mode 2. In this mode, ports are defined as either Trunks or Access. Access ports have a switch that enables/disables L2PT.

Warning! *If a VLAN # is added to a port and is the same VLAN # assigned for a tag on management traffic, saving these changes will disrupt management indefinitely.*

5.8 OAM AH

Select **OAM AH** to display the following screen and monitor the status, configuration, loopback, event log and statistics.

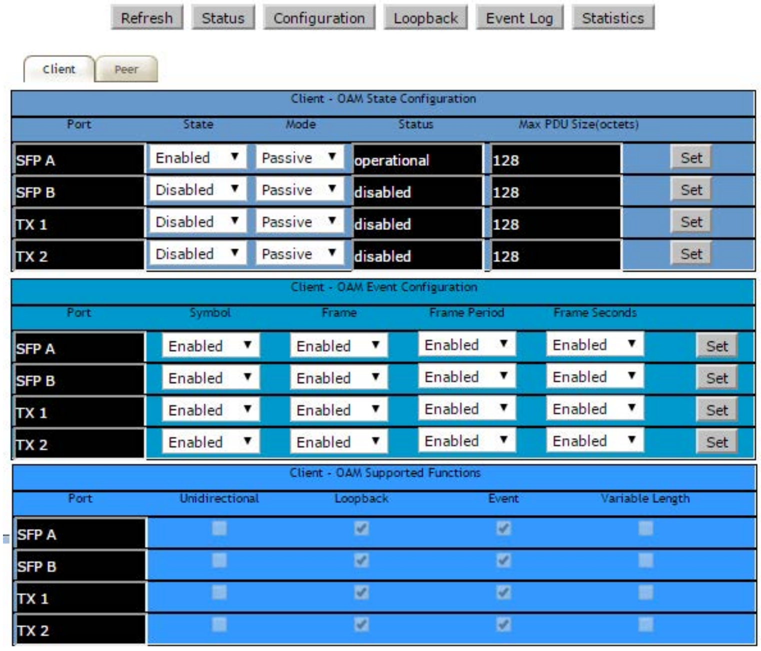


Client - OAM Configuration					
Port	State	Mode	Link Status	Max PDU Size	Loopback
SFP A	Enabled	Active	operational	128	inactive
SFP B	Enabled	Passive	linkFault	128	inactive
TX 1	Disabled	Passive	disabled	128	inactive
TX 2	Disabled	Passive	disabled	128	inactive

Peer - OAM Configuration					
Port	Mode	MAC Address	Max PDU Size	OUI	Info
SFP Port	Passive	00:00:29:02:62:FF	128	00:00:29	IE-MultiWay

Figure 5.8 OAM AH

From the above screen, select **Configuration** to display state and event configuration information as well as OAM supported functions:



Client - OAM State Configuration

Port	State	Mode	Status	Max PDU Size(octets)	
SFP A	Enabled	Passive	operational	128	Set
SFP B	Disabled	Passive	disabled	128	Set
TX 1	Disabled	Passive	disabled	128	Set
TX 2	Disabled	Passive	disabled	128	Set

Client - OAM Event Configuration

Port	Symbol	Frame	Frame Period	Frame Seconds	
SFP A	Enabled	Enabled	Enabled	Enabled	Set
SFP B	Enabled	Enabled	Enabled	Enabled	Set
TX 1	Enabled	Enabled	Enabled	Enabled	Set
TX 2	Enabled	Enabled	Enabled	Enabled	Set

Client - OAM Supported Functions

Port	Unidirectional	Loopback	Event	Variable Length
SFP A	□	☑	☑	□
SFP B	□	☑	☑	□
TX 1	□	☑	☑	□
TX 2	□	☑	☑	□

Figure 5.9 OAM AH > Configuration

5.8.1 Loopback Testing

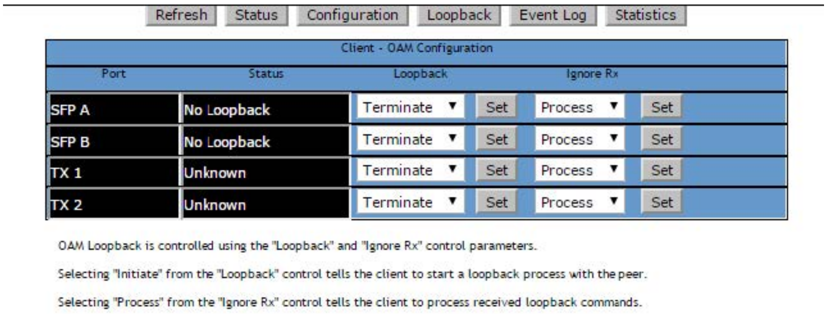
The IMC-574I-SFP includes Loopback testing functionality. This feature is selectable via iView^2 within the OAM AH configuration. The menu choices for all ports includes:

- Terminate/initiate
- Process/ignore

OAM Loopback is controlled by using the **Loopback** and **Ignore Rx** control parameters. Selecting **Initiate** from the **Loopback** drop-down menu tells the client to start a loopback process with the peer. Selecting **Process** from the **Ignore Rx** drop-down menu tells the client to process received loopback commands.

Only AH "Active" units can send a Loopback command to a remote unit. Either Active or Passive AH units can respond to a Loopback command, but must be configured to process these commands or they will be ignored.

Select **Loopback** to display loopback data and define how loopback is configured:



Client - OAM Configuration

Port	Status	Loopback		Ignore Rx	
SFP A	No Loopback	Terminate	Set	Process	Set
SFP B	No Loopback	Terminate	Set	Process	Set
TX 1	Unknown	Terminate	Set	Process	Set
TX 2	Unknown	Terminate	Set	Process	Set

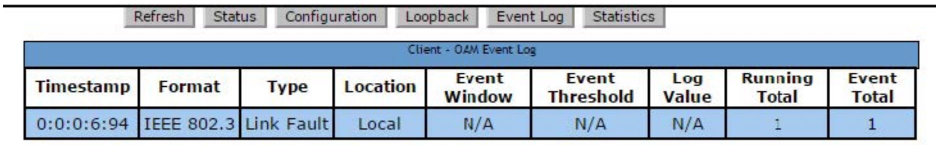
OAM Loopback is controlled using the "Loopback" and "Ignore Rx" control parameters.

Selecting "Initiate" from the "Loopback" control tells the client to start a loopback process with the peer.

Selecting "Process" from the "Ignore Rx" control tells the client to process received loopback commands.

Figure 5.10 OAM AH > Loopback

Select **Event Log** to display the OAM event log showing fault changes that have occurred via OAM configuration.

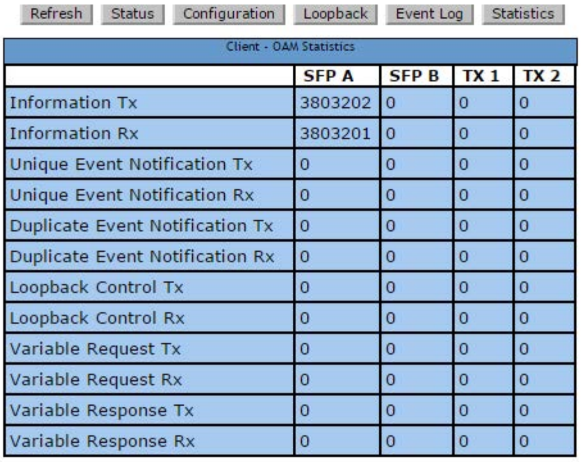


Client - OAM Event Log

Timestamp	Format	Type	Location	Event Window	Event Threshold	Log Value	Running Total	Event Total
0:0:0:6:94	IEEE 802.3	Link Fault	Local	N/A	N/A	N/A	1	1

Figure 5.11 OAM AH > Event Log

Select **Statistics** to display OAM statistics.



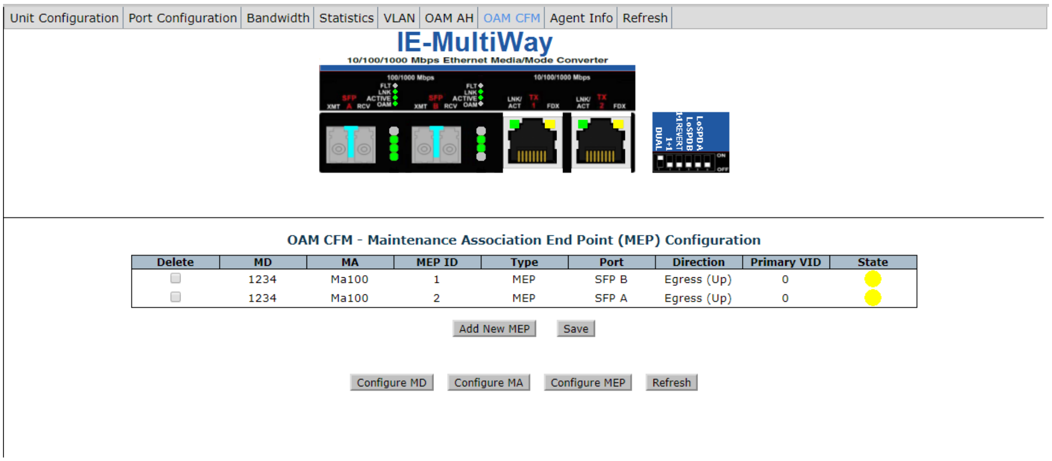
Client - OAM Statistics

	SFP A	SFP B	TX 1	TX 2
Information Tx	3803202	0	0	0
Information Rx	3803201	0	0	0
Unique Event Notification Tx	0	0	0	0
Unique Event Notification Rx	0	0	0	0
Duplicate Event Notification Tx	0	0	0	0
Duplicate Event Notification Rx	0	0	0	0
Loopback Control Tx	0	0	0	0
Loopback Control Rx	0	0	0	0
Variable Request Tx	0	0	0	0
Variable Request Rx	0	0	0	0
Variable Response Tx	0	0	0	0
Variable Response Rx	0	0	0	0

Figure 5.12 OAM AH > Statistics

5.9 OAM CFM

Select **OAM CFM** to display the following screen and perform administrative control for Maintenance Domains (MDs), Maintenance Associations (MAs) and Maintenance Association End Points (MEPs). The page contains a list of the local MEPs and provides menu controls to access the administrative functions associated with Create, Delete, and List MD, MA, and MEP information. An example of a default OAM CFM Configuration page is shown below.



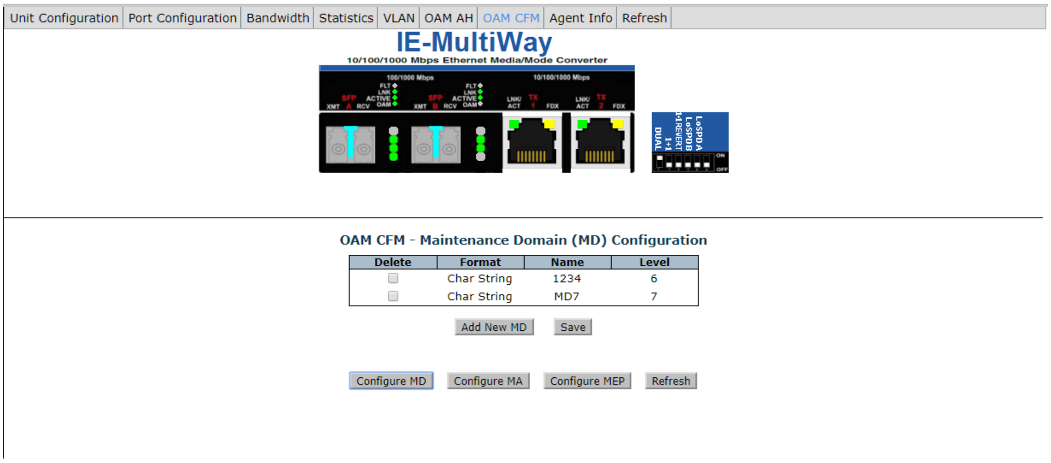
OAM CFM - Maintenance Association End Point (MEP) Configuration

Delete	MD	MA	MEP ID	Type	Port	Direction	Primary VID	State
□	1234	Ma100	1	MEP	SFP B	Egress (Up)	0	●
□	1234	Ma100	2	MEP	SFP A	Egress (Up)	0	●

Figure 5.13 OAM CFM

The OAM CFM Configuration page defaults to the “Configure MEP” selections.

For the first-time configuration, the user must first create an MD, then an MA, then local and peer MEPs can be added. To create an MD, click the **Configure MD** button to display the OAM CFM Maintenance Domain Configuration page as shown below.



OAM CFM - Maintenance Domain (MD) Configuration

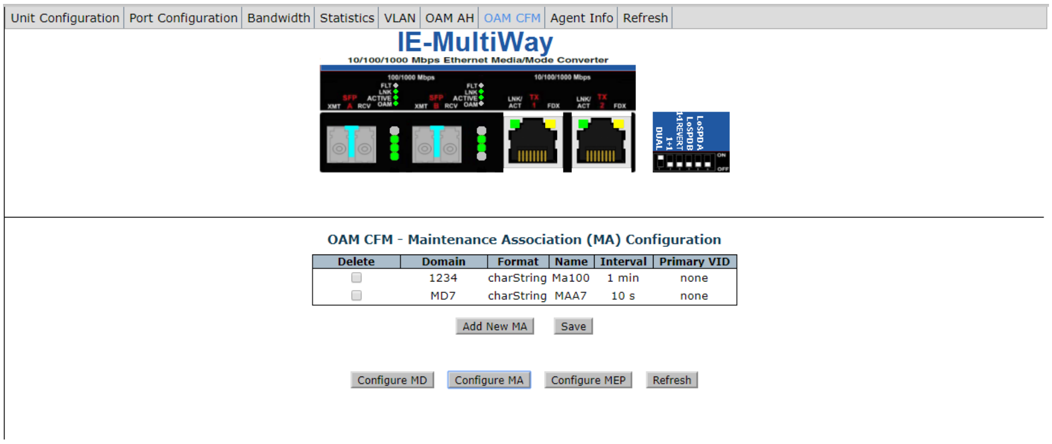
Delete	Format	Name	Level
□	Char String	1234	6
□	Char String	MD7	7

Figure 5.14 OAM CFM > Configure MD

Note! *iView^2 will automatically display this page if there is no MD yet defined when the user attempts to access any other menu control.*

Enter the MD name and select the level for the domain. To cancel the MD, select Delete. To store the MD, press Save and the screen is refreshed.

For the first configuration, create an MA after the MD. Select **Configure MA** to display the OAM CFM Maintenance Association Configuration screen as shown below.



OAM CFM - Maintenance Association (MA) Configuration

Delete	Domain	Format	Name	Interval	Primary VID
□	1234	charString	Ma100	1 min	none
□	MD7	charString	MAA7	10 s	none

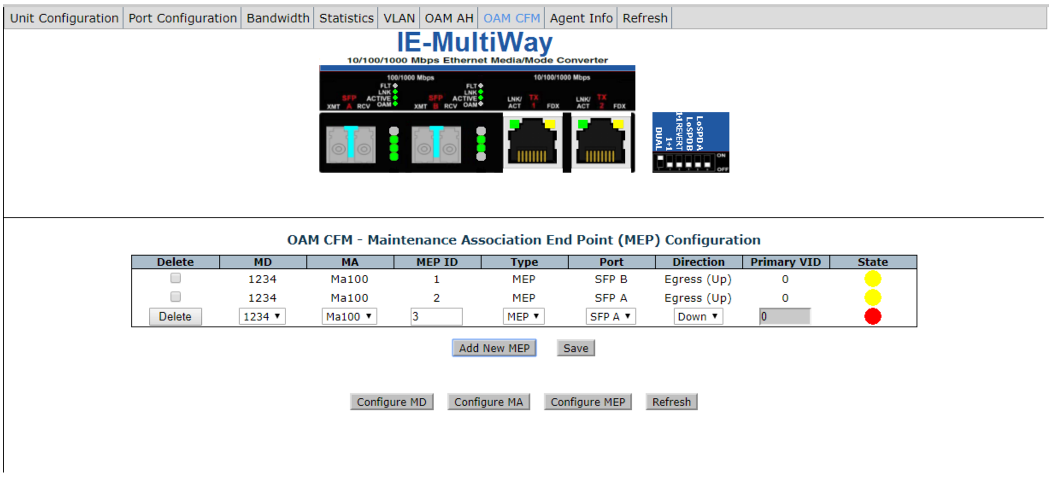
Figure 5.15 OAM CFM > Configure MA

Note!

iView^2 automatically displays this page if there is no MA yet defined when the user attempts to access any other menu control.

Select the **Domain** and **Format**, and enter the MA name in the Name field. Use **Interval** to select the interval for continuity check messaging, and choose **Primary VID**, if applicable. To cancel the MA without saving, select **Delete**. To store the MA, select **Save** and the screen is refreshed.

For a first time configuration, the next step is to create a MEP. Select **Add New MEP** to display the OAM CFM MEP configuration page as shown below:

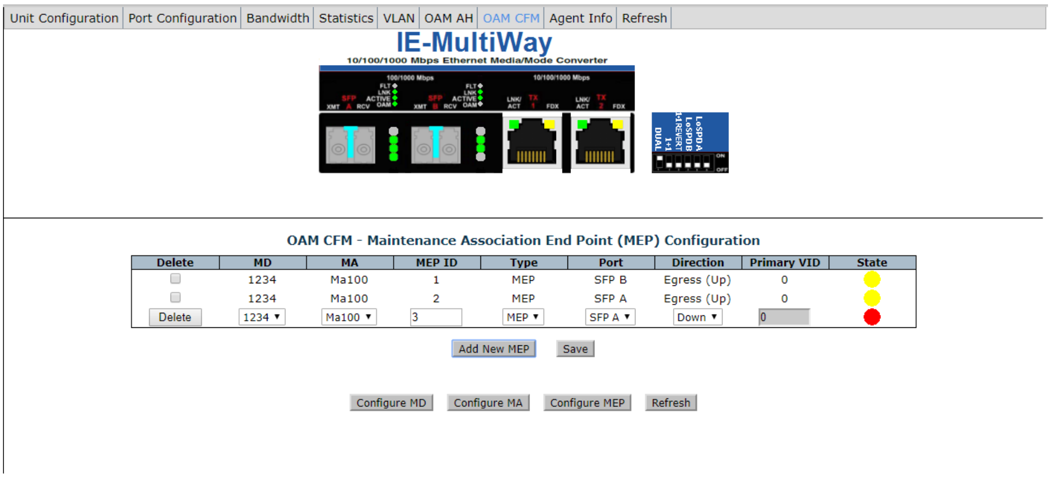


OAM CFM - Maintenance Association End Point (MEP) Configuration

Delete	MD	MA	MEP ID	Type	Port	Direction	Primary VID	State
□	1234	Ma100	1	MEP	SFP B	Egress (Up)	0	●
□	1234	Ma100	2	MEP	SFP A	Egress (Up)	0	●
Delete	1234 ▾	Ma100 ▾	3	MEP ▾	SFP A ▾	Down ▾	0	●

Select the MD, MA, enter the MEP ID, select the appropriate type, port and direction, and select the **Primary VID**, if applicable. To cancel the MEP without saving, select **Delete**. To store the MEP, select **Save** and the screen is refreshed.

Once the user has configured the MD, MA and at least one MEP, a particular instance of an MEP can be accessed for more detailed configuration. To access a particular instance of an MEP, click on the row containing the desired MEP as shown below:



OAM CFM - Maintenance Association End Point (MEP) Configuration

Delete	MD	MA	MEP ID	Type	Port	Direction	Primary VID	State
□	1234	Ma100	1	MEP	SFP B	Egress (Up)	0	●
□	1234	Ma100	2	MEP	SFP A	Egress (Up)	0	●
Delete	1234 ▾	Ma100 ▾	3	MEP ▾	SFP A ▾	Down ▾	0	●

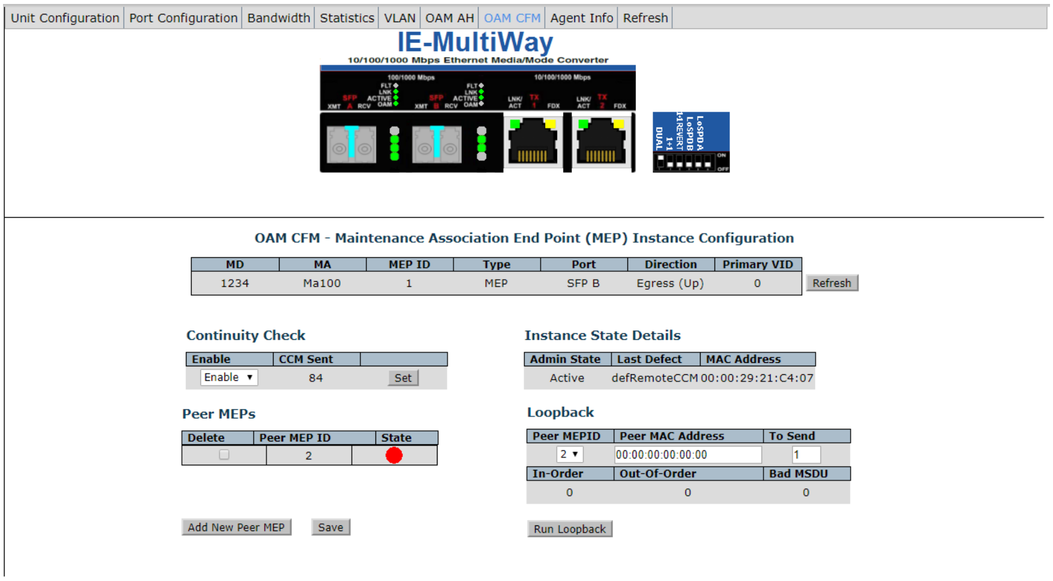
The current state of the MEP is shown by the color in the “State” column.

Color	Description
Green	Correctly functioning MEP - all MEPs are active and sending CCMs.
Red	Idle state or problem associated with the MEP.
Yellow	Not all peer MEP CCMs are being received.

Moving the mouse over the displayed color displays a comment giving additional information about the current state. Valid comments are:

- MEP is Idle
- MEP is Active
- Remote MEP Idle
- Remote MEP Failed

The MEP Instance Configuration page offers more details about an individual MEP as shown below.



OAM CFM - Maintenance Association End Point (MEP) Instance Configuration

MD	MA	MEP ID	Type	Port	Direction	Primary VID
1234	Ma100	1	MEP	SFP B	Egress (Up)	0

Continuity Check

Enable	CCM Sent	
Enable ▾	84	Set

Instance State Details

Admin State	Last Defect	MAC Address
Active	defRemoteCCM	00:00:29:21:C4:07

Peer MEPs

Delete	Peer MEP ID	State
□	2	●

Loopback

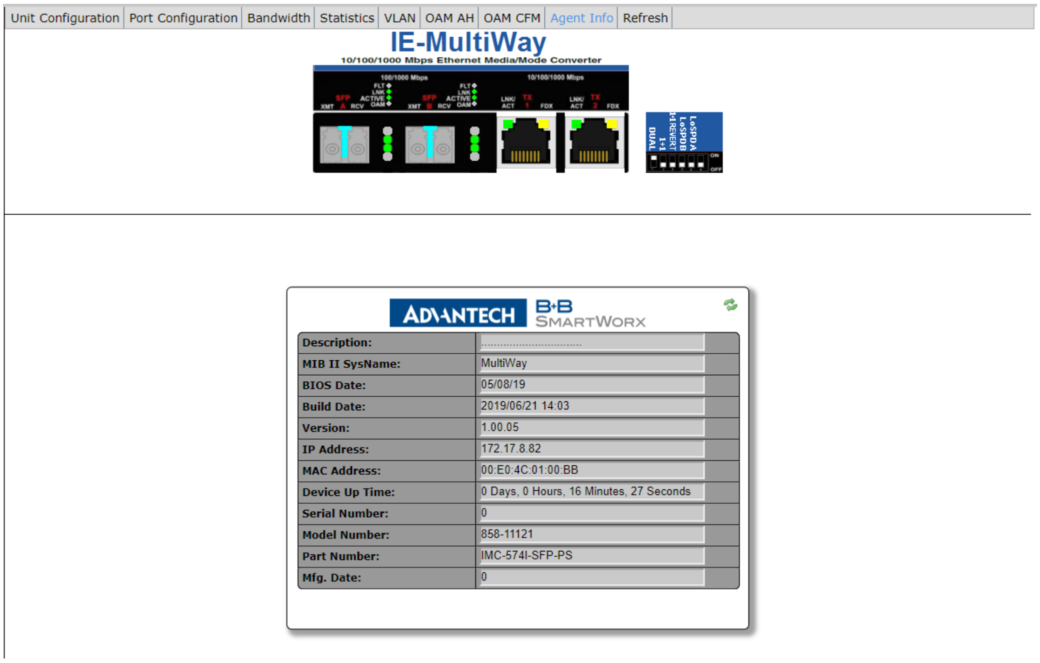
Peer MEPID	Peer MAC Address	To Send
2 ▾	00:00:00:00:00:00	1
In-Order	**Out-Of-Order**	**Bad MSDU**
0	0	0

From this screen, the user can perform the following functions.

Function	Description
Continuity Check	Enable/disable CCMs and verify the number of CCMs that have been sent.
Instance State Details	Verify the current administrative state of the MEP, view the last defect identified by the MEP, and view the MAC address of the MEP.
Peer MEPs	Create/List/Delete Peer MEPS associated with the MEP.
Loopback	Activate loopback and see the results of loopback operations.

5.10 Agent Info

Select **Agent Info** to obtain data on IP address, firmware version and other info.



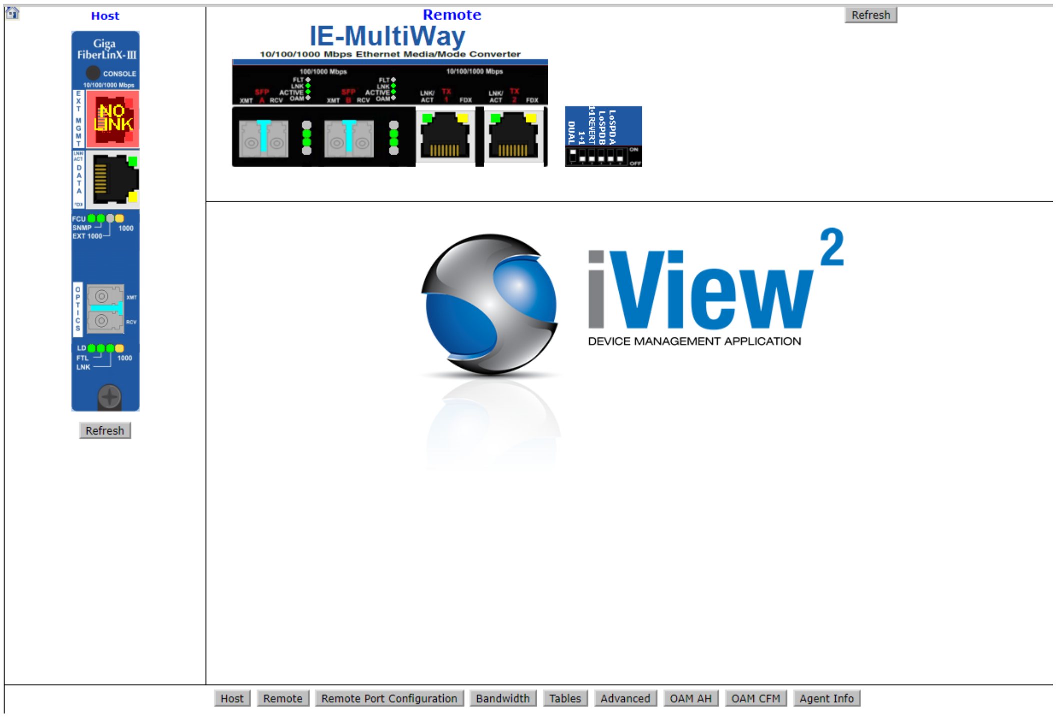
Description:	....
MIB II SysName:	MultiWay
BIOS Date:	05/08/19
Build Date:	2019/06/21 14:03
Version:	1.00.05
IP Address:	172.17.8.82
MAC Address:	00:E0:4C:01:00:BB
Device Up Time:	0 Days, 0 Hours, 16 Minutes, 27 Seconds
Serial Number:	0
Model Number:	858-11121
Part Number:	IMC-574I-SFP-PS
Mfg. Date:	0

Figure 5.16 Agent Info

5.11 Connecting IMC-574I-SFP to iMcV-Giga-FiberLinX-II or -III

If the IMC-574I-SFP is being set up as a Remote to a Host connection with an iMcV-Giga-FiberLinX-II or iMcV-Giga-FiberLinX-III, iView^2 provides support for SNMP management of the pair. Several pairs can be managed via UMA through the SNMP management module on the same IP address.

For information or instructions on the use of Unified Management Agent (UMA) refer to the SNMP Management module manual, available on the Advantech website.



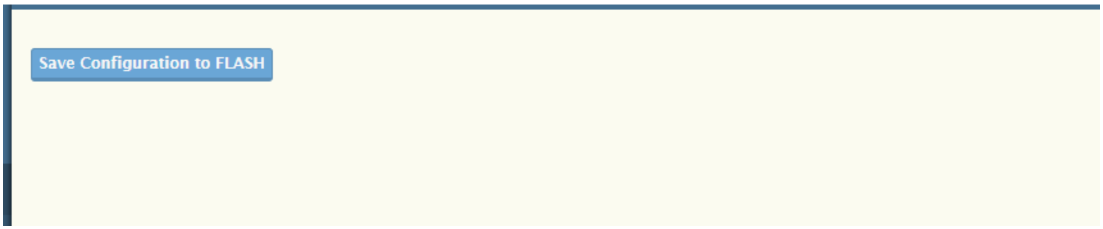
5.11.1 Configuration File Save/Restore Function

5.11.2 Requirements

The Configuration File Save/Restore Function available through the web interface (web-http) allows a user to backup all the configuration settings of a unit. With this backup, a user can restore settings to a unit if necessary or use the backup to apply the same settings to a different unit.

5.11.3 Saving a Configuration File to Flash

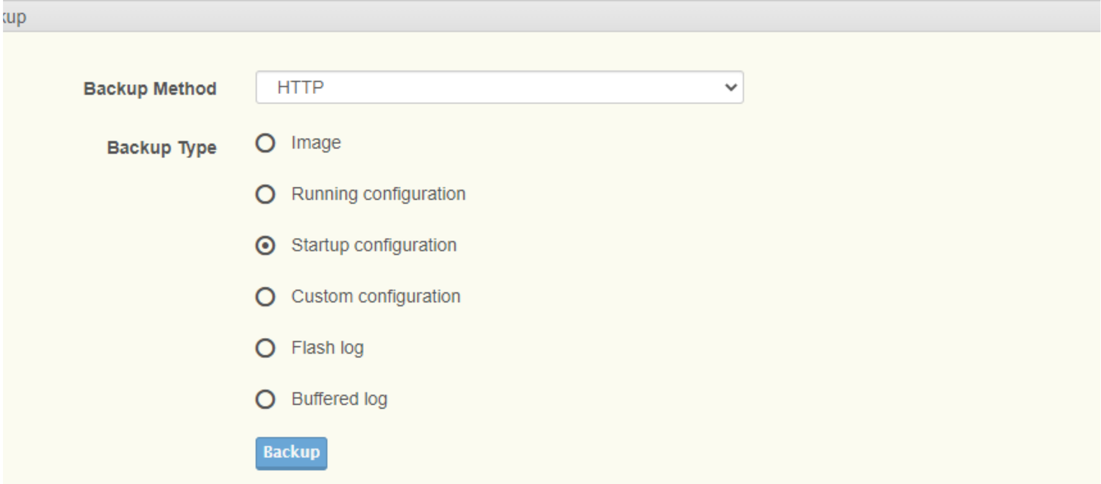
1. To access this page, log in to the user interface through a browser.
2. Navigate to **Tools** > **Save Configuration**.
3. Click the **Save Configuration to FLASH** button from the Save Configuration page.



The configuration settings are saved to FLASH.

5.11.4 Backing Up Configuration

1. To access this page, log in to the user interface through a browser.
2. Navigate to **Tools** > **Backup Manager**.
3. Click the Backup Method drop-down menu and select the method to use for the procedure.
4. Under Backup Type, click the type of configuration backup to create. Options:
   - Image
   - Running Configuration
   - Startup Configuration
   - Custom Configuration
   - Flash log
   - Buffered log
5. Click **Backup** to continue. The configuration is saved.



Backup Method: HTTP

Backup Type:
○ Image
○ Running configuration
● Startup configuration
○ Custom configuration
○ Flash log
○ Buffered log

5.11.5 Uploading a Saved Configuration File

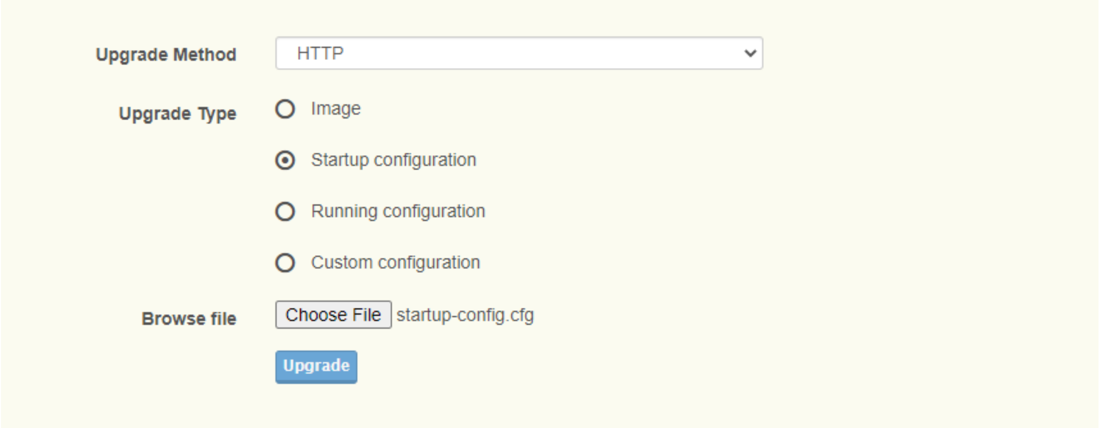
1. To access this page, log in to the user interface through a browser.
2. Navigate to **Tools** > **Upgrade Manager**.
3. Click the **Upgrade Method** drop-down menu and select the method to use for upgrading. Options: TFTP (default), HTTP, SFTP.

   If TFTP is selected, enter the following:
   - Server IP: Enter the IPv4 or IPv6 address of the source server.
   - File Name: Enter the file name of the corresponding configuration file.

   If SFTP is selected, enter the following:
   - Server IP: Enter the IPv4 or IPv6 address of the source server.
   - User Name: Enter the user name with access to the listed server.
   - Password: Enter the password corresponding to the listed user name.
   - File Name: Enter the file name of the corresponding configuration file.

   For this procedure the **Upgrade Method** selected is HTTP. The following instructions are specific to the HTTP uploading procedure.
4. Under Upgrade Type, select **Startup configuration**.
5. Under Browse file, click the **Choose File** to open an explorer window.
6. Select the configuration file and click **OK** to continue. The Upgrade page displays.

7. From the Upgrade page, click **Upgrade** to start the process.

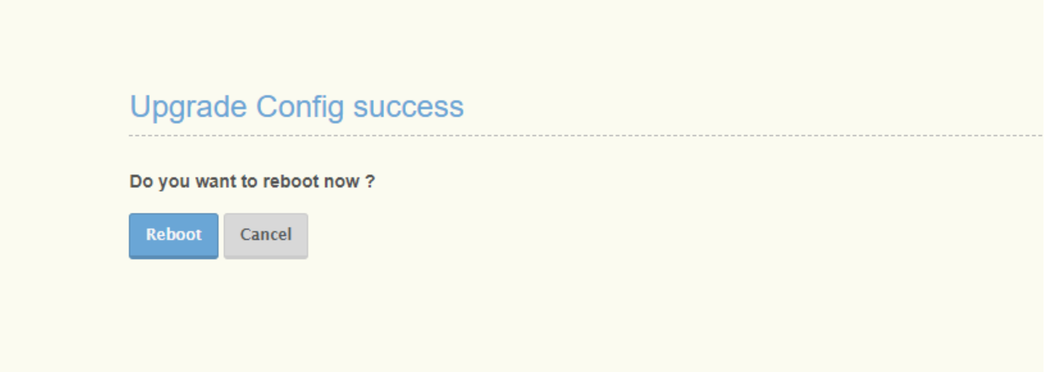


Upgrade Method: HTTP

Upgrade Type:
○ Image
● Startup configuration
○ Running configuration
○ Custom configuration

Browse file: Choose File startup-config.cfg

8. Once the upgrade process is completed a Upgrade Config Success screen displays.
9. To initiate the new configuration settings, the device requires a reboot. Click **Reboot** to restart the system to allow for the initiation of the new settings. Or, click **Cancel** to disregard the new configuration settings.



Upgrade Config success

Do you want to reboot now ?

The upgraded configuration is initiated after the system reboots.

Chapter 6

Troubleshooting

6.1 Troubleshooting

If a fiber connection cannot be established, perform the following to make sure that the fiber transceivers on the IMC-574I-SFP are not over/under driving the fiber receivers:

1. Make sure the fiber wavelength on both connected devices match (i.e. both are 1310 nm single-mode fiber).
2. Make sure the twisted-pair port speed on the IMC-574I-SFP matches that of the end devices connected to the IMC-574I-SFP. Configure the IMC-574I-SFP and its link partner to Auto Negotiation or, if using Force mode, make sure speed and duplex match.
3. IMC-574I-SFP allows the end user to assign a VLAN tag to all management traffic (SNMP and Telnet). It is important to understand that IF using Telnet or iView^2 to assign a VLAN tag to management traffic then as soon as this setting is saved the connectivity will be lost until the PC becomes a member of the VLAN which was assigned to management traffic.

   If a VLAN tag has been assigned to management traffic and the end user cannot re-establish a connection to the device via iView^2 or telnet, directly connect a PC to the device via the serial cable and review/modify the changes made.

6.2 Fiber Optic Cleaning Guidelines

Fiber Optic transmitters and receivers are extremely susceptible to contamination by particles of dirt or dust, which can obstruct the optic path and cause performance degradation. Good system performance requires clean optics and connector ferrules.

1. Use fiber patch cords (or connectors, if you terminate your own fiber) only from a reputable supplier; low-quality components can cause many hard-to-diagnose problems in an installation.
2. Dust caps are installed at the factory to ensure factory-clean optical devices. These protective caps should not be removed until the moment of connecting the fiber cable to the device. Should it be necessary to disconnect the fiber device, reinstall the protective dust caps.
3. Store spare caps in a dust-free environment such as a sealed plastic bag or box so that, when reinstalled, they do not introduce any contamination to the optics.
4. If you suspect that the optics have been contaminated, alternate between blasting with clean, dry, compressed air and flushing with methanol to remove particles of dirt.

6.3 Electrostatic Discharge Precautions

modules or standalone units, containing electronic components. Always observe the following precautions when installing or handling these kinds of products:

1. Do not remove unit from its protective packaging until ready to install.
2. Wear an ESD wrist grounding strap before handling any module or component. If a wrist strap is not available, maintain grounded contact with the system unit throughout any procedure requiring ESD protection.
3. Hold the units by the edges; do not touch the electronic components or gold connectors.
4. After removal, always place the boards on a grounded, static-free surface, ESD pad or in a proper ESD bag. Do not slide the modules or standalone units over any surface.

Warning! *Integrated circuits and fiber optic components are extremely susceptible to electrostatic discharge damage. Do not handle these components directly unless you are a qualified service technician and use tools and techniques that conform to accepted industry practices.*

ADVANTECH

Enabling an Intelligent Planet

www.advantech.com

Please verify specifications before quoting. This guide is intended for reference purposes only.

All product specifications are subject to change without notice.